

**JUSTIFICATION AND APPROVAL
FOR
OTHER THAN FULL AND OPEN COMPETITION
REQUISITION 192115VHQJTF0002**

This procurement is a GSA Schedule 70 order. This Justification for Other than Full and Open Competition (JOFOC) is submitted to justify restricting consideration due to "Brand Name" in accordance with FAR 6.302-1(c). The restriction of consideration is justified by the following facts and rationale:

(1) Agency and Contracting Activity

U.S. Department of Homeland Security (DHS)
U.S. Immigration and Customs Enforcement (ICE)
Office of Acquisition Management (OAQ)
801 I Street, NW, 8th Floor
Washington, DC 20536

(2) Nature and/or description of the action being approved

This is a "Brand Name" justification for Palantir Gotham software training and support services for the HSI (Homeland Security Investigations) Joint Task Force-Investigations. The JTF-I utilizes Palantir Gotham software (in its ICE application, called FALCON) to perform data analysis, federated data searches, and investigatory analysis of potential immigration and law violations.

(3) Description of the Supplies/Services

Vendor will provide one full-time training and desk-side support personnel to assist approximately 60 Special Agents, Criminal Investigators, Intelligence Analysts, Task Force Officers, and support personnel in achieving a high level of proficiency in utilizing FALCON Workspace to fulfill the missions and objectives of the JTF-I.

The Vendor employee will be responsible for the following tasks:

- Providing initial, introductory training in FALCON Workspace to new employees of the JTF-I;
- Providing advanced training in the functions and features of FALCON Workspace to veteran employees of the JTF-I;
- Ensuring that JTF-I employees, by the end of the period of performance, achieve independent proficiency in the features and functions of FALCON Workspace;
- Acquiring sufficient knowledge of JTF-I missions, objectives, policies, and procedures to work iteratively with JTF-I personnel to create innovative and effective workflows utilizing FALCON Workspace to achieve JTF-I goals;
- Coordinate with Palantir Technologies Forward Deployed Engineers and other Palantir system support staff to ensure that JTF-I employees are familiarized with and trained in the operations of new versions of FALCON Workspace which are deployed by Palantir

Technologies.

The total estimated cost for the base year and one option year is \$462,000.00.

(4) Identification of Statutory Authority Permitting Other Than Full and Open Competition

This procurement is a request for a competitive GSA Schedule 70 order. This JOFOC justifies restricting consideration due to "Brand Name". In accordance with 41 USC 253 (c) (1), as implemented by FAR 6.302-1(c) Application for Brand Name Descriptions, there is only one responsible source and no other supply or service will satisfy the agency's requirement. Accordingly, Palantir Gotham is the software package to be supported, and only training and support vendors who are authorized by Palantir to support their Gotham software are able to provide the required services.

(5) Demonstration That the Nature of the Acquisition Requires the Use of the Authority Cited

Palantir Gotham software is only sold by Palantir Technologies, not by any third-party resellers. Palantir Technologies has authorized three vendors to provide training and support services for their Gotham software.

(6) Efforts to Obtain Competition

This requirement for Palantir Gotham training and support services will be solicited to the 3 vendors authorized by Palantir Technologies to provide such services. Two of the vendors currently have GSA Schedule 70 pricing in place, and the third is anticipated to have such pricing in place by mid-September, 2015.

(7) Determination by the Contracting Officer that the Anticipated Cost to the Government will be Fair and Reasonable

It is anticipated that the purchase of FALCON training and support services will result in a competitive firm-fixed price (FFP) GSA Schedule 70 Delivery Order. Adequate price competition among GSA Schedule 70 vendors will be the primary basis for ensuring that prices are fair and reasonable, and there is a reasonable expectation of receiving at least three quotations. The award price will also be based on a price analysis of the Independent Government Cost Estimate (IGCE) and comparison of the proposed offers received.

(8) Description of Market Research Conducted

HSI contacted Palantir Technologies for their list of approved vendors. Internet research was also conducted, as well as reviews of various vendors' GSA Schedules.

(9) Other Facts Supporting the Use of Other Than Full and Open Competition

Not applicable.

(10) A Listing of Sources, if any, that have Expressed an Interest in this Acquisition

(b)(7)(E)

(11) A Statement of Actions, if any, the Agency May Take to Remove or Overcome any Barriers to Competition

To overcome barriers to competition, future requirements for Palantir Gotham software training and support services will be competed amongst all vendors authorized by Palantir Technologies to provide such services and awarded to the contractor that provides the best value to the Government.

(12) Technical/Requirements Personnel Certification:

I certify that the data supporting the recommendation to award of the FALCON/Palantir Gotham training and support services by other than full and open competition is complete and accurate to the best of my knowledge. I certify that this requirement meets the Government's minimum needs.

(b)(6);(b)(7)(C)

08/18/2015

Technical Representative/COTR

Date

(13) Contracting Officer's Certification:

I hereby determine that the anticipated cost (b)(7)(E) for the FALCON/Palantir Gotham software training and support services is fair and reasonable based on adequate price competition and price analysis supported by the historical data, and prices offered by GSA Schedule 70 vendors. I certify that this requirement meets the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate. Based on the foregoing, I approve the purchase of FALCON/Palantir Gotham software training and support services by other than full and open competition pursuant to the authority of FAR 6.302-1(c) Application for Brand Name Descriptions, as there is only one responsible source and no other supply or service will satisfy the agency's requirement.

Contracting Officer

Date



U.S. Immigration and Customs Enforcement

Background Memorandum:

ICE Analytics Procurement Strategy for the FALCON System

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Page 2975

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 2976

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 2977

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 2978

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 2979

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 2980

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

**JUSTIFICATION AND APPROVAL
FOR
OTHER THAN FULL AND OPEN COMPETITION
FALCON Cloud Hosting and Cloud Management Services**

This procurement is a sole source contract. This Justification for Other than Full and Open Competition (JOFOC) is submitted to justify restricting consideration due to “Unique supplies or services available from only one source or only one supplier with unique capabilities” in accordance with FAR 6.302-1(b)(1)(i). The restriction of consideration is justified by the following facts and rationale:

(1) Agency and Contracting Activity

U.S. Department of Homeland Security (DHS)
U.S. Immigration and Customs Enforcement (ICE)
Office of Acquisition Management (OAQ)
801 I Street, NW, (b)(6);(b)(7)
Washington, DC 20536

(2) Nature and/or description of the action being approved

The name of the proposed vendor is:
Palantir Technologies
100 Hamilton Avenue, Suite 300
Palo Alto, CA 94301

(b)(7)(E)

(3) Description of the Supplies/Services

(b)(7)(E)

(b)(7)(E)

(4) Identification of Statutory Authority Permitting Other Than Full and Open Competition

This JOFOC justifies restricting consideration due to “Unique supplies or services available from only one source or only one supplier with unique capabilities”. The statutory authority permitting other than full and open completion is 41 U.S.C 3304(a)(1) implemented by Federal Acquisition Regulation (FAR subpart 6.302-1 entitled “Only One Responsible source and no other supplies or services will satisfy agency requirements.”

(5) Demonstration That the Nature of the Acquisition Requires the Use of the Authority Cited

(b)(7)(E)

(b)(7)(E)

(6) Efforts to Obtain Competition

Please see the description of relative factors listed below in Section (8).

(7) Determination by the Contracting Officer that the Anticipated Cost to the Government will be Fair and Reasonable

The Contracting Officer has determined that the anticipated price will be fair and reasonable based on a comparison with the most recently awarded comparable services (Palantir PCloud Cloud management services, Amazon AWS GovCloud hosting services, and AWS support services for ICM and TLS).

(8) Description of Market Research Conducted

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(9) Other Facts Supporting the Use of Other Than Full and Open Competition

Not applicable.

(10) A Listing of Sources, if any, that have Expressed an Interest in this Acquisition

Palantir Technologies, Inc.

(11) A Statement of Actions, if any, the Agency May Take to Remove or Overcome any Barriers to Competition

To overcome barriers to competition, future requirements for FALCON Cloud Hosting and Cloud Management Services will be competed amongst all vendors that meet the Government's technical requirements to provide such services and awarded to the contractor that provides the best value to the Government.

(12) Technical/Requirements Personnel Certification:

I certify that the data supporting the recommendation to award of the FALCON Cloud Hosting and Cloud Management Services by other than full and open competition is complete and accurate to the best of my knowledge. I certify that this requirement meets the Government's minimum needs.

(b)(6);(b)(7)(C)

Technical Representative/COTR

09/27/2016

Date

(13) Contracting Officer's Certification:

I hereby determine that the anticipated cost of \$6,761,109 (\$1,647,016 for the initial 8-month period of performance) for the FALCON Cloud Hosting and Cloud Management Services is fair and reasonable based on price analysis supported by the historical data. I certify that this requirement meets the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate. Based on the foregoing, I approve the purchase of FALCON Cloud Hosting and Cloud Management Services by other than full and open competition pursuant to the authority of FAR 6.302-1(b)(1)(i) "Unique supplies or services available from only one source or only one supplier with unique capabilities," as there is only one responsible source and no other supply or service will satisfy the agency's requirement.

Contracting Officer

Date



U.S. Immigration
and Customs
Enforcement

For Official Use Only

FALCON OPERATIONS & MAINTENANCE SUPPORT & SYSTEM ENHANCEMENT Performance Work Statement

May 11, 2015

Homeland Security Investigations (HSI)

Mission Support



Homeland
Security

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

FALCON System Operations & Maintenance Support Services and System Enhancement

1.0 PROJECT TITLE

Performance Work Statement (PWS) for FALCON System Operations and Maintenance Support Services and System Enhancement

2.0 BACKGROUND

United States Immigration and Customs Enforcement (ICE) is the largest investigative branch of the Department of Homeland Security (DHS). As part of ICE, Homeland Security Investigations (HSI) is a critical asset in accomplishing the ICE mission and is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within and out of the United States. For this acquisition, the Contractor shall be responsible for the overall management, planning, implementation, operation, maintenance, coordination, and support of one of HSI Information Sharing and Infrastructure Management's (ISIM) technology platforms and software assets, FALCON. FALCON provides HSI's agents and analysts with a key investigative resource: a wholly integrated, consolidated platform performing federated search, analytics, geospatial referencing, reporting and situational awareness capabilities across a broadly diverse universe of structured and unstructured law enforcement data residing in numerous, disparate source environments.

The FALCON system is comprised of several sub-components. The largest of these is FALCON-SA (Search and Analysis)/Workspace, used by the entire community of FALCON users. Users of FALCON-SA/Workspace/DARTTS have access to the following data sets:

(b)(7)(E)

ords

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

below which describes this process).

A FAR 52.217-8, 6-month optional extension allows for six months' worth of Operations and Maintenance Support Services to be purchased after the end of Option Year 2.

3.0 SCOPE

FALCON uses commercial software sold by Palantir Technologies, Inc., called Palantir Gotham, configured for ICE. Current and future releases of FALCON are required to have System Maintenance and Services support for the purpose of applying adaptive, perfective and corrective maintenance to the application as well as operating and maintaining the FALCON infrastructure, authoring and delivering training, supporting the end user community, and delivering small-to medium-scale enhancements to the existing application.

(b)(6);(b)(7)(C)

At the beginning of each year of contract performance, the AD and DAD over the FALCON program, with the input of the ESC and of the Contractor will agree upon the addition of up to five outcomes to be completed during the upcoming year (the number of outcomes may be higher if both parties agree). If ICE and the Contractor are unable to agree upon the scope of a given outcome or set of outcomes, the Contractor will provide a detailed technical rationale as to why the outcome falls outside the scope of PWS. This written rationale shall include the level of effort and why this level of effort is not attainable and shall be presented to the ICE FALCON Program Manager and COR/ACOR within five (5) business days of the Contractor's initial announcement of lack of agreement on the Statement of Outcomes. In this scenario, HSI management and the Contractor's management will use this information to reach a final agreement on the Statement of Outcomes. Contractor will provide the implementation support

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

for all tasks listed in an annual outcomes statement to which both HSI and the Contractor agree.

The Contractor will provide the implementation support for all tasks listed in the annual outcomes statement and will provide all processing power required to support any tasks listed in the annual outcomes statement with no degradation to existing levels of performance. The annual Statement of Outcomes shall be incorporated into the contract through bilateral modification.

Should the provision by the Contractor of a technical rationale for the non-feasibility of an outcome fail to result in agreement between HSI management and the Contractor's management on the contents of the Statement of Outcomes, either party may request adjudication from the assigned ICE Contracting Officer (CO), who shall make a determination within five (5) business days of receipt of the adjudication request as to whether or not the disputed outcome(s) shall be included in the Statement of Outcomes. In the event that HSI's priorities change during the period of time covered by a Statement of Outcomes and HSI requests that the Statement of Outcomes be amended, and the Contractor determines that this new request for work does not clearly fall within the scope of the existing Statement of Outcomes, the Contractor may present the change request to the CO, who shall review the request to determine whether HSI's request falls within the scope of that document. Such determinations must be made within five (5) business days of the escalation request. The Contractor will not be obligated to take any action on the new request for work unless and until the CO, in coordination with the Contractor, approves the request and determines that such request falls within the scope of an existing Statement of Outcomes or otherwise amends such document to include the new request for work. In the event the CO and Contractor are unable to reach an agreement, the matter will be referred to ICE's Informational Technology Division Assistant Director for final adjudication. For any priority tasks outside the scope of the existing Statement of Outcomes, HSI may request a level of effort from Contractor; Contractor shall not be obligated to perform such tasks unless (i) the task consists of high priority case work and is specifically requested by the Executive Assistant Director of HSI (or his/her designee); and (ii) a required task of a comparable level of effort is explicitly postponed or eliminated.

Changes to the annual Statement of Outcomes shall be incorporated into the contract through bilateral modification.

4.0 APPLICABLE DOCUMENTS

All ICE systems shall comply with the following guidelines and regulations:

- DHS Acquisition Management Directive 102-01 Handbook
- ICE Enterprise Systems Assurance Plan
- ICE System Lifecycle Management (SLM) Handbook, Version 1.4, January, 2012
- ICE Technical Architecture Guidebook

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

- ICE Technical Reference Model (TRM) (Standards Profile)
 - The Offeror shall identify any hardware, software, and/or licenses required for its proposed solution. The Government is prepared to provide any hardware and software items that are included within the ICE TRM that would reasonably be utilized by Offerors for the system development. Test and evaluation tools listed within the TRM are not provided as Government Furnished Equipment (GFE).
- 4300A DHS Information Security Policy
- 4300A Sensitive Systems Handbook

The following documents are applicable to understanding the target ICE/HSI systems:

- International Information Systems Security Certification Consortium (ISC²) Standards
- National Industrial Security Program Operating Manual (NISPOM), February 28, 2006
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)
 - o Guidelines
 - o Special Publications
 - o Standards
- NIST Special Publication 800-37, Guide for the Certification and Accreditation of Federal Information Systems
- Federal Information Processing Standard (FIPS) 199
- Federal Information Security Management Act (FISMA), November 22, 2002
- Federal Information Technology Security Assessment Framework (FITSAF), November 28, 2000
- Federal OMB Circular A-130, Management of Federal Information Resources
- Federal Privacy Act of 1974 (As Amended)
- Federal Records Act
- DHS 4300A, Sensitive Systems Policy Directive, Version 6.1.1, October 31, 2008
- DHS Management Directive (MD) 4300.1, Information Technology Systems Security, November 03, 2008
- DHS MD Volume 11000 – Security
- DHS Office of Chief Information Officer (OCIO) E-Government Act Report 2008

Please note that if newer versions of these documents are officially released, the Contractor shall comply with the updated versions within the timeframe established by the Government.

5.0 TASKS

The Contractor shall provide qualified, experienced personnel to deliver support for the continued System Maintenance and Services tasks associated with FALCON. This requirement includes the tasks described in the following sections:

5.1 Tier 1 – Help Desk Support

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Help Desk Support consists of the following responsibilities:

- Receiving and recording accurately all inquiries from End Users regarding application functionality and services and assigning tasks as needed to the appropriate Software Maintenance Tier 2 or Tier 3 Support group for resolution;
- Dealing directly with:
 - simple requests such as password resets and account unlocks
 - basic network and application troubleshooting
 - application usage and operational feature questions and issues;
- Monitoring the tickets created to ensure users are updated on tickets' status and progress;
- Providing reports to ICE management and System / Application Program Management as required or requested.

Tier 1 hours of operation shall be from 0900 to 1700 Eastern Time (ET) Monday thru Friday with support response times during these hours being immediate for telephonic inquiries and within one hour for email reports. Non-emergency, off-hours inquiries/ticket submissions will be addressed as soon as is practical and serviced no later than one hour after the commencement of normal operating hours.

At the government's discretion Tier 1 – Help Desk Support may be ultimately transitioned to the ICE Enterprise Help Desk. The contractor will be required to support such a transition by providing 'How Tos,' FAQ responses, scripted tutorials, etc. consistent with the provision of this level of customer support.

Tier 2 System Maintenance and Support

All items that cannot be resolved at the Tier 1 Support level shall be automatically turned over to Tier 2 System Maintenance and Support;

- The Contractor shall report the status of the ticket using Atlassian Jira tracking software;
- Typical Tier 2 activities would include patching systems, running scripts, effecting minor fixes, etc.;
- Tier 2 System Maintenance and Support shall be operational in accordance with the performance levels identified in Section 6.0;
- The Contractor shall respond to all Tier 2 System Maintenance tickets in accordance with the contract;
- The Contractor shall implement an application feedback loop, whereas systemic issues identified during common Tier 1, 2, and 3 escalation procedures are routinely evaluated and reviewed with the appropriate Project Manager to assess the need for a SCR for a future release.
- If Tier 2 System Maintenance Support cannot resolve the assigned ticket or perform the required tasks then the ticket shall be referred to the Tier 3 - System Maintenance and Support.

Tier 3 - System Maintenance and Support

The Contractor shall identify and correct software, performance, and implementation failures for

FALCON Operations & Maintenance Support & System Enhancement

Performance Work Statement

the application software as well as evaluate and estimate the level of effort associated with requests for system modification. Corrective work includes performing SCRs that reflect a change to requirements or technical specifications, as well as updating and maintaining the required SLM documentation as necessary. Contractor staff and the COR will come to mutual agreement over which changes to the system constitute SCRs, as opposed to every day System Tuning (Section 5.2.3) and System Administration (Section 5.2.4) actions not requiring the SCR process.

- All maintenance activities that reach this level shall have an SCR opened and be reported using Atlassian Jira;
- SCRs will be prioritized and agreed to by the authorized government personnel and entered into the ICE approved management tracking tool. SCRs will be approved in writing by the government;
- Prior to commencing a system modification, the Contractor and the Office of the Chief Information Officer (OCIO) Information Technology (IT) project manager shall agree on the degree of the modification as minor, moderate, or major (see table below for classification);
- The Contractor shall implement an application feedback loop, whereas systemic issues identified during common Tier 1, 2, and 3 escalation procedures are routinely evaluated and reviewed with the IT Project Manager to assess the need for a SCR in future release.
- The Contractor shall respond to all Tier 3 System Maintenance Support tickets in accordance with the contract;
- Software changes to applications are based upon the submission of an SCR, and are classified as minor, moderate, or major changes, where:

Table 1: Change Requests

Type Change	Estimated Effort Required
Minor Change	1–40 Hours
Moderate Change	41–500 Hours
Major Change	501–1500 Hours

The Contractor shall provide Software Maintenance Tier 2 and Tier 3 Support. Software Maintenance Tier 2 and Tier 3 Support hours of operation shall be Monday through Friday 8am-6pm, ET, excluding holidays and weekends.

For emergency situations both during and outside of the normal support business hours that involve a system outage or a widespread interruption in user access to FALCON, the Contractor shall notify the FALCON Program Manager or designate within 30 minutes of occurrence. Emergencies will be further defined as part of the Software Tier 3 Support procedures, but in general an emergency is when the system is down or when multiple users are unable to access FALCON. The Contractor shall document all user problem notifications and solutions.

For Tier 3 Software Maintenance and Support, the number of anticipated SCRs is listed in the matrix below:

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Change Classification	Estimated Effort Required	Estimated number of SCRs to Be Conducted – Per Year
Minor Change	1 – 40 Hours	20
Moderate Change	41 – 500 Hours	10
Major Change	501 – 1500 Hours	5

SCRs for FALCON may include Contractor's assistance with requirements analysis for which the contracting officer anticipates no reasonable expectation of organizational conflicts of interest, design, enhancement, development (in the case of a major SCR), integration & testing, and implementation, including any updates needed to product documentation. Typically, these activities involve the delivery of helper applications to assist end users with automating common, repetitive tasks in the system (such as importing and exporting various types of data and formatting that data), interfacing programs communicating with FALCON via the common operating Application Program Interfaces (APIs) and the mapping and integration of additional data sources.

ICE reserves the right to request FAR 52.227-14 (Alt IV) for any software development/modification/enhancement that is mutually determined in writing to be a major SCR under this performance work statement.

5.2 Operational Support

The Contractor shall provide Operational Support for the FALCON system. Table 2 and Table 3 detail the hardware and software infrastructure currently in place for FALCON. The hardware and software listed below is subject to change based on future expansion requirements and datacenter moves as requested by FALCON PMO.

Table 2. FALCON System Hardware

Hardware/Operating System	Location	Remarks
(b)(7)(E)		

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Hardware/Operating System	Location	Remarks
(b)(7)(E)		

Table 3. FALCON System Software

Operating Information System	Location	Remarks
(b)(7)(E)		

PCN-Potomac Center North, 500 12th St SW, Washington, DC 20536

Table 4. FALCON System Firmware

Hardware Device	Firmware	Remarks
(b)(7)(E)		

Operational support shall include the activities below:

5.2.1 Operational Support - Interfaces and Data Sources

(b)(7)(E)

(b)(7)(E)

5.2.2 Operational Support - Database

The Contractor shall support all management and updates to the FALCON data stores and indices. This includes all database structural changes and ontology updates to support system enhancements and defect corrections and the implementation of database scripts to update or query information in the database as required. The Contractor shall support ad-hoc queries as requested by the HSI FALCON program management office (PMO) and/or perform data analysis as requested.

5.2.3 Operational Support – System Tuning

The Contractor shall conduct performance tuning of the FALCON system as a result of findings during regular system monitoring and/or as operational needs arise. The Contractor shall provide the FALCON PMO with recommendations regarding system performance improvements to foster a more stable and robust operational system.

5.2.4 Operational Support – System Administration

The Contractor shall provide system administration activities to include regular monitoring of system resource utilization, disk storage utilization, identification of corrupt files or processes, system archiving, data archiving, installing operating system/software updates/versions and performing application backups; correcting flaws in software applications that escaped detection during testing of the system, or that have been introduced during previous maintenance activities; and improving software attributes such as performance, memory usage, and documentation.

5.3 Configuration Management

The Contractor shall conduct application-level configuration management for all Software Operation and Maintenance (O&M) changes made to the system. The Contractor shall handle all requests for changes to established baselines and configuration management thereof via the ICE approved SCR process. The Contractor shall assign proper identification of all configuration items in accordance with agreed upon naming and numbering conventions.

5.4 Training Support Included in Operations and Maintenance Services

The Contractor shall maintain and update training materials to include User Guides, Training Plans, and System Administration and Operations Manuals when an enhancement, or other significant Software O&M release, occurs. The Contractor shall provide an electronic copy of all training material. The Contractor shall also coordinate with the FALCON PMO to insure that all members are familiar with the updates to the application. The Contractor shall provide training to Special agents and analyst groups meeting the established, written criteria for successful Strategic training classes as approved by the FALCON PMO and agreed to by the Contractor, to include such services as classroom training, desk-side support of individual ICE

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Agents, Special Agents, Group Supervisors, or other employees involved in directly supporting active investigations, or small groups of such employees (6 or fewer), with desk-side support training pursued on a strategic basis targeting only users with a clear, operational use for the FALCON system. Additionally, Contractor staff will work with the Office of Training Development (OTD) and Federal Law Enforcement Training Center (FLETC) staff to productively include FALCON training in their regular programs as requested. There is no explicit training goal by user count. While the above specified training is included in O&M, any significant expansion beyond the Strategic Training program, or any broad solicitation of new training requests across substantially the whole of ICE's organization must be discussed and agreed to with the Contractor staff to avoid logistically, or financially prohibitive training commitments.

5.5 Support of FALCON Mobile Technology

Contractor support for the FALCON Mobile system on the Apple iOS operating system utilized for the iPhone shall include support for the following features:

- Ability to track team movements on map for operational and officer safety
- Ability to coordinate movements of entire teams by communicating across mobile devices
- Ability to create charts, structured dossiers with mugshots, and other complex intelligence products and relay them directly to mobile devices in the field
- Ability to plot target locations to show clusters of activity
- Simple, quick searches of both ingested and remotely accessible data; searches can be performed from remote locations
- Ability to access user-published ad hoc data
- Deconfliction of data elements (persons, places, objects, events)
- Ability to send text messages and photos to command center

Contractor shall ensure the FALCON infrastructure incorporates adequate server cores and processing power to enable the entire contingent of HSI Special Agents (approximately 7,000 employees) to have access to FALCON Mobile by March 13, 2016 and shall ensure there will be no degradation of overall system performance from current levels.

5.6 System Enhancements to Be Instituted During the Initial POP, Option Years 1-2, and the Optional Six-Month Extension

(b)(7)(E)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

(b)(7)(E)

5.6.1 Project Plans and Schedules

The Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten work days after the beginning of a contract year a draft Schedule of Outcomes, listing the planned start dates of each planned outcome-based project. Based upon this Schedule of Outcomes, the Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten working days prior to the initiation of work on a particular outcome-based project a Project Plan and a Project Schedule. The one exception shall be for the first of the planned outcome-based projects, for which a Project Plan and a Project Schedule shall be delivered by the Contractor concurrently with delivery of the draft Schedule of Outcomes.

Project Plans, mutually agreed to by HSI and the Contractor, shall identify specific user groups, workflows and discrete tasks. The Project Plans will define the agreed upon scope of each outcome – any and all changes to the Project Plans must be mutually agreed upon by the parties and documented in weekly and/or monthly reports. Specifically, any addition of a new task within the Project Plan must be mutually agreed upon by the parties, and counterbalanced with the deletion or delay of an existing task of equal effort, as documented in weekly and/or monthly reports. Project Schedules shall list high-level tasks for a specified outcome-based project. Project Plans and Schedules may be amended by the two parties' mutual agreement.

5.6.2 Escalations / Resolutions of Disagreements Concerning Project Scope

As described in Section 5.6.1 above, at the beginning of each year of contract performance, the AD and DAD over the FALCON program, with the input of the ESC and of the Contractor will agree upon the addition of up to five outcomes to be completed during the upcoming year

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(the number of outcomes may be higher if both parties agree). If ICE and the Contractor are unable to agree upon the scope of a given outcome or set of outcomes, the Contractor will provide a detailed technical rationale as to why the outcome falls outside the scope of PWS. This written rationale shall include the level of effort and why this level of effort is not attainable and shall be presented to the ICE FALCON Program Manager and COR/ACOR within five (5) business days of the Contractor's initial announcement of lack of agreement on the Statement of Outcomes. In this scenario, HSI management and the Contractor's management will use this information to reach a final agreement on the Statement of Outcomes. Contractor will provide the implementation support for all tasks listed in an annual outcomes statement to which both HSI and the Contractor agree.

Should the provision by the Contractor of a technical rationale for the non-feasibility of an outcome fail to result in agreement between HSI management and the Contractor's management on the contents of the Statement of Outcomes, either party may request adjudication from the assigned ICE Contracting Officer (CO), who shall make a determination within five (5) business days of receipt of the adjudication request as to whether or not the disputed outcome(s) shall be included in the Statement of Outcomes. In the event that HSI's priorities change during the period of time covered by a Statement of Outcomes and HSI requests that the Statement of Outcomes be amended, and the Contractor determines that this new request for work does not clearly fall within the scope of the existing Statement of Outcomes, the Contractor may present the change request to the CO, who shall review the request to determine whether HSI's request falls within the scope of that document. Such determinations must be made within five (5) business days of the escalation request. The Contractor will not be obligated to take any action on the new request for work unless and until the CO, in coordination with the Contractor, approves the request and determines that such request falls within the scope of an existing Statement of Outcomes or otherwise amends such document to include the new request for work. In the event the CO and Contractor are unable to reach an agreement, the matter will be referred to ICE's Informational Technology Division Assistant Director for final adjudication. For any priority tasks outside the scope of the existing Statement of Outcomes, HSI may request a level of effort from Contractor; Contractor shall not be obligated to perform such tasks unless (i) the task consists of high priority case work and is specifically requested by the Executive Assistant Director of HSI (or his/her designee); and (ii) a required task of a comparable level of effort is explicitly postponed or eliminated.

Changes to the annual Statement of Outcomes shall be incorporated into the contract through bilateral modification.

6.0 PERFORMANCE STANDARDS

The following table defines the performance standards to be adhered to for the FALCON System Maintenance and Services effort and regarding maintaining overall system performance as new

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(5)

Table 5. Performance Standards

Tasks	Metric	Service Level Agreement	How it will be measured
Tier 1 – Help Desk Support	Response Time for incoming emails during business hours M-F 09:00-17:00pm EST	The end of the current day	Time the email is received in the Help Desk Inbox until time the request is accessed for action.
Tier 1 – Help Desk Support	Response Time for incoming emails after help desk hours	The end of the following day	Time the email is received in the Help Desk Inbox until time the request is accessed for action.
Tier 1 – Help Desk Support	Resolution Time for incoming emails that have been accessed for action during 09:00-17:00pm EST and after hours.	No More than 24 hours, or when the user stops responding	24 hours from the time when the email is accessed for action until it is resolved or moved to Tier 2 or 3.
Tier 2 Software Support	Response time for Tier 2 tickets received during defined business hours	The end of the current day	Time the ticket is assigned to Tier 2 until the time the ticket is accessed for action.
Tier 2 Software Support	Average resolution time of Tier 2 tickets	8 business days	Time the ticket is placed in the Tier 2 queue for action to the time it appears as closed or referred, divided by the total number of tickets.

¹ Any enhancements, corrective maintenance, or other code changes to FALCON should not negatively impact system performance. Specifically, system performance will be baselined at the beginning of the contract and will be re-baselined at the completion of any major releases. This baseline will serve as the minimum for acceptable system performance.

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Tier 2 Software Support	Response time for Tier 2 tickets, after hours	The end of the following day	Time the ticket is assigned until the time the ticket is picked up for action.
Tier 2 Software Support	Average resolution time for Tier 2 tickets, received after defined business hours	8 business days	Time the ticket is placed in the Tier 2 queue for action to the time it appears as closed or referred, system, divided by the total number of tickets.
Tier 3 Software Support	Response time for Tier 3 tickets during specified business hours not involving a system outage or denial of access to substantial numbers of users	No more than 4 hours	Time the ticket is assigned to Tier 3 until the time the ticket is accessed for action.
Tier 3 Software Support	Average resolution time of Tier 3 tickets not involving a system outage or denial of access to substantial numbers of users	8 business days	Time the ticket is placed in the Tier 3 queue for action to the time it appears as closed or referred, system, divided by the total number of tickets

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Tier 3 Software Support	Response time for Emergency tickets, either during specified business hours or after hours, that involve a system outage or denial of access to substantial numbers of users	FALCON Program Manager or designate shall be alerted no more than 30 minutes after occurrence	Time the ticket is assigned as an Emergency until the time the ticket is picked up for action.
Tier 3 Software Support	Average resolution time for Emergency tickets, either during specified business hours or after hours	No more than 8 hours	Time the ticket is placed in the Tier 3 queue for action to the time it appears as closed or referred, system, divided by the total number of tickets
Workspace Quick Search	Average time for users to receive results from a search conducted in FALCON Workspace	1 second	Performance data provided by Contractor in QASP reports
Workspace Document Load	Average time for users to see a document on their FALCON Workspace screen once the document has been selected	0.5 seconds	Performance data provided by Contractor in QASP reports

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

DARTTS Search	Average time for server to return results from a search conducted in FALCON-DARTTS	0.35 seconds	Performance data provided by Contractor in QASP reports
---------------	--	--------------	---

Tasks	Metric	Service Level Agreement	How it will be measured
Operational Support	Uptime Rate - Percentage of time that the application is available to users in fully-functioning mode ²	98% or higher	Cumulative uptime per month divided by the total time per month that FALCON is scheduled available.
Configuration Management	All SCR level changes will be tracked	100%	No changes will be made to the baseline without an associated SCR.
Training	Training and Training Material Delivery	100% on time	Delivery date versus scheduled delivery date.
Transition Out	Transition Out Plan	90 calendar days prior to end of POP	Delivery date

7.0 DELIVERABLES AND DELIVERY SCHEDULE

Specific deliverables related to each activity are outlined below.

7.1 System Lifecycle Management (SLM) Deliverables

² The uptime rate refers to specific application outages—not external/network issues. Additionally, uptime rate will not include outages for scheduled maintenance and enhancements.

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

The Contractor shall provide SLM deliverables as required for System Maintenance Services projects. All appropriate documentation shall be prepared in accordance with the guidelines specified by the SLM and the approved Project Tailoring Plan.

7.2 Quarterly Progress Report

The Contractor shall prepare a quarterly progress report to be briefed quarterly at the Unit Chief level and twice per year to the Executive Steering Committee. The initial report is due forty-five calendar days after start of the task and shall cover the first calendar month of performance. Subsequent reports shall be provided quarterly within five calendar days of the end of each quarter until the last quarter of performance. The final delivery shall occur ten days before the end of the final option period and shall summarize performance during the period of performance and provide the status of any planned transition activity. The quarterly reports can be delivered via email and shall contain the following:

- Description of work accomplished (Accomplishments)
- Work planned for the following month (Planned Activities)
- Deviations from planned activities
- Open risks and issues

7.3 Certification and Accreditation (C&A) Documentation

The Contractor shall be responsible for maintaining and updating existing C&A artifacts to stay current with DHS/ICE and Federal requirements. These C&A updates will be required every three years unless a major change impacts security. The Contractor shall also be responsible for supporting the Information Systems Security Officer (ISSO) for any annual C&A activities, which may be requested (i.e. self-assessments, contingency plan tests, vulnerability scans, etc.).

7.4 Quality Assurance Surveillance Plan

The Quality Assurance Surveillance Plan (QASP) is the document used by the Government to evaluate Contractor actions while implementing the PWS. It is designed to provide an effective surveillance method of monitoring Contractor performance for each listed task in the PWS.

The QASP provides a systematic method to evaluate the services the Contractor is required to furnish. The Contractor, and not the Government, is responsible for management and quality control actions to meet the terms of this task order. The role of the Government is quality assurance monitoring to ensure that the task order standards are achieved.

The Contractor shall be required to develop a comprehensive program of inspections and monitoring actions. Once the quality control program is approved by the Government, careful application of the process and standards presented in the QASP document will ensure a robust quality assurance program. The QASP below was developed by ICE and is indicative of the type of metrics that apply to the deliverables. The offeror may propose other metrics they determine upon the uniqueness and relevance of their own technical approach in meeting the task order objectives. The QASP is subject to discussions/negotiations.

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

FALCON Operations and Maintenance (O&M) Support Services Contract Quality Assurance Surveillance Plan (QASP)
Attachment 1

Tasks	Metrics	Service Level Agreement	How it will be measured	Exceptional Rating	Very Good Rating	Satisfactory Rating	Marginal Rating	Unsatisfactory Rating
Tier 1 – Help Desk Support	Response Time for incoming emails	The end of the current day	Time the email is received in the Help Desk Inbox until time the request is accessed for action.	Meets SLA 98-100% of instances	Meets SLA 95-97.9% of instances	Meets SLA 90-94.9% of instances	Meets SLA 85-89.9% of instances	Meets SLA less than 85% of instances
Tier 2 Software Support	Response time for Tier 2	The end of the current day	Time the ticket is assigned to Tier 2 until the time the ticket is accessed for action.	Meets SLA 98-100% of instances	Meets SLA 95-97.9% of instances	Meets SLA 90-94.9% of instances	Meets SLA 85-89.9% of instances	Meets SLA less than 85% of instances
Tier 3 Software Support	Response time for Tier 3 tickets not involving system outage or denial of service to substantial numbers of users	No more than 4 hours	Time the ticket is assigned to Tier 3 until the time the ticket is accessed for action.	Meets SLA 98-100% of instances	Meets SLA 95-97.9% of instances	Meets SLA 90-94.9% of instances	Meets SLA 85-89.9% of instances	Meets SLA less than 85% of instances

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Tasks	Metrics	Service Level Agreement	How it will be measured	Exceptional Rating	Very Good Rating	Satisfactory Rating	Marginal Rating	Unsatisfactory Rating
Tier 2 and Tier 3 Software Support	Average resolution time of Tier 2 and Tier 3 tickets	8 business days	Time the ticket is placed in the Tier 2 or Tier 3 queue for action to the time it appears as closed or referred, system, divided by the total number of tickets.	Average of 5 or fewer business days	Average of 6 to 7 business days	Meets SLA of average of 8 business days	Average of 9 to 12 business days	Average of more than 12 business days
Tier 3 Software Support	Response time for Emergency tickets, during business hours or after hours, involving system outage or denial of service to substantial numbers of users	No more than 30 minutes	Time the FALCON PM or designate is informed of situation.	Meets SLA 98-100% of instances	Meets SLA 95-97.9% of instances	Meets SLA 90-94.9% of instances	Meets SLA 85-89.9% of instances	Meets SLA less than 85% of instances

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Tasks	Metrics	Service Level Agreement	How it will be measured	Exceptional Rating	Very Good Rating	Satisfactory Rating	Marginal Rating	Unsatisfactory Rating
Tier 3 Software Support	Average resolution time for Emergency tickets, during business hours or after hours, involving system outage or denial of service to substantial numbers of users	No more than 8 hours	Time the ticket is assigned as an Emergency until the time the ticket is closed.	Average is less than 6.5 hours	Average is 6.5 to 7.49 hours	Average is 7.5 to 8.49 hours	Average is 8.5 to 9.49 hours	Average is 9.5 hours or longer
Operational Support	Uptime Rate ³ - Percentage of time that the application is available to users in fully-functioning mode	98% or higher	Cumulative uptime per month divided by the total time per month that FALCON is scheduled as available.	99.5-100% available	98.5-99.49% available	97.5-98.49% available	96.5-97.49% available	Less than 96.5% available

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Tasks	Metrics	Service Level Agreement	How it will be measured	Exceptional Rating	Very Good Rating	Satisfactory Rating	Marginal Rating	Unsatisfactory Rating
Configuration Management	All changes will be tracked	100%	No changes will be made to the baseline without an associated SCR.	100%	98-99.9%	96-97.9%	94-95.9%	Less than 94%
Workspace Quick Search	Average time for users to receive results from a search conducted in FALCON	1 second	Contractor's statistics from prior quarter	Less than 0.85 seconds	0.85-0.95 seconds	.095-1.05 seconds	1.05-1.15 seconds	More than 1.15 seconds
Workspace Document Load	Average time for users to receive results from a FALCON Quick Search in Workspace	0.5 seconds	Contractor's statistics from prior quarter	Less than 0.35 seconds	0.35-0.45 seconds	0.45-0.55 seconds	0.55-0.65 seconds	More than 0.65 seconds
DARTTS Search	Average time for server to return results from a search conducted in FALCON-DARTTS	0.35 seconds	Contractor's statistics from prior quarter	Less than 0.2 seconds	0.2-0.3 seconds	0.3-0.4 seconds	0.4-0.5 seconds	More than 0.5 seconds
Training	Training and Training Material Delivery	100% on time	Delivery date versus scheduled delivery date.	99-100% of instances on time	95-98.9% of instances on time	90-94.9% of instances on time	85-89.9% of instances on time	Less than 85% of instances on time

FALCON Operations & Maintenance Support & System Enhancement*Performance Work Statement*

Tasks	Metrics	Service Level Agreement	How it will be measured	Exceptional Rating	Very Good Rating	Satisfactory Rating	Marginal Rating	Unsatisfactory Rating
ICE Employee Satisfaction with Training	Rating on Feedback Form Received from Trained ICE Employees Following Training (Ratings of Very Satisfied, Satisfied, Partially Satisfied, or Not Satisfied)	90% or more of respondents report being Satisfied or Very Satisfied	Feedback forms turned in from ICE employees who received classroom or desk-side training	98% or more of respondents report being Satisfied or Very Satisfied	93-97.9% of respondents report being Satisfied or Very Satisfied	88-92.9% of respondents report being Satisfied or Very Satisfied	83-87.9% of respondents report being Satisfied or Very Satisfied	Less than 83% of respondents report being Satisfied or Very Satisfied

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

- Measurements will be performed quarterly.
- Measurements will be carried out by Contractor.
- QASP measurement report will be turned in quarterly to the government Contracting Officer's Representative (COR) within fifteen calendar days after the end of the quarter under review.
- An overall quarterly QASP Rating will be computed for the Contractor by the COR, according to the following methodology:
 - For each of the QASP Tasks listed above, the Contractor will be assigned the following number of points:
 - Exceptional: 4 points
 - Very Good: 3.5 points
 - Satisfactory: 2.75 points
 - Marginal: 1.75 points
 - Unsatisfactory: 0 points
 - The points for the 10 QASP Tasks will be averaged (the sum total divided by 10). The overall quarterly QASP Rating will be assigned as follows (CPARS is the Contractor Performance Assessment Reporting System):

QASP Rating	Point Level	Consequence
Exceptional	3.7 – 4.0	Exceptional rating for quarter entered into CPARS at end of performance period
Very Good	3.2 – 3.69	Very Good rating for quarter entered into CPARS at end of performance period
Satisfactory	2.7 – 3.19	Satisfactory rating for quarter entered into CPARS at end of performance period
Marginal	1.7 – 2.69	Marginal rating for quarter entered into CPARS at end of performance period.
Unsatisfactory	< 1.7	Unsatisfactory rating for quarter entered into CPARS at end of performance period.

7.5 Deliverables Table

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

The Contractor shall provide the following deliverables via email to the COR, unless noted otherwise:

<u>Deliverable</u>	<u>Frequency</u>	<u>Recipients</u>
SLM Deliverables (Doc) & Software (SW) (Software includes updates/new versions of the primary Gotham platform; new workflow applications and updated versions of existing workflow applications; data ingestions; and customized versions of Gotham Mobile and the Phoenix and Raptor plug-ins)	As Required	Electronic copy - PM Software (SW): ICE source control repository (Subversion); OCIO representative on FALCON PMO (either Chris Oslin or alternative OCIO representative)
Schedule of Outcomes (annual)	10 working days after beginning of contract year	Electronic copy - PM, Contracting Officer, COR/ACOR
Project Plan for first of five annual outcome-based projects	10 working days after beginning of contract year	Electronic copy - PM, Contracting Officer, COR/ACOR
Project Plans for subsequent annual outcome-based projects	10 working days prior to the initiation of work according to Schedule of Outcomes	Electronic copy - PM, Contracting Officer, COR/ACOR
Project Schedule for first of five annual outcome-based projects	10 working days after beginning of contract year	Electronic copy - PM, Contracting Officer, COR/ACOR
Project Schedules for subsequent annual outcome-based projects	10 working days prior to the initiation of work according to Schedule of Outcomes	Electronic copy - PM, Contracting Officer, COR/ACOR
Quarterly Progress Report	Quarterly, within 15 calendar days of the end of the quarter being reviewed	Electronic copy: PM, Contracting Officer, COR/ACOR

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Certification and Accreditation Documentation	As Required	Electronic copy: PM, COR/ACOR
Transition In Plan- Final	15 calendar days after award	Electronic copy: PM, Contracting Officer, COR/ACOR
Transition Out Plan	120 calendar days before the end of the POP	Electronic copy: PM, Contracting Officer, COR/ACOR
QASP- Final	15 calendar days after award	Electronic copy: PM, Contracting Officer, COR/ACOR

7.6 Delivery Instructions

The Contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment. The electronic copies shall be compatible with MS Office 2010 or other applications as appropriate and mutually agreed to by the parties. The documents shall be considered final upon receiving Government approval. All deliverables shall be delivered electronically (unless a hardcopy is requested) to the COR. If a hardcopy is requested, it will be delivered to the designated COR, not later than 4:00 PM ET on the deliverable's due date. Once created, deliverables and work products are considered the property of the Federal Government. Any work that deviates from this task order and the approved deliverables listed herein shall not be accepted without prior approval from the COR.

7.7 Draft Deliverables

The Government will provide written acceptance, comments and/or change requests, if any, within 15 working days from receipt by the Government of each draft deliverable. Upon receipt of the Government comments, the Contractor shall have 15 working days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

7.8 Written Acceptance/Rejection by the Government

The Government shall provide written notification of acceptance or rejection of all final deliverables within fifteen (15) calendar days. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

Items must be approved by the COR and/or the appropriate Government authority to be considered "accepted." The Government will provide written acceptance, comments, or change requests within fifteen (15) calendar days from receipt by the Government, of all required deliverables.

7.9 Non-Conforming Products or Services

28

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Non-conforming products or services will be rejected. The Government will provide written notification of non-conforming products or services within fifteen (15) calendar days. Deficiencies shall be corrected within 30 days of the rejection notice. If the deficiencies cannot be corrected within 30 calendar days, the Contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten (10) calendar days.

7.10 Notice Regarding Late Delivery

The Contractor shall notify the COR as soon as it becomes apparent to the Contractor that a scheduled delivery will be late. The Contractor shall include in the notification the rationale for late delivery, the expected date for the delivery, and the impact of the late delivery on the project. The COR will review the new schedule with the PM and provide guidance to the Contractor.

8.0 CONSTRAINTS

8.1 General Constraints

The following project constraints are applicable to the FALCON System Maintenance and Services task order:

(b)(7)(E)

8.2 DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- 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 and 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 Enterprise Architecture (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 U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special 8 ITAR Quick Essentials Guide 2011 v2.0 Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

8.3 Maintenance of Existing FALCON System Functionality

Contractor shall ensure that all new work performed under this contract will adhere to the following stipulations.

8.3.1 Continuation of Existing FALCON System Functionality

New work performed under this contract shall not adversely affect the ease of operation of the following existing FALCON Search and Analysis system features, which shall retain their existing “look and feel” unless changes are mutually agreed to:

Data Integration

(b)(7)(E)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

Search & Discovery

(b)(7)(E)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

Advanced Analytics

(b)(6);(b)(7)(C)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

-
-
-
-
-
-
-
-

Ease of Use

(b)(7)(E)

Knowledge Management

(b)(7)(E)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

Security & Access Controls

(b)(7)(E)

Enterprise-Wide Collaboration

(b)(7)(E)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

Workflow Management

A workflow application for tracking tickets.

- A ticketing application for workflow management to track and assign cases and gather information, tips, and research into case folders
- Information can be shared with other case management systems via configurable importers and exporters
- Tickets—a case, work item, or tip—can be circulated to different individuals for investigation and research until the ticket reaches resolution and can be closed
- Configurable ticket forms that can be updated to meet new requirements, which generate error messages when tickets are incorrectly completed
- A “Tip Line” for entering and recording tips as tickets: tips can be entered directly and become part of the broader repository for complete system of record tracking
- Tip Line tickets include a notes field for attaching narrative information; ability to link the tickets to other objects in the repository; and attachments for media objects such as images or video

Mobile Application

(b)(7)(E)

Flexibility, Extensibility, and Scalability

An open and extensible back-end architecture for a configurable data environment and scalability.

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

•

•

•

•

•

•

•

•

8.3.2 Compatibility of New Work with Existing FALCON Features and Data Sets

(b)(7)(E)

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

8.4 Level of Service

Contractor shall ensure that the FALCON system shall be able to accommodate the following minimum levels of service, with no diminishment of performance levels from performance levels met by the system prior to the initiation of this contract. The following levels of service will apply (the speed of the ramping up of service levels from existing levels to the levels listed below will be contingent upon the installation of additional hardware and software):

Individual Data Records Accessible by FALCON:	as many as are required based on outcomes prioritized by HSI
FALCON-SA User Base:	HSI Enterprise-wide (currently 10,000)
FALCON-SA Concurrent Users:	Based upon growth of usage
FALCON Web Access User Base:	HSI Enterprise-wide (currently 10,000)
FALCON Web Access Concurrent Users:	Based upon growth of usage
FALCON Mobile User Base:	All HSI SA's (by March 13, 2016)
FALCON Mobile Concurrent Users:	Based upon growth of usage

9.0 GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION

The Contractor shall keep an inventory of Government-furnished equipment (GFE), which shall be made available to the COR, Assistant COR, and Government Call Monitor upon request. The Government will provide basic equipment (e.g., laptops, desktops, VPN tokens, and aircards) in accordance with the contract. All GFE shall be entered into ICE's Property Inventory System (Sunflower) within 48 hours of receipt. The Contractor shall provide their own network connectivity capability with a minimum connection speed of 10Mbps.

Items of GFE which are inventoried and tracked in Sunflower include the following seventeen

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

laptops and four i-Phone handheld devices:

Model Number	Serial Number	Laptop/VPN/i-Phone
(b)(7)(E)		

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

(b)(7)(E)

9.1 Remote Access

Contractor shall be provided with remote access to the DHS network for mutual convenience while the contractor performs business for the DHS Component.

10.0 OTHER DIRECT COSTS (ODCs)

Travel outside the local metropolitan Washington, DC area may be expected during performance of the resulting task order. Therefore, travel will be undertaken following the General Services Administration Field Travel Regulation. Reimbursement for allowable costs will be made. Any travel and training expenditures shall be pre-approved by the COR. Costs for transportation, lodging, meals and incidental expenses incurred by Contractor personnel on official company business are allowable subject to FAR 31.205-46, Travel Costs. These costs will be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the Federal Travel Regulations. The Contractor will not be reimbursed for travel and per diem within a 50-mile radius of the worksite where a Contractor has an office. Local travel expenses within the

FALCON Operations & Maintenance Support & System Enhancement

Performance Work Statement

Washington Metropolitan area will not be reimbursed (this includes parking). All travel outside the Washington Metropolitan area must be approved by the COR in advance. No travel will be reimbursed without prior approval from the COR.

11.0 PLACE OF PERFORMANCE

Work, meetings, and briefings will be performed primarily at Contractor facilities. Frequent travel to ICE offices located at 801 I Street NW, Washington, D.C., or 500 12th St SW, Washington, D.C., or to the Tech Ops facility in Lorton, VA will be required. Additionally, travel to the Law Enforcement Support Center (LESC) facility located in Williston, VT may be required. Due to regular interaction with a multitude of program stakeholders, the Contractor's staff shall be located in the Greater Washington Area (GWA).

12.0 PERIOD OF PERFORMANCE

The period of performance of the FALCON System Maintenance and Services contract will consist of a base period of twelve (12) months plus two (2) twelve (12) month option periods. A FAR 52.217-8 6-month optional extension allows for an additional six months' worth of Operations and Maintenance Support Services to be purchased after the end of Option Year 2.

13.0 SECURITY

Contractor personnel performing work under this PWS will not be dealing with classified information, but will be Sensitive but Unclassified (SBU) data. If it is determined that a higher security classification is necessary, based on a change to the scope of work of this PWS, required documentation from the contractor will be requested by the contracting officer prior to any modification adding classified work to this task order.

13.1 Section 508 Compliance

The DHS Office of Accessible Systems and Technology has determined that for the purposes of compliance with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, a National Security Exception applies. ICE received a National Security Exemption (**ICE-20120201-001**) on 2/01/2012.

13.2 General Clause

To ensure the security of the DHS/ICE information in their charge, ICE Contractors and Sub-contractors shall adhere to the same computer security rules and regulations as Federal Government employees unless an exception to policy is agreed to by the prime Contractors, ICE Information Systems Security Manager (ISSM) and Contracting Officer and detailed in the contract. Non-DHS Federal employees or Contractors who fail to comply with DHS/ICE security policies are subject to having their access to DHS/ICE IT systems and facilities terminated,

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

whether or not the failure results in criminal prosecution. The DHS Rules of Behavior document applies to DHS/ICE support Contractors and Sub-contractors.

13.3 Security Policy References Clause

The following primary DHS/ICE IT Security documents are applicable to Contractor/Sub-contractor operations supporting Sensitive But Unclassified (SBU) based contracts. Additionally, ICE and its Contractors shall conform to other DHS Management Directives (MD) (Note: these additional MD documents appear on DHS-Online in the Management Directives Section. Volume 11000 “Security and Volume 4000 “IT Systems” are of particular importance in the support of computer security practices):

- ☐ DHS 4300A, Sensitive Systems Policy Directive
- ☐ DHS 4300A, IT Security Sensitive Systems Handbook
- ☐ ICE Directive, IT Security Policy for SBU Systems

13.3.1 Contractor Information Systems Security Officer (ISSO) Point of Contact Clause

The Contractor shall appoint and submit a name to ICE ISSM for approval, via the ICE COR, of a qualified individual to act as ISSO to interact with ICE personnel on any IT security matters.

13.3.2 Protection of Sensitive Information

The Contractor shall protect all DHS/ICE “sensitive information” to which the Contractor is granted physical or electronic access by adhering to the specific IT security requirements of this contract and the DHS/ICE security policies specified in the Reference Section above. The Contractor shall ensure that their systems containing DHS/ICE information and data be protected from unauthorized access, modification and denial of service. Further, the data shall be protected in order to ensure the privacy of individual’s personal information.

13.3.3 Information Technology Security Program

If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall establish and maintain an IT Security Program. This program shall be consistent with the referenced DHS/ICE IT security policy documents and at a minimum contain and address the following elements:

- Handling of DHS/ICE sensitive information and IT resources to include media protection, access control, auditing, network security, and rules of behavior
- Certification and Accreditation (C&A) and FISMA compliance of Systems containing, processing or transmitting of DHS/ICE data
- Training and Awareness for Contractor personnel
- Security Incident Reporting
- Contingency Planning
- Security Reviews
- Contract Closeout Actions

13.3.4 Handling of Sensitive Information and IT Resources

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

The Contractor shall protect DHS/ICE sensitive information and all government provided and Contractor-owned IT systems used to store or process DHS/ICE sensitive information. The Contractor shall adhere to the following requirements for handling sensitive information:

- **Media Protection.** The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive information stored on media to be surplus, transferred to another individual, or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using DHS/ICE approved sanitization methods. The Contractor shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen. These procedures shall address the handling and protection of paper and electronic outputs from systems (computers, printers, faxes, copiers) and the transportation and mailing of sensitive media.)
- **Access Control.** The Contractor shall control user access to DHS/ICE sensitive information based on positive user identification, authentication, and authorization (Roles and Rules based) mechanisms. Access control measures employed shall provide protection from unauthorized alternation, loss, unavailability, or disclosure of information. The Contractor shall ensure its personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. The Contractor shall divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process.
- **Auditing.** The Contractor shall ensure that its Contractor-owned IT systems used to store or process DHS/ICE sensitive information maintain an audit trail sufficient to reconstruct security relevant events. Audit trails shall include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. The Contractor shall periodically review audit logs and ensure that audit trails are protected from modification, authorized access, or destruction and are retained and regularly backed up.
- **Network Security.** The Contractor shall monitor its networks for security events and employ intrusion detection systems capable of detecting inappropriate, incorrect, or malicious activity. Any interconnections between Contractor-owned IT systems that process or store DHS/ICE sensitive information and IT systems not controlled by DHS/ICE shall be established through controlled interfaces and documented through formal Interconnection Security Agreements (ISA). The Contractor shall employ boundary protection devices to enforce access control between networks, including Internet and extranet access. The Contractor shall ensure its e-mail systems are secure, properly configured, and that network protection mechanisms implemented in accordance with DHS/ICE requirements. The Contractor shall conduct periodic vulnerability assessments and tests on its IT systems containing DHS/ICE sensitive information to identify security vulnerabilities. The results, of this information, will be provided to the ICE OCIO for review and to coordinate remediation plans and actions.
- DHS employees and Contractors shall not transmit sensitive DHS/ICE information to any personal e-mail account that is not authorized to receive it.
- **Rules of Behavior.** The Contractor shall develop and enforce Rules of Behavior for

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Contractor-owned IT systems that process or store DHS/ICE sensitive information. These Rules of Behavior shall meet or exceed the DHS/ICE rules of behavior.

- The Contractor shall adhere to the policy and guidance contained in the DHS/ICE reference documents.

13.3.5 Training and Awareness

The Contractor shall ensure that all Contractor personnel (including Sub-contractor personnel) who are involved in the management, use, or operation of any IT systems that handle DHS/ICE sensitive information, receive annual training in security awareness, accepted security practices, and system rules of behavior. If the Contractor does not use the ICE-provided annual awareness training, then they shall submit to the ICE ISSM their awareness training for approval. Should Contractor Training be approved for use, the Contractor shall provide proof of training completed to the ICE ISSM when requested.

The Contractor shall ensure that all Contractor personnel, including Sub-contractor personnel, with IT security responsibilities, receive specialized DHS/ICE annual training tailored to their specific security responsibilities. If the Contractor does not use the ICE-provided special training, then they shall submit to the ICE ISSM their awareness training for approval. Should Contractor training be approved for use, the Contractor shall provide proof of training completed to the ICE ISSM when requested.

Any Contractor personnel who are appointed as ISSO, Assistant ISSOs, or other position with IT security responsibilities, i.e., System/LAN Database administrators, system analyst and programmers may be required to attend and participate in the annual DHS Security Conference.

13.3.6 Certification and Accreditation (C&A) and FISMA compliance

The Contractor shall ensure that any Contractor-owned systems that process, store, transmit or access DHS/ICE information shall comply with the DHS/ICE C&A and FISMA requirements.

Any work on developing, maintaining or modifying DHS/ICE systems shall be done to ensure that DHS/ICE systems are in compliance with the C&A and FISMA requirements. The Contractor shall ensure that the necessary C&A and FISMA compliance requirements are being effectively met prior to the System or application's release into Production (this also includes pilots). The Contractor shall use the DHS provided tools for C&A and FISMA compliance and reporting requirements.

13.3.7 Security Incident Reporting

The Contractor shall establish and maintain a computer incident response capability that reports all incidents to the ICE Computer Security Incident Response Center (CSIRC) in accordance with the guidance and procedures contained in the referenced documents.

13.3.8 Contingency Planning

If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

owned information systems, the Contractor shall develop and maintain contingency plans to be implemented in the event normal operations are disrupted. All Contractor personnel involved with contingency planning efforts shall be identified and trained in the procedures and logistics needed to implement these plans. The Contractor shall conduct periodic tests to evaluate the effectiveness of these contingency plans. The plans shall at a minimum address emergency response, backup operations, and post-disaster recovery.

13.3.9 Security Review and Reporting

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.

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/ICE, including the Office of Inspector General, ICE ISSM, and other government oversight organizations, access to the Contractor's and Sub-contractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/ICE data or the function of computer systems operated on behalf of DHS/ICE, and to preserve evidence of computer crime.

13.3.10 Use of Government Equipment

Contractors are not authorized to use Government office equipment (IT systems/computers) for personal use under any circumstances, unless limited personal use is specifically permitted by the contract. When so authorized, Contractors shall be governed by the limited personal use policies in the referenced documents.

13.3.11 Contract Closeout

At the expiration of this contract, the Contractor shall return all sensitive DHS/ICE information and IT resources provided during the life of this contract. The Contractor shall certify that all DHS/ICE information has been purged from any Contractor-owned system used to store or process DHS/ICE information. Electronic media shall be sanitized (overwritten or degaussed) in accordance with the sanitation guidance and procedures contained in reference documents and with DHS/NIST/National Security Agency (NSA) approved hardware and software. Note that these procedures may be waived by the COR, contingent upon approval of a follow-on contract with the current Contractor.

13.3.12 Personnel Security

DHS/ICE does not permit the use of non U.S. Citizens in the performance of this contract or to access DHS/ICE systems or information.

All Contractor personnel (including Sub-contractor personnel) shall have favorably adjudicated

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/ICE sensitive information.

The Contractor shall ensure all Contractor personnel are properly submitted for appropriate clearances.

The Contractor shall ensure appropriate controls have been implemented to prevent Contractor personnel from obtaining access to DHS/ICE sensitive information before a favorably adjudicated background investigation has been completed and appropriate clearances have been issued. At the option of the Government, interim access may be granted pending completion of a pre-employment check. Final access may be granted only upon favorable completion of an appropriate background investigation based on the risk level assigned to this contract by the Contracting Officer.

The Contractor shall ensure its personnel have a validated need to access DHS/ICE sensitive information and are granted the most restrictive set of access privileges needed for performance of authorized tasks.

The Contractor shall ensure that its personnel comply with applicable Rules of Behavior for all DHS/ICE and Contractor-owned IT systems to which its personnel have been granted access privileges.

The Contractor shall implement procedures to ensure that system access privileges are revoked for Contractor personnel whose employment is terminated or who are reassigned to other duties and no longer require access to DHS/ICE sensitive information.

The Contractor shall conduct exit interviews to ensure that Contractor personnel who no longer require access to DHS/ICE sensitive information understand their obligation not to discuss or disclose DHS/ICE sensitive information to which they were granted access under this contract.

13.3.13 Physical Security

The Contractor shall ensure that access to Contractor buildings, rooms, work areas and spaces, and structures that house DHS/ICE sensitive information or IT systems through which DHS/ICE sensitive information can be accessed, is limited to authorized personnel. The Contractor shall ensure that controls are implemented to deter, detect, monitor, restrict, and regulate access to controlled areas at all times. Controls shall be sufficient to safeguard IT assets and DHS/ICE sensitive information against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. Physical security controls shall be implemented in accordance with the policy and guidance contained in the referenced documents.

13.4 ISO Terms and Conditions for Sensitive but Unclassified Requests

13.4.1 DHS Security Policy Requirement

The following terms and conditions should be included in all acquisition documents.
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.

13.4.1.1 Encryption Compliance Requirement

The following terms and conditions should be included in all acquisition documents.

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).

13.4.1.2 Security Review Requirement

The following requirements should be included in all acquisition documents.

13.4.1.2.1 Security Review

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

13.4.1.3 Interconnection Security Agreement (ISA)

The following requirements should be included in the acquisition document if the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity.

13.4.1.3.1 Interconnection Security Agreement Requirements

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

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

The following requirements should be included in acquisition documents for information systems

FALCON Operations & Maintenance Support & System Enhancement

Performance Work Statement

which are hosted, operated, maintained, and used on behalf of DHS at non-DHS facilities. Contractors are fully responsible and accountable for ensuring compliance with all Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) and related DHS security control requirements (to include configuration guides, hardening guidance, DHS Security Policy, Procedures, and Architectural guidance). The contractor security procedures shall be the same or greater than those that are provided by DHS Enterprise Data Center(s). Please note that all of the subsections from **Security Authorization** to **Log Retention** are included in this requirement.

13.4.3 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 COTR 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 requirements. 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.

13.4.4 Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture in accordance with applicable laws and DHS policies to the satisfaction of the DHS COTR. Areas of consideration could include:

1. Use of multi-tier design (separating web, application and data base) with policy

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

- 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

13.4.5 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

13.4.6 Specific Protections

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

13.4.6.1 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.

13.4.6.2 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

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

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.

13.4.6.3 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 COTR 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.

13.4.6.4 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 COTR 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.

13.4.6.5 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.

13.4.6.6 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.

13.4.6.7 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 COTR 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.

13.4.6.8 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.

13.4.6.9 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.

13.4.6.10 Supply Chain Risk Management Requirement

Supply Chain risks result from adversarial exploitation of the organizations, people, activities, information, resources, or facilities that provide hardware, software, or services. These risks can result in a loss of confidentiality, integrity, or availability of information or information systems. A compromise to even minor system components can lead to adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorities:

Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management

Department of Homeland Security, Security Policy for Sensitive Systems 4300A

Homeland Security Presidential Directive 23, Cyber Security and Monitoring, 8 January 2008

Office of Budget and Management Circulation A-130, Appendix III

•National Institute of Standards and Technology, Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

13.4.6.10.1 Supply Chain Risk Management

The following requirements should be included in all hardware and software requests to ensure the confidentiality, integrity, and availability of government information.

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

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

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.

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

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.

13.4.6.11 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"

13.4.6.11.1 Personal Identification Verification (PIV) Credential Compliance Requirement

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.

13.4.7 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006) (3052.204-70 Security

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

requirements for unclassified information technology resources.)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within ["insert number of days"] days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.
(End of clause)

13.4.8 CONTRACTOR EMPLOYEE ACCESS (SEP 2012) (3052.204-71 Contractor employee access.)

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

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

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

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.

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

and

(2) 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.

14.4 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

14.4.1 General

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in Contract_HSCTE-13-F-00010 requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

14.4.2 Fitness Determination

ICE will exercise full control over granting; denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. ICE may, as it deems appropriate, authorize and make a favorable expedited pre-employment determination based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment determination or a full employment determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment determination or full employment determination by the OPR-PSU. Contract employees are processed under the DHS Management Directive 6-8.0. The contractor shall comply with the pre-screening requirements specified in the DHS Special Security Requirement – Contractor Pre-Screening paragraph located in this contract, if HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology (IT) Resources; and/or 3052.204-71, Contractor Employee Access are included in the Clause section of this contract.

14.4.3 Background Investigations

56

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Prospective Contractor employees shall submit the following completed forms to the Personnel Security Unit through the Contracting Offices Representative (COR), no less than 35 days before the starting date of the contract or 5 days prior to the expected entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P (SF 85P) "Questionnaire for Public Trust Positions" Form shall be submitted via e-QIP (electronic Questionnaires for Investigation Processing) (Original and One Copy)
2. Three signed eQip Signature forms: Signature Page, Release of Information and Release of Medical Information (Originals and One Copy)
3. Two FD 258, "Fingerprint Card"
4. Foreign National Relatives or Associates Statement (Original and One Copy)
5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (Original and One Copy)
6. Optional Form 306 Declaration for Federal Employment (applies to contractors as well) (Original and One Copy)

Prospective Contractor employees who currently have an adequate current investigation and security clearance issued by the Defense Industrial Security Clearance Office (DISCO) or by another Federal Agency may not be required to submit complete security packages, and the investigation will be accepted for adjudication under reciprocity.

An adequate and current investigation is one where the investigation is not more than five years old and the subject has not had a break in service of more than two years.

Required forms will be provided by ICE at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

14.4.4 Transfers From Other DHS Contracts

Personnel may transfer from other DHS Contracts provided they have an adequate and current investigation (see above). If the prospective employee does not have an adequate and current investigation, an eQip Worksheet shall be submitted to the Intake Team to initiate a new investigation.

Transfers will be submitted on the COR Transfer Form, which will be provided by the Dallas PSU Office along with other forms and instructions.

14.4.5 Continued Eligibility

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

The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU may require reinvestigations when derogatory information is received and/or every 5 years.

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

14.4.6 Required Reports

The Contractor shall notify OPR-PSU of all terminations/ resignations within five days of occurrence. The Contractor shall return any expired ICE issued identification cards and building passes, or those of terminated employees to the COR. If an identification card or building pass is

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

not available to be returned, a report must be submitted to the COR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor shall provide, through the COR, a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation) . The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

Submit reports to the email address (b)(7)(E)

14.4.7 Employment Eligibility

The contractor shall agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represents the best means available for employers to verify the work authorization of their employees.

The Contractor shall agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

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

14.4.8 Security Management

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

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

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

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (INS). These entities are hereafter referred to as the Department.

14.4.9 Information Technology Security Clearance

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS IT Security Program Publication DHS MD 4300.Pub. or its replacement*. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

14.4.10 Information Technology Security Training and Oversight

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

Contractors involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department 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 Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

14.4.11 Non-Disclosure Agreement

Contractors are required to sign DHS 11000-6, Attachment 9 - Non-Disclosure Agreement, due to access to a sensitive ICE system. Non-Disclosure Agreements shall be provided to the COR and CO prior to the commencement of work on this task order.

15.0 LIST OF ACRONYMS

The list of acronyms in connection to this PWS is attached as Appendix A.

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

PWS Appendix A: List of Acronyms

AHS	Application Hosting Services
ADIS	Arrival and Departure Information System
AIDW	Automated Information Data Warehouse
AJAX	Asynchronous Java and XML
API	Application Programming Interface
ATS	Automated Targeting System
C&A	Certification and Accreditation
CCB	Change Control Board
CCDI	Consular Consolidated Database
CFR	Code of Federal Regulation
CLAIMS	Computer Linked Application Information Management System
CO	Contracting Officer
COB	Close of Business
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative (same as COR)
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CPU	Central Processing Units
CSIRC	Computer Security Incident Response Center
CSRC	Computer Security Resource Center
DARTTS	Data Analysis and Research for Trade Transparency System
DC	District of Columbia
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DISCO	Defense Industrial Security Clearance Office
DoJ	Department of Justice
E3	Next Generation of ENFORCE
EA	Enterprise Architecture
EADM	Enforcement Alien Detention Module
EARM	Enforcement Alien Removal Module
EID	Enforcement Integrated Database
EIT	Electronic and Information Technology
EIU	Executive Information Unit

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

ELMS	Electronic Library Management System
ENFORCE	Enforcement Case Tracking System
EOD	Entry on Duty
ETL	Extract, Transfer and Load
E-VERIFY	Eligibility Verification
FAR	Federal Acquisition Regulations
FINS	Former Immigration Naturalization Service
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FITSAF	Federal Information Technology Security Assessment Framework
FRD	Functional Requirements Document
FTR	Federal Travel Regulations
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GNR	Global Name Recognition
GOTS	Government Off-The-Shelf
GWA	Greater Washington, DC Area
HSI	Homeland Security Investigations
HSTC	Human Smuggling and Trafficking Center
I2MS	Investigative Information Management System
IBM	International Business Machines
ICE	Immigration and Customs Enforcement
ICEPIC	ICE Pattern Analysis Information Collection Tool
ICE/SAC	ICE Special Agent in Charge
ICM	Investigative Case Management (New TECS)
ID	Identification Card
IPT	Integrated Project Team
IRRIS	Investigation Records Review for Information Sharing
ISA	Interconnection Security Agreements
ISB	Investigative Systems Branch
ISC2	International Info Systems Security Certification Consortium
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITCR	Information Technology Change Request

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

KITE	Palantir Data Ingestion
LECAD	Law Enforcement Centralized Access Development
LEISS	Law Enforcement Information Sharing System
LESC	Law Enforcement Support Center
LPR	Lawful Permanent Residents
MCC	Mobile Command Center
MD	Management Directive
MS	Microsoft
NCIC	National Crime Information Center
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSEERs	National Security Entry and Exit Registration System
O&M	Operations and Maintenance
OAST	Office on Accessible Systems and Technology
OCIO	Office of the Chief Information Officer
OCONUS	Outside of the Continental United States
ODC	Other Direct Cost
OI	Office of Investigations
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OPR	Office of Professional Responsibility
PCN	Potomac Center North
PCTS	Parole Case Tracking System
PHOENIX	Palantir Big Data Platform
PM	Program Manager
PMO	Program Management Office
PMP	Project Management Professional
POP	Period of Performance
PSU	Personnel Security Unit
QAP	Quality Assurance Plan
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Plan
RAPTOR	Palantir Data Index Tool
RELRES	Relationship Resolution
RFD	Request for Deviation

FALCON Operations & Maintenance Support & System Enhancement
Performance Work Statement

ROI	Records of Investigation
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCR	System Change Request
SDA	System Design Alternative
SDD	Systems Development Division
SEACATS	Seized Asset and Case Tracking System
SELC	System Enterprise Lifecycle
SEN	Significant Event Notification
SEVIS	Student Exchange Visitor Information System
SLA	Service Level Agreement
SLM	System Lifecycle Management
SOP	Standard Operating Procedure
SOW	Statement of Work
SRD	System Requirements Document
SW	Software
TAIS	Telecommunications and Automated Information Systems
TLS	Telephone Linking System
TMP	Transition Management Plan
TO	Task Order
TRM	Technical Reference Model
TS	Top Secret
TTU	Trade Transparency Unit
UAT	User Acceptance Testing
USCIS	United States Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VPN	Virtual Private Network

To: (b)(6);(b)(7)(C) Contracting Officer

Office of Acquisition Management

From: (b)(6);(b)(7)(C) COR, Palantir FALCON O&M Contract

IS&IM, Investigative Systems

Date: 9/27/2016

**RE: Request to Modify HSCETC-15-C-00001 Utilizing FY 2016 TEOF
Funding**

(b)(7)(E)

(b)(7)(E)

Language to be added to the 2016-17 Statement of Outcomes is provided below and is highlighted in yellow. The proposed modification has been vetted from an IT programmatic vantage by CIO Brown.



Homeland
Security

For Official Use Only

FALCON OPERATIONS & MAINTENANCE SUPPORT & SYSTEM ENHANCEMENT

Statement of Outcomes

5/28/2016 – 5/27/2017

(Performance Work Statement Appendix B-1)

September 27, 2016

Homeland Security Investigations (HSI)

Mission Support



Homeland
Security

Statement of Outcomes – FALCON OPERATIONS & MAINTENANCE SUPPORT & SYSTEM ENHANCEMENT Contract

(Appendix B-1)

Period of Performance - 5/28/2016-5/27/2017

1.0 BACKGROUND

Appendix B-1 shall be considered an addendum to **Section 5.8 of the Performance Work Statement: Additional Work to Be Performed During the Initial POP, Option Years 1-2, and the Optional Six-Month Extension.**

During the twelve-month period 5/28/2016 to 5/27/2017, or longer if mutually agreed to by the parties, the Contractor shall perform configuration, integration, and training services for the following projects, which are not presented in priority order. The parties shall mutually agree to the list priorities and project timelines.

2.0 PROJECT PLANS AND SCHEDULES

The Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten work days after the beginning of a contract year a draft Schedule of Outcomes, listing the planned start dates of each planned outcome-based project. Based upon this Schedule of Outcomes, the Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten working days prior to the initiation of work on a particular outcome-based project a Project Plan and a Project Schedule. The one exception shall be for the first of the planned outcome-based projects, for which a Project Plan and a Project Schedule shall be delivered by the Contractor concurrently with delivery of the draft Schedule of Outcomes.

Project Plans, mutually agreed to by HSI and the Contractor, shall identify specific user groups, workflows and discrete tasks. The Project Plans will define the agreed upon scope of each outcome – any and all changes to the Project Plans must be mutually agreed upon by the parties and documented in weekly and/or monthly reports. Specifically, any addition of a new task within the Project Plan must be mutually agreed upon by the parties, and counterbalanced with the deletion or delay of an existing task of equal effort, as documented in weekly and/or monthly reports. Project Schedules shall list high-level tasks for a specified outcome-based project. Project Plans and Schedules may be amended by the two parties' mutual agreement.

Government delay has prevented delivery of 2015 – 2016 Period of Performance Outcomes 2, 3, and 7 prior to the conclusion of the Base Period; work associated with these Outcomes shall be referred to as "Residual Outcome Work." For Residual Outcome Work from the prior contract performance period, which will need to be completed at no additional cost during the current contract performance period, the Contractor shall deliver Revised Schedules, broken out by Outcome, no later than twenty-one (21) working days following the initiation of the current

contract performance period. These Revised Schedules shall be finalized through consultations and agreement between the Contractor and the FALCON PMO.

Regarding delay of work caused by government action or inaction, Equitable Adjustments shall take the form of adjustments in schedule with no penalty to the Contractor. In cases of extraordinary delay caused by government action or inaction (completion of work by the Contractor is anticipated to be delayed beyond one additional Period of Performance; for example, from the Base POP into Option Year 2), the government and the Contractor shall mutually agree upon a change in contract scope, at no penalty to the Contractor, whereby more feasible work of a similar magnitude shall be substituted for the work affected by an extraordinary delay. Equitable Adjustments shall not take the form of additional monetary compensation to the Contractor, due to the contract's Firm Fixed Price.

3.0 PROJECT MANAGEMENT

As part of the Draft Project Plan for each planned outcome-based project, Contractor shall identify a project lead, who will (a) coordinate all Contractor work on that particular outcome-based project; (b) manage the Project Plan and Project Schedule; and (c) report on progress and achievement of project milestones at weekly meetings with the FALCON PMO Team and to inquiries made by the FALCON Program Manager or other HSI authorities. At the Contractor's discretion, a particular employee may be assigned as project lead for more than one outcome-based project.

In addition to weekly progress meetings, the Contractor shall provide (a) quarterly briefings to which all HSI Unit Chiefs are invited to participate; and (b) twice yearly briefings to the Executive Steering Committee (ESC), coordinated with the October '16 and April '17 ESC meetings, on progress and achievement of project milestones across all outcomes.

The FALCON Program Manager shall identify a governmental project lead for each planned outcome-based project. This governmental project lead will (a) identify governmental Subject Matter Experts (SMEs) as necessary for requirements gathering, user feedback, and user testing; (b) facilitate meetings between governmental SMEs and Contractor staff; (c) coordinate agreements between the FALCON PMO and other bodies within ICE or other governmental agencies required for exchanges of data necessary for the accomplishment of the outcome-based project; (d) review/approve all changes to the Project Plan and/or Project Schedule proposed by the Contractor; and (d) alert the FALCON Program Manager and the FALCON COR/ACOR whenever schedule breeches are anticipated to occur or other problems arise which may adversely impact either project quality or the achievement of project deadlines.

All training activities conducted in support of these outcomes must be coordinated, in advance, with the FALCON Program Management Office (PMO).

During the first week of February, Contractor's project leads will meet with the FALCON PMO and other key stakeholders identified by the government to present status updates regarding any Outcome work which the Contractor estimates will not be completed by the end of the current

Period of Performance. If the delay in Outcome work is due to Government or Contractor delay—delayed access to data or delayed Palantir Cloud authorization, for example—Contractor shall present draft action plans reflecting the decreased remaining time to complete the project in the Period of Performance, which shall be finalized through consultations and mutually agreed upon by the Contractor and the FALCON PMO.

4.0 LIST OF RESIDUAL OUTCOME WORK FROM APPENDIX B (2015-2016 OUTCOMES) NOT COMPLETED DUE TO GOVERNMENT DELAY PRIOR TO 5/26/2016 WHICH SHALL BE COMPLETED DURING THE 5/28/2016-5/27/2017 PERIOD AT NO ADDITIONAL COST TO THE GOVERNMENT

Completion of some final technical elements of the following 2015-16 Outcomes are dependent upon IOC deployment of the Investigative Case Management (ICM) system, which, due to no fault of the Contractor's, has been delayed from March, 2016 to 6/20/2016 (with IOC window extending to September, 2016). Contractor shall complete all elements of the following Outcomes at the earliest date practicable, following a revised Project Schedule mutually agreed upon between Contractor and the government. Completion of this work shall not count against 2016-2017 Outcomes, as payment for this work has been made to Contractor during the 2015-2016 contract year.

(b)(7)(E);(b)(5)

(b)(5);(b)(7)(E)

5.0 LIST OF 2016-2017 OUTCOME-BASED PROJECTS

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

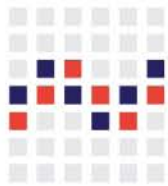
(b)(7)(E)

5.0 ESCALATION

At the beginning of each year of contract performance, the AD and DAD over the FALCON program, with the input of the ESC and of the Contractor will agree upon the addition of up to five outcomes to be completed during the upcoming year (the number of outcomes may be higher if both parties agree). If ICE and the Contractor are unable to agree upon the scope of a given outcome or set of outcomes, the Contractor will provide a detailed technical rationale as to why the outcome falls outside the scope of PWS. This written rationale shall include the level of effort and why this level of effort is not attainable and shall be presented to the ICE FALCON Program Manager and COR/ACOR within five (5) business days of the Contractor's initial announcement of lack of agreement on the Statement of Outcomes. In this scenario, HSI management and the Contractor's management will use this information to reach a final agreement on the Statement of Outcomes. Contractor will provide the implementation support for all tasks listed in an annual outcomes statement to which both HSI and the Contractor agree.

Should the provision by the Contractor of a technical rationale for the non-feasibility of an outcome fail to result in agreement between HSI management and the Contractor's management on the contents of the Statement of Outcomes, either party may request adjudication from the assigned ICE Contracting Officer (CO), who shall make a determination within five (5) business days of receipt of the adjudication request as to whether or not the disputed outcome(s) shall be included in the Statement of Outcomes. In the event that HSI's priorities change during the period of time covered by a Statement of Outcomes and HSI requests that the Statement of Outcomes be amended, and the Contractor determines that this new request for work does not clearly fall within the scope of the existing Statement of Outcomes, the Contractor may present the change request to the CO, who shall review the request to determine whether HSI's request falls within the scope of that document. Such determinations must be made within five (5) business days of the escalation request. The Contractor will not be obligated to take any action on the new request for work unless and until the CO, in coordination with the Contractor, approves the request and determines that such request falls within the scope of an existing Statement of Outcomes or otherwise amends such document to include the new request for work. In the event the CO and Contractor are unable to reach an agreement, the matter will be referred to ICE's Head of Contracting Authority (HCA) for final adjudication. For any priority tasks outside the scope of the existing Statement of Outcomes, HSI may request a level of effort from Contractor; Contractor shall not be obligated to perform such tasks unless (i) the task consists of high priority case work and is specifically requested by the Executive Assistant Director of HSI (or his/her designee); and (ii) a required task of a comparable level of effort is explicitly postponed or eliminated.

Changes to the annual Statement of Outcomes shall be incorporated into the contract through bilateral modification.



Palantir Change Order Proposal to Task Order HSCETE-13-F-00030



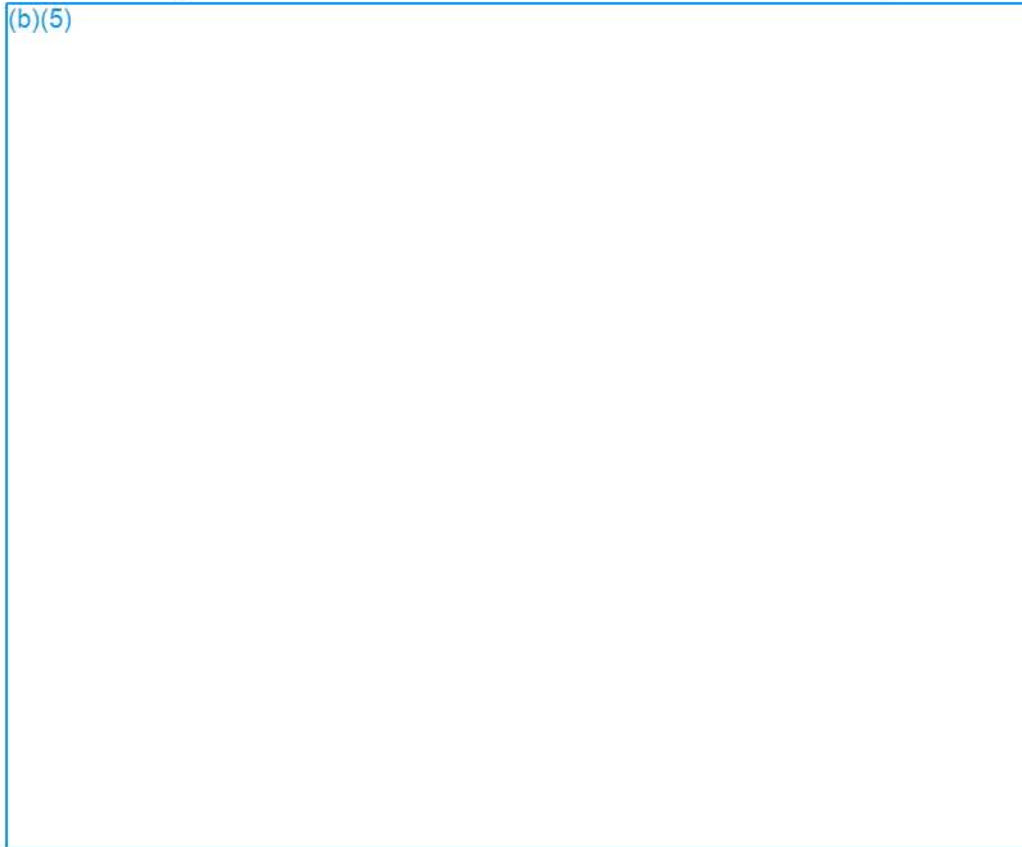
Intent of Change Proposal

2

(b)(5);(b)(7)(E)

Comparison: Steady-State vs. Exercise of 8 Core Expansion Option

3




Change Proposal: Palantir Gotham FFP License

4

(b)(5);(b)(7)(E)

PWS Deliverable Comparison: Palantir Gotham FFP License vs. Core-base

(b)(5);(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

The Trade Transparency Unit's (TTU) Data Processing Requirements

(b)(7)(E)

HSI's Requirement for the DARTTS Data Set to Be Accessed by FALCON

(b)(7)(E)

