



U.S. Immigration
and Customs
Enforcement

~~For Official Use Only~~

FALCON OPERATIONS & MAINTENANCE SUPPORT Performance Work Statement (Conversion to Unlimited Gotham License)

August 1, 2014

Homeland Security Investigations (HSI)

Mission Support



Homeland
Security

FALCON System Operations & Maintenance Support Services
Performance Work Statement

(b)(4)

1.0 PROJECT TITLE

Performance Work Statement (PWS) for FALCON System Operations and Maintenance Support Services (b)(4)

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, development, operation, maintenance, coordination, and support of one of HSI Information Sharing and Infrastructure Management's (ISIM) technology platforms and software assets, FALCON. (b)(7)(E)

(b)(7)(E)

The FALCON system is comprised of several sub-components. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



3.0 SCOPE

(b)(7)(E)



(b)(7)(E)



The additional data sets (this list is not exhaustive) are listed below.

(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

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
- 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 Technical Reference Model (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 task order purchase includes the tasks described in the following sections:

5.1 Tier 1 – Help Desk Support

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:
 - o simple requests such as password resets and account unlocks
 - o basic network and application troubleshooting
 - o 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 at the EOC. 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 and problem resolution.

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 service level agreements (SLA);
- The Contractor shall respond to all Tier 2 System Maintenance tickets in accordance with the SLA;
- The Contractor shall develop 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 System Change Request (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 the application software as well as evaluate and estimate the level of effort associated with requests for system modification. Corrective work includes performing System Change Requests (SCRs) that reflect a change to requirements or technical specifications, as well as updating and maintaining the required Systems Lifecycle Methodology (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);

FALCON Operations & Maintenance Support
Performance Work Statement

- (b)(7)(E)
- The Contractor shall respond to all Tier 3 System Maintenance Support tickets in accordance with service level agreements (SLA's);
- 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	41–250 Hours
Major Change	251–1000 Hours

*Development is any enhancement that is estimated to exceed 250 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. It is anticipated that these calls will occur no more than 10 times a year and can most likely be addressed via telephone and/or remote access to the FALCON operating infrastructure. 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:

Change Classification	Estimated Effort Required	Estimated number of SCRs to Be Conducted – Per Year
Minor Change	1 – 40 Hours	20
Moderate Change	41 – 250 Hours	12
Major Change	251 – 1000 Hours	5

SCRs for FALCON may include requirements analysis, design, development, integration &

FALCON Operations & Maintenance Support
Performance Work Statement

testing, and implementation, including any updates needed to product documentation.

(b)(7)(E)

ICE reserves the right to request FAR 52.227-14 (Alt IV) for any software development/modification/enhancement that is mutually determined 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)		

Table 3. FALCON System Software

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

FALCON Operations & Maintenance Support
Performance Work Statement

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)

5.2.2 Operational Support - Database

(b)(7)(E)

5.2.3 Operational Support – System Tuning

(b)(7)(E)

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.2.4 Operational Support – System Administration

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.3 Configuration Management

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.4 Training Support Included in Operations and Maintenance Services

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.5 Optional Classroom Training

FALCON Operations & Maintenance Support
Performance Work Statement

Contingent upon requests from the FALCON PMO, the Contractor shall arrange for and provide classroom training of the types and for the numbers of ICE employees and/or contractors, as well as classroom locations, specified in the individual service call. The Contractor shall be responsible for collecting all necessary permission forms and feedback forms from attending ICE employees and returning these forms to the FALCON PMO.

5.6 Support of FALCON Mobile Technology

Contractor shall ensure the support for the FALCON Mobile system on the Apple iOS operating system utilized for the iPhone. This includes the following features:

- (b)(7)(E)
-
-
-
-
-
-
-
-

(b)(7)(E)

5.7 Conversion of Legacy DARTTS to FALCON-DARTTS

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

(b)(7)(E)



5.8 Inclusion of EID Data Set in FALCON during Option Year 1

(b)(7)(E)



5.9 Migration of Telecommunications Linking System from TECS Mainframe to FALCON

(b)(7)(E)



(b)(7)(E)



5.10 Addition of Three Enhancements/New Features to FALCON-DARTTS

(b)(7)(E)



The three new features are described below:

5.10.1

(b)(7)(E)



FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)



5.10.2

(b)(7)(E)



(b)(7)(E)



(b)(7)(E)

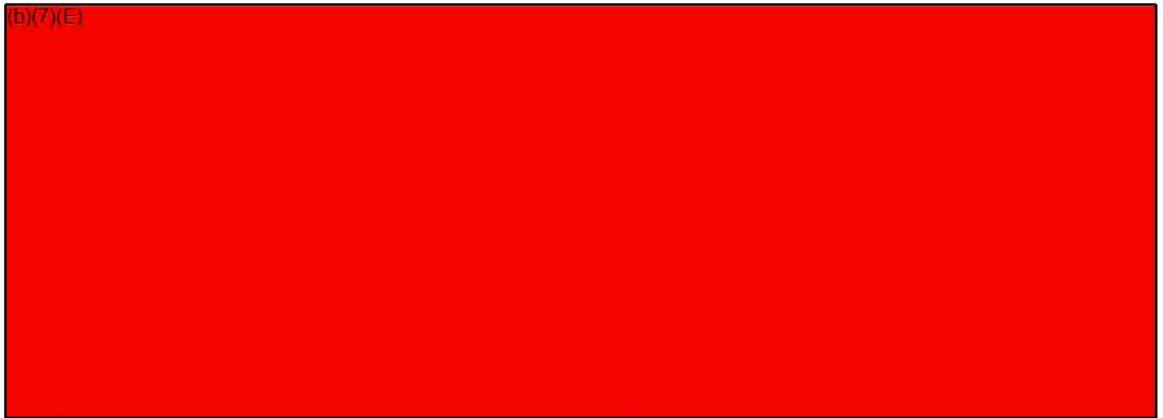


FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)



Contractor shall:

- (b)(7)(E)
 -
 -
 -
 -
 -
- 

5.10.3

(b)(7)(E)



(b)(7)(E)



Contractor shall:

- (b)(7)(E)
- 

FALCON Operations & Maintenance Support
Performance Work Statement

- (b)(7)(E)
-
-

5.11 Additional Work to Be Performed (b)(4) **During**

(b)(4)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

6.0 PERFORMANCE STANDARDS

The following table defines the performance standards to be adhered to for the FALCON System Maintenance and Services effort.¹

¹ Any enhancements, corrective maintenance, or other code changes to FALCON should not negatively impact system

FALCON Operations & Maintenance Support
Performance Work Statement

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, system, divided by the total number of tickets.

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
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
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

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.

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.

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

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 at the Unit Chief level. 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

FALCON Operations & Maintenance Support
Performance Work Statement

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
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
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

FALCON Operations & Maintenance Support

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	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
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

FALCON Operations & Maintenance Support

Performance Work Statement

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
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%

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

Performance Work Statement

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
---	--	---	--	---	--	--	--	---

- 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
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) (b)(4),(b)(7)(E) (b)(4),(b)(7)(E)	As Required	Electronic copy - PM, Electronic Library Management System (ELMS) Software (SW): ICE source control repository (Subversion); OCIO representative on FALCON PMO (either Walter Wagner or alternative OCIO representative)
Project Schedule (SLM Deliverable)	As Required	Electronic copy - PM, ELMS, Contracting Officer
Quarterly Progress Report	Quarterly, within 15 calendar days of the end of the quarter being reviewed	Electronic copy: PM, Contracting Officer, COR
Certification and Accreditation Documentation	As Required	Electronic copy: PM, ELMS, COR
Transition In Plan- Final	15 calendar days after award	Electronic copy: PM, Contracting Officer, COR
Transition Out Plan	120 calendar days before the end of the POP	Electronic copy: PM, Contracting Officer, COR
QASP- Final	15 calendar days after award	Electronic copy: PM, Contracting Officer, COR

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

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

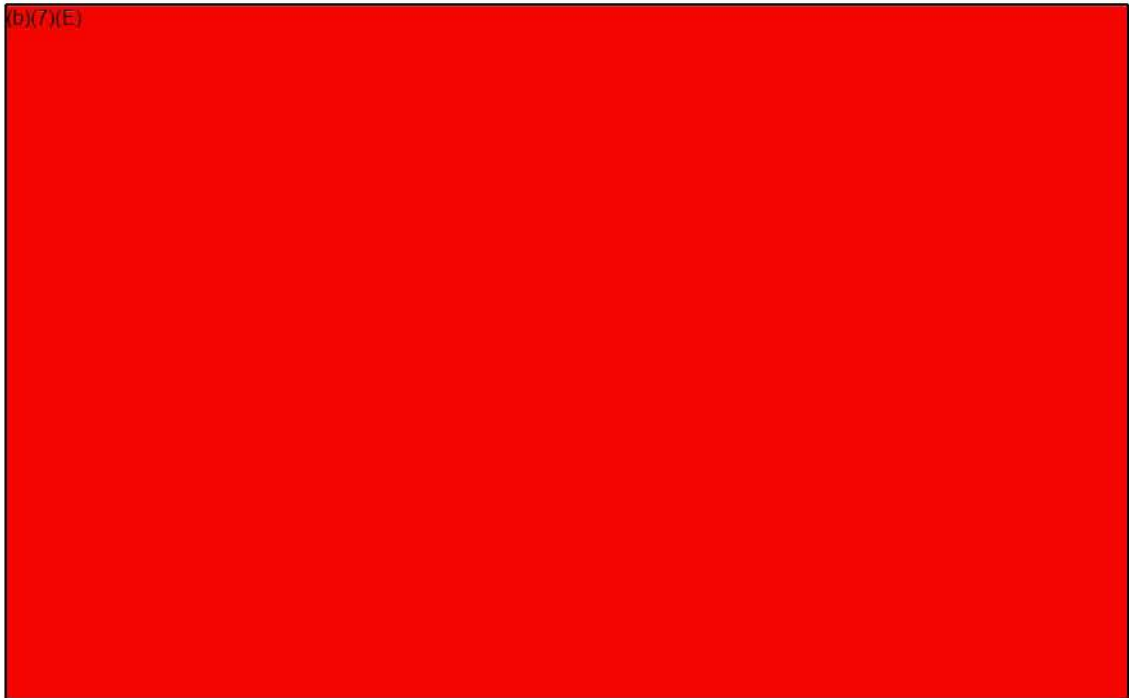
8.1 General Constraints

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.
- 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

(b)(7)(E)

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

(b)(7)(E)

-
-
-
-

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

(b)(7)(E)

(b)(7)(E)

(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.

Start of Initial Period of Performance

Individual Data Records Accessible by FALCON:

FALCON-SA User Base:

FALCON-SA Concurrent Users:

FALCON Web Access User Base:

FALCON Web Access Concurrent Users:

FALCON Mobile User Base:

FALCON Mobile Concurrent Users:

Upon Deployment of FALCON-DARTTS

Individual Data Records Accessible by FALCON:

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

FALCON-SA User Base:
FALCON-SA Concurrent Users:
FALCON Web Access User Base:
FALCON Web Access Concurrent Users:
FALCON Mobile User Base:
FALCON Mobile Concurrent Users:

(b)(7)(E)

Upon Deployment of EID Data Set in Option Year 1

Individual Data Records Accessible by FALCON:
FALCON-SA User Base:
FALCON-SA Concurrent Users:
FALCON Web Access User Base:
FALCON Web Access Concurrent Users:
FALCON Mobile User Base:
FALCON Mobile Concurrent Users:

From the initiation of the contract modification instituting the Gotham Unlimited License, the following levels of service will apply:

Individual Data Records Accessible by FALCON:
FALCON-SA User Base:
FALCON-SA Concurrent Users:
FALCON Web Access User Base:
FALCON Web Access Concurrent Users:
FALCON Mobile User Base:
FALCON Mobile Concurrent Users:

(b)(7)(E)

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 laptops and four i-Phone handheld devices:

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

(b)(7)(E)



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 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 nine (9) months plus four (4) 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 4.

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, 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

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 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-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.

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 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.

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

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

FALCON Operations & Maintenance Support
Performance Work Statement

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 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 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.

FALCON Operations & Maintenance Support
Performance Work Statement

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.

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 (FINS). 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 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.

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
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
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
(b)(4),(b)(7)(E)	

FALCON Operations & Maintenance Support
Performance Work Statement

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
(b)(4),(b)(7)(E)	
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
(b)(4),(b)(7)(E)	
RELRES	Relationship Resolution
RFD	Request for Deviation
ROI	Records of Investigation

FALCON Operations & Maintenance Support
Performance Work Statement

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



U.S. Immigration
and Customs
Enforcement

~~For Official Use Only~~

FALCON OPERATIONS & MAINTENANCE SUPPORT Performance Work Statement (Conversion to Unlimited Gotham License)

August 7, 2014

Homeland Security Investigations (HSI)

Mission Support



Homeland
Security

FALCON System Operations & Maintenance Support Services
Performance Work Statement

(b)(4)

1.0 PROJECT TITLE

Performance Work Statement (PWS) for FALCON System Operations and Maintenance Support Services (b)(4)

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, development, operation, maintenance, coordination, and support of one of HSI Information Sharing and Infrastructure Management's (ISIM) technology platforms and software assets, FALCON. (b)(7)(E)

(b)(7)(E)

The FALCON system is comprised of several sub-components. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

3.0 SCOPE

(b)(7)(E)

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

(b)(7)(E)

(b)(7)(E)

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
- 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 Technical Reference Model (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 task order purchase includes the tasks described in the following sections:

5.1 Tier 1 – Help Desk Support

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:
 - o simple requests such as password resets and account unlocks
 - o basic network and application troubleshooting
 - o 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 at the EOC. 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 and problem resolution.

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 service level agreements (SLA);
- The Contractor shall respond to all Tier 2 System Maintenance tickets in accordance with the SLA;
- The Contractor shall develop 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 System Change Request (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 the application software as well as evaluate and estimate the level of effort associated with requests for system modification. Corrective work includes performing System Change Requests (SCRs) that reflect a change to requirements or technical specifications, as well as updating and maintaining the required Systems Lifecycle Methodology (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);

FALCON Operations & Maintenance Support
Performance Work Statement

- The Contractor shall develop 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 System Change Request (SCR) in future release.
- The Contractor shall respond to all Tier 3 System Maintenance Support tickets in accordance with service level agreements (SLA's);
- 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	41–250 Hours
Major Change	251–1000 Hours

*Development is any enhancement that is estimated to exceed 250 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. It is anticipated that these calls will occur no more than 10 times a year and can most likely be addressed via telephone and/or remote access to the FALCON operating infrastructure. 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:

Change Classification	Estimated Effort Required	Estimated number of SCRs to Be Conducted – Per Year
Minor Change	1 – 40 Hours	20
Moderate Change	41 – 250 Hours	12
Major Change	251 – 1000 Hours	5

SCRs for FALCON may include requirements analysis, design, development, integration &

FALCON Operations & Maintenance Support
Performance Work Statement

testing, and implementation, including any updates needed to product documentation.

(b)(7)(E)



ICE reserves the right to request FAR 52.227-14 (Alt IV) for any software development/modification/enhancement that is mutually determined 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)		

Table 3. FALCON System Software

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

FALCON Operations & Maintenance Support
Performance Work Statement

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)

5.2.2 Operational Support - Database

(b)(7)(E)

5.2.3 Operational Support – System Tuning

(b)(7)(E)

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.2.4 Operational Support – System Administration

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.3 Configuration Management

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.4 Training Support Included in Operations and Maintenance Services

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.5 Optional Classroom Training

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.6 Support of FALCON Mobile Technology

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

-
-
-
-
-
-
-
-

5.7 Inclusion of EID Data Set in FALCON during Option Year 1

(b)(7)(E)

A large rectangular area of the document is completely redacted with a solid black fill.

5.8 Migration of Telecommunications Linking System from TECS Mainframe to FALCON

(b)(7)(E)



5.9 Addition of Three Enhancements/New Features to FALCON-DARTTS

(b)(7)(E)



The three new features are described below:

5.9.1

(b)(7)(E)



(b)(7)(E)



5.9.2

(b)(7)(E)



(b)(7)(E)



FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)

(b)(7)(E)

Contractor shall:

-
-
-
-
-

(b)(7)(E)

5.9.3

(b)(7)(E)

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)



Contractor shall:

-
-
-
-

(b)(7)(E)



**5.10 Additional Work to Be Performed Under the Gotham Unlimited License During
Option Years 2-4 and the Optional Six-Month Extension**

(b)(7)(E)



FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

6.0 PERFORMANCE STANDARDS

The following table defines the performance standards to be adhered to for the FALCON System Maintenance and Services effort.¹

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.

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
Performance Work Statement

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.
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.

FALCON Operations & Maintenance Support
Performance Work Statement

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
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

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.

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
Performance Work Statement

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

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 at the Unit Chief level. 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
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
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

FALCON Operations & Maintenance Support

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	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
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

FALCON Operations & Maintenance Support

Performance Work Statement

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
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%

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

Performance Work Statement

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
---	--	---	--	---	--	--	--	---

- 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
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) (b)(4),(b)(7)(E)	As Required	Electronic copy - PM, Electronic Library Management System (ELMS) Software (SW): ICE source control repository (Subversion); OCIO representative on FALCON PMO (either Walter Wagner or alternative OCIO representative)
Project Schedule (SLM Deliverable)	As Required	Electronic copy - PM, ELMS, Contracting Officer
Quarterly Progress Report	Quarterly, within 15 calendar days of the end of the quarter being reviewed	Electronic copy: PM, Contracting Officer, COR
Certification and Accreditation Documentation	As Required	Electronic copy: PM, ELMS, COR
Transition In Plan- Final	15 calendar days after award	Electronic copy: PM, Contracting Officer, COR
Transition Out Plan	120 calendar days before the end of the POP	Electronic copy: PM, Contracting Officer, COR
QASP- Final	15 calendar days after award	Electronic copy: PM, Contracting Officer, COR

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

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.
- 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

(b)(7)(E)



-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

(b)(7)(E)



-
-
-
-

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

(b)(7)(E)



(b)(7)(E)

(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.

Start of Initial Period of Performance

Individual Data Records Accessible by FALCON:

FALCON-SA User Base:

FALCON-SA Concurrent Users:

FALCON Web Access User Base:

FALCON Web Access Concurrent Users:

FALCON Mobile User Base:

FALCON Mobile Concurrent Users:

Upon Deployment of FALCON-DARTTS

Individual Data Records Accessible by FALCON:

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

FALCON-SA User Base:
FALCON-SA Concurrent Users:
FALCON Web Access User Base:
FALCON Web Access Concurrent Users:
FALCON Mobile User Base:
FALCON Mobile Concurrent Users:

(b)(7)(E)

Upon Deployment of EID Data Set in Option Year 1

Individual Data Records Accessible by FALCON:
FALCON-SA User Base:
FALCON-SA Concurrent Users:
FALCON Web Access User Base:
FALCON Web Access Concurrent Users:
FALCON Mobile User Base:
FALCON Mobile Concurrent Users:

From the initiation of the contract modification instituting the Gotham Unlimited License, the following levels of service will apply:

Individual Data Records Accessible by FALCON:
FALCON-SA User Base:
FALCON-SA Concurrent Users:
FALCON Web Access User Base:
FALCON Web Access Concurrent Users:
FALCON Mobile User Base:
FALCON Mobile Concurrent Users:

(b)(7)(E)

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 laptops and four i-Phone handheld devices:

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

(b)(7)(E)

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 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 nine (9) months plus four (4) 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 4.

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, 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

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 alteration, 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, unauthorized 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 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-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.

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 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.

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

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

FALCON Operations & Maintenance Support
Performance Work Statement

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 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 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.

FALCON Operations & Maintenance Support
Performance Work Statement

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.

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 (FINS). 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 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.

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
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
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
(b)(4),(b)(7)(E)	

FALCON Operations & Maintenance Support
Performance Work Statement

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
(b)(4),(b)(7)(E)	
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
(b)(4),(b)(7)(E)	
RELRES	Relationship Resolution
RFD	Request for Deviation
ROI	Records of Investigation

FALCON Operations & Maintenance Support
Performance Work Statement

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

**U.S. Department of Homeland Security
Immigration and Customs Enforcement**

Homeland Security Investigations

Information Sharing and Infrastructure Management

Statement of Work

Version 8

FALCON

500 12th Street, S.W.
Washington, D.C. 20536

March 12, 2013

TABLE OF CONTENTS

1.0	PROJECT TITLE
2.0	BACKGROUND.....
3.0	SCOPE OF WORK.....
4.0	SPECIFIC TASKS
5.0	KEY PERSONNEL
6.0	PLACE OF PERFORMANCE
7.0	HOURS OF OPERATION.....
8.0	PERIOD OF PERFORMANCE.....
9.0	IT SECURITY REQUIREMENTS.....
10.0	PRICING
11.0	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....
12.0	DHS ENTERPRISE ARCHITECTURE COMPLIANCE
APPENDIX A – LIST OF ACRONYMS.....	

1.0 PROJECT TITLE

FALCON

2.0 BACKGROUND

HSI is a critical asset in 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. HSI uses its legal authority to investigate issues such as immigration crime; National security threats, human rights violations, human smuggling and child pornography/exploitation; smuggling of narcotics, weapons and other types of contraband; and financial crimes, cyber crime, commercial fraud and export enforcement issues. ICE special agents also conduct investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack or exploitation.

With ICE investigations covering such a broad range of areas, its agents and analysts require a wholly integrated, consolidated platform providing search, analytic, geospatial, reporting and situational awareness capabilities that can support these functions across a broadly diverse universe of structured and unstructured law enforcement data residing in various source environments.

This task will directly support the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), , Homeland Security Investigations (HSI), Mission Support (MS), Information Sharing and Infrastructure Management (ISIM), Information Sharing Support (ISS) which is responsible for deploying (in close cooperation with the Office of the Chief Information Officer (OCIO), Systems Development Division (SDD)) a consolidated Commercial Off The Shelf (COTS) platform that provides (b)(7)(E) in support of the ICE mission. This effort is intended to support the requirements of HSI.

3.0 SCOPE OF WORK

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

4.0 SPECIFIC TASKS

4.1 Requirements, Maintenance, Operations and Production Support

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

(b)(5), (b)(7)(E)



1. Data Integration

a. (b)(5), (b)(7)(E)



b.

c.

d.

e.

f.

g.

h.

i.

j.

k.

2. Data Modeling

a. (b)(5), (b)(7)(E)



b.

c.

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

3. Search & Discovery

A large black rectangular redaction box covers the majority of the page, obscuring all content except for the header and footer. The box is solid black and extends from the top margin down to the bottom margin, and across most of the page width.

[illegible]

a.

b.

c.

(b)(5),(b)(7)(E)

d.

e.

f.

g.

5. Collaboration

a.

(b)(5),(b)(7)(E)

b.

c.

6. Security

a.

(b)(5),(b)(7)(E)

b.

c.

(b)(5),(b)(7)(E)

d.

e.

f.

7. Openness and Extensibility

a. (b)(5),(b)(7)(E)

b.

c.

d.

e.

f.

g.

h.

8. Data Management

a. (b)(5),(b)(7)(E)

b.

c.

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

A large rectangular area of the document is completely redacted with a solid black fill.

d.

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

A large rectangular area of the document is completely redacted with a solid black fill.

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

A large rectangular area of the document is completely redacted with a solid black fill.

|

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

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

9. **Workflow Applications**

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

10. (b)(5);(b)(7)(E)

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

10.2

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

10.3

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

4.2 Training

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

5.0 KEY PERSONNEL

The Government has determined that the Project Manager and Project Leads are key personnel for this Scope of Work. The Contractor may designate other positions as necessary as key to the work to be performed under this contract. Key personnel shall be located within the greater Washington, D.C. area (GWA) to enable them to interface with client personnel on a regular basis.

The Project Manager shall possess the technical and leadership skills necessary for a project of this magnitude. Prior experience working with DHS/ICE, IT-related program management experience, experience managing law enforcement and/or enterprise-wide systems is preferred.

Project Leads shall possess the technical and leadership skills necessary for a project of this magnitude. Prior experience working with DHS/ICE, IT-related program management experience, experience managing law enforcement and/or enterprise-wide systems is preferred.

6.0 PLACE OF PERFORMANCE

Work shall be performed primarily at ICE Headquarters, 500 12th Street S.W., Washington D.C. 20536 and Contractor facilities in the greater Washington, D.C. area (GWA).

7.0 HOURS OF OPERATION

The Contractor shall cover the normal operational hours of 9:00 am and 5:00 pm Monday through Friday (Eastern US Time Zone). As necessary, the Contractor shall provide support on an on-call basis for after normal operational (working) hours. The Contractor shall have the capacity to provide resources and support 24x7, 365 days a year as required by the Government, including Government holidays.

8.0 PERIOD OF PERFORMANCE

This requirement will consist of a three month base period.

In addition to compliance with the SLM, EA Standards, and Security standards, COTS and Government Off-The-Shelf (GOTS) products shall be approved through the IT Change Request (ITCR) process, if required.

9.0 PRICING

This SOW hereby incorporates by reference Palantir's July 18, 2012 quote.

10.0 IT SECURITY REQUIREMENTS

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

9.2 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

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

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

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.

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

Handling of Sensitive Information and IT Resources

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 alteration, 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 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.

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 will 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 will 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.

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.

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.

Contingency Planning

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

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.

Use of Government Equipment

Contractors are not authorized to use Government office equipment of 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.

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.

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 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.

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.

11.0 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

10.1 General

ICE has determined that performance of this contract requires that the Contractor, Sub-contractor(s), vendors(s), etc. have access to sensitive ICE information which requires DHS 6C position of public trust adjudication. A limited number of Contractor support personnel will require up to Top Secret with SCI caveats and that the Contractor shall adhere to the following requirements.

11.2 Suitability Determination

ICE shall have and 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 EOD decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the purchase order. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office. Contract employees assigned to the contract not needing access to sensitive ICE information or recurring access to ICE facilities will not be subject to security suitability screening.

11.3 Background Investigations

Contract 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 OPR-PSU. Prospective Contractor employees with adequate security clearances issued by the Defense Industrial Security Clearance Office (DISCO) may not be required to submit complete security packages, as the clearance issued by DISCO may be accepted. Prospective Contractor employees without adequate security clearances issued by DISCO shall submit the following completed forms to the OPR-PSU through the COTR, no less than 35 days before the starting date of the contract or 35 days prior to the expected entry on duty of any employees, whether a replacement, addition, Sub-contractor employee, or vendor:

- Standard Form 86, "Questionnaire for National Security Positions"
- Form will be submitted via e-Qip (electronic forms submission).
- FD Form 258, "Fingerprint Card" **(2 copies)**
- Foreign National Relatives or Associates Statement
- DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
- Optional Form 306 Declaration for Federal Employment (applies to Contractors as well)
- Authorization for Release of Medical Information

Required forms will be provided by DHS 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 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 IT systems and the information contained therein, to include, the development and / or maintenance of DHS IT systems; or access to information contained in and / or derived from any DHS IT system.

In the interest of limiting access to potentially sensitive information and systems, ICE will consider only U.S. Citizens.

11.4 Continued Eligibility

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

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.

DHS 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 DHS determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU through the COTR. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

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

11.5 Employment Eligibility

The Contractor will 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 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 Sub-contractor(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 will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

11.6 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 COTR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COTR 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 COTR 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) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

11.7 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.*. Contractor personnel shall 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).

11.8 Information Technology Security Training and Oversight

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

Contractors who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of 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 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).

12.0 DHS ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet DHS EA policies, standards, and procedures as it relates to this SOW and associated Task Orders. Specifically, the Contractor shall comply with the following DHS requirements:

- All developed solutions and requirements shall be compliant with the DHS EA.
- All IT hardware or software shall be compliant with the DHS EA Technology Reference Model Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office for review and insertion into the DHS Data Reference Model.
- In compliance with Office of Management and Budget (OMB) mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

APPENDIX A – LIST OF ACRONYMS

AHS	Application Hosting Services
AIDW	Automated Information Data Warehouse
AJAX	Asynchronous Java and XML
C&A	Certification and Accreditation
CCB	Change Control Board
CO	Contracting Officer
COB	Close of Business
COTR	Contracting Officer Technical Representative
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
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DISCO	Defense Industrial Security Clearance Office
DoJ	Department of Justice
EA	Enterprise Architecture
EADM	Enforcement Alien Detention Module
EARM	Enforcement Alien Removal Module
EIT	Electronic and Information Technology
EIU	Executive Information Unit
ELMS	Electronic Library Management System
EOD	Entry on Duty
ETL	Extract, Transfer and Load
FAR	Federal Acquisition Regulations
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
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
IRRIIS	Investigation Records Review for Information Sharing
ISA	Interconnection Security Agreements
ISB	Investigative Systems Branch
ISC ²	International Info Systems Security Certification Consortium
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ITCR	Information Technology Change Request
LECAD	Law Enforcement Centralized Access Development
LEISS	Law Enforcement Information Sharing System
MCC	Mobile Command Center
MD	Management Directive
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
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
PMP	Project Management Professional
POP	Period of Performance
PSU	Personnel Security Unit
QCP	Quality Control Plan
RELRES	Relationship Resolution
RFD	Request for Deviation
ROI	Records of Investigation
SCI	Sensitive Compartmented Information
SBU	Sensitive But Unclassified
SCR	System Change Request
SDA	System Design Alternative
SDD	Systems Development Division
SELC	System Enterprise Lifecycle
SLM	System Lifecycle Management

SOP	Standard Operating Procedure
SOW	Statement of Work
SRD	System Requirements Document
TAIS	Telecommunications and Automated Information Systems
TLS	Telephone Linking System
TMP	Transition Management Plan
TO	Task Order
TS	Top Secret
UAT	User Acceptance Testing