



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Configuration Management Board (CMB) FALCON: Conversion from Core-Based Pricing Model to Unlimited Palantir Gotham License (Firm Fixed Price) *[Enter date of briefing here]*

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

Special Agent/Section Chief, Law Enforcement Support and Information Management 202-

732-(b)(6);(b)(7)(C)

FALCON Overview



U.S. Immigration
and Customs
Enforcement

(b)(7)(E)

FALCON Overview



U.S. Immigration
and Customs
Enforcement

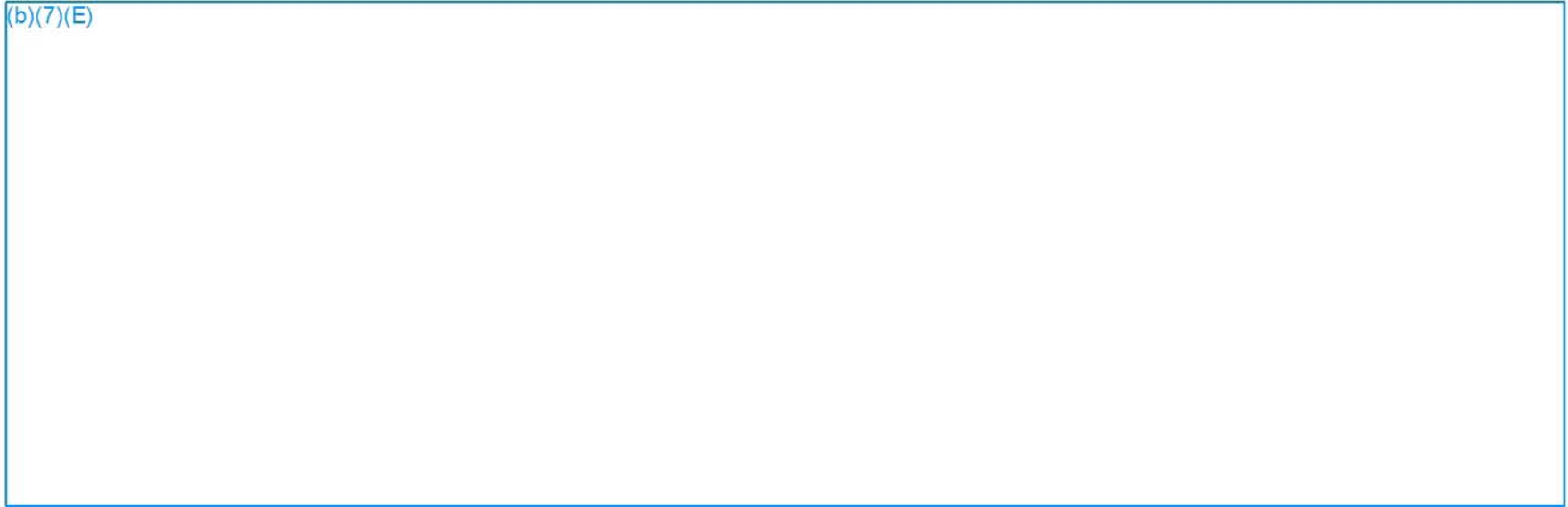
■ (b)(7)(E)

Funding Issues Regarding FALCON



U.S. Immigration
and Customs
Enforcement

- (b)(7)(E)



Costs of Projected FALCON Expansion Under Current Core-Based Pricing Model



U.S. Immigration
and Customs
Enforcement

(b)(5)

Costs of Projected FALCON Expansion Under New Unlimited Palantir Gotham License Plan



U.S. Immigration
and Customs
Enforcement

(b)(5)

- * Approximate amount from DPICS2

Savings of Unlimited Palantir Gotham License Plan vs. Traditional Core-Based Pricing



U.S. Immigration
and Customs
Enforcement

(b)(5)

Option 1: Steady-State Funding With Purchase of 8 Server Cores Per Option Year (No Unlimited Licns)



U.S. Immigration
and Customs
Enforcement

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

Option 2: Remaining with Current Contract Model; Multiple Contract Amendments Adding Cores



U.S. Immigration
and Customs
Enforcement

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

Option 3: Transitioning to Unlimited Gotham License, Away from Core-Based Pricing



U.S. Immigration
and Customs
Enforcement

(b)(5)

ESC Summary



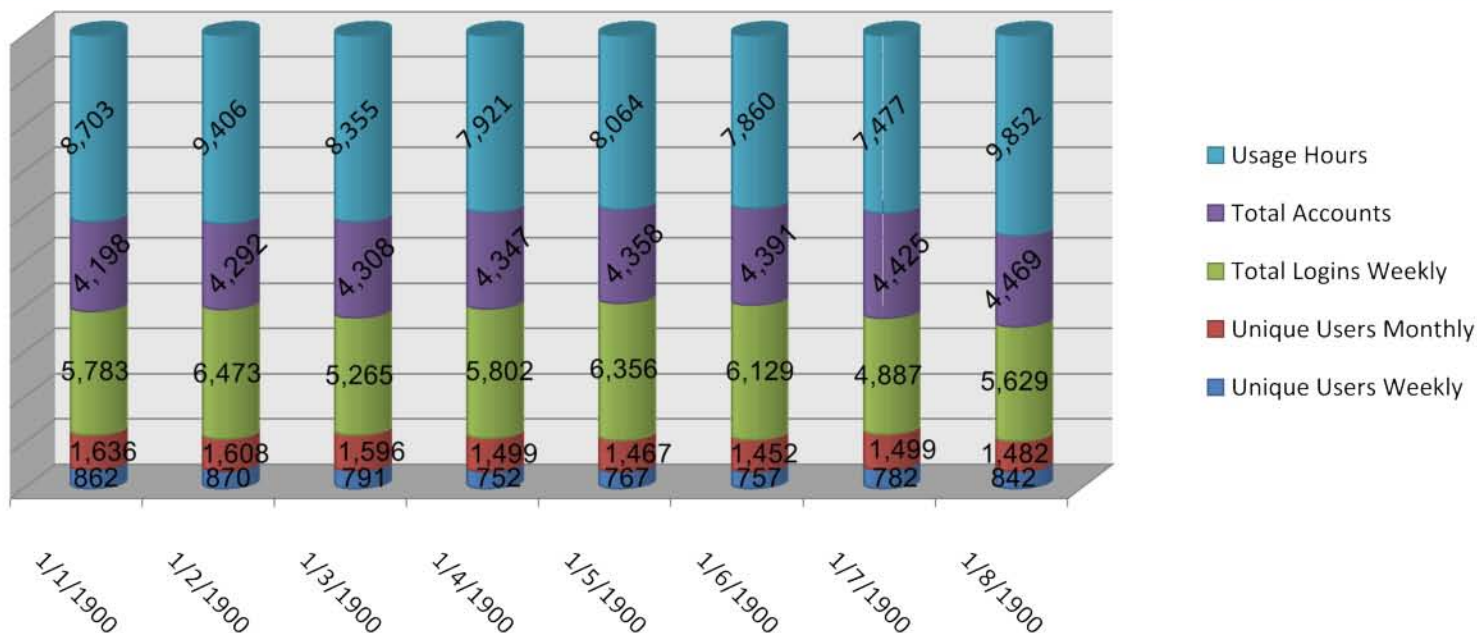
U.S. Immigration
and Customs
Enforcement

(b)(5)

FALCON Weekly System Usage



U.S. Immigration
and Customs
Enforcement



Week	Unique Users Weekly	UniqueUsers Monthly (New)	TotalLogins	TotalAccounts(New)	Hours ofUsage
Apr 28 – May 4	862	1636	5783	4198	8703
May 12–May 18	870	1608	6473	4292	9406
May 19 –May 25	791	1596	5265	4308	8355
Jun 2 – Jun 8	752	1499	5802	4347	7921
Jun 9 – Jun 15	767	1467	6356	4358	8064
Jun 16 – Jun 22	757	1452	6129	4391	7860
Jun 23 – Jun 29	782	1499	4887	4425	7477
Jul 7 – Jul 13	842	1482	5629	4469	9852



Questions?

Funding Request for Follow-on Contract with Palantir USG

Anticipated Period of Performance:

Base Year: March 2013 through March 2014 (with two option years)

Independent Government Cost Estimate:

(b)(5)



*The above costs reflect an inflationary rise of 3% for Operation and Maintenance per year.

➤ **Maintenance**

(b)(7)(E)



➤ **Technical Support**

✓ *Helpdesk Support*

(b)(7)(E)



✓ *Onsite Support*

(b)(7)(E)

✓ *Training*

(b)(7)(E)

✓ *Remote Support*

(b)(7)(E)

Capacity Expansion to Allow More Users and Provide Enhancements

- The Base Year allows for expansion and enhancements for additional users, helpers and features to be added to the FALCON system
- The Option Year 1 allows for expansion and enhancements for additional users, helpers and features to be added to the FALCON system
- The Option Year 2 allows for expansion and enhancements for additional users, helpers and features to be added to the FALCON system

(b)(5)

**These numbers reflect an inflationary rise in cost of 3% per year.*

The system enhancements added to FALCON would include:

(b)(5)

Backup/Recovery Infrastructure

(b)(5)

FALCON Benefits

➤ HSI

- ✓ Train and support of agent base to improve investigative capabilities and increase user growth exceeding the current Intel majority user base
- ✓ Optimize operational methods through implementation of FALCON Mobile capabilities to SAC offices
- ✓ Achieve significant results by improved Analyst/Agent collaboration efforts

➤ INTEL

- ✓ Increase process efficiencies through continued use of Help Desk support and one-on-one desk side assistance
- ✓ Initiate new and evolving customized helpers, enhanced features and importers for improved charting and advanced investigative case work

➤ OIA

- ✓ Train and support of OIA personnel in international offices to improve process efficiencies across HSI
- ✓ Foster cooperation with domestic case agents and analysts using FALCON
- ✓ Maximize operational security through implementation of FALCON Mobile
- ✓ Extend visibility and control with FALCON PGWeb search capabilities

➤ OPR

- ✓ Train and support of OPR personnel to streamline processes
- ✓ Implement and tailor restricted access features
- ✓ Customize auditing and monitoring functionality to optimize control

Contract Year	Contract Term	Description	Total
(b)(4),(b)(7)(E)			

(b)(5)

(b)(4)

DARTTS Development Overview

Overview

DARTTS (Data Analysis and Research for Trade Transparency System) is a web-based system that tracks the import and export data between the United States and a variety of countries.

(b)(7)(E)

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

(b)(4)

13

Talantur Torch is an example of our web visualization tools that allow an analyst to quickly identify trends and isolate discrepancies

The Executive Dashboard can highlight recent incidents and top events in a region, or across the country

Prepared By: (b)(6);(b)(7) Created Date: 4/19/2013
Email: (b)(6);(b)(7)(C) Expiration Date: 5/18/2013
Account Name: ICE Contact Name: Tony Tortora

(b)(4)

Phase I: DARTTS Sunset Pricing for Replacement and Enhancement of current DARTTS Capabilities

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



U.S. Immigration and Customs Enforcement

Limited Source Justification

This acquisition is conducted under the authority of the Multiple Award Schedule Program, Title III of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 3102, et seq), Title 40 U.S.C. 501, Services for Executive Agencies, and is justified by the following facts and rationale under FAR 8.405-6(a)(1)(i)(B) and FAR 8.405-6(b)(1).

1 Agency and Contracting Activity

Department of Homeland Security (DHS)
Immigration and Customs Enforcement (ICE)
Office of Acquisition Management (OAQ)
Information Technology Architecture and Development (ITAD)
801 I Street, NW; Washington, DC 20001

2 Nature and/or Description of the Action Being Approved

This requirement is for brand name licenses, operations support and maintenance, and training from Palantir as the single available source and brand name under the authority of the Multiple-Award Schedule Program. This is for a Firm-Fixed price GSA Schedule 70 purchase that includes Palantir annual licenses (to include Palantir Phoenix services and Palantir mobile subscription services), annual support and maintenance services, an option for additional Palantir annual license and support & maintenance services, optional Bootcamp training, and optional advanced training.

3 Description of Supplies/Services

ICE/HSI requires the following support:

- Tier 1, 2, and 3 user/help desk support
- Product Extension, Engineering, Operations and Integration Services support
- Annual Support and Maintenance for all purchased cores. This includes all upgrades, patches, and fixes as required to maintain the operability and usability of the product, and maintain the required security certifications.
- Instructor training tailored to ICE for trainees to be performed at designated locations.

The Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Mission Support and Law Enforcement Support & Information Management (MS/LESIM) has a requirement to procure licenses, Operations and Maintenance (O&M) support services, optional licenses and O&M services, and training related

to the “Palantir Government” product. Palantir Technologies Inc. is located at 100 Hamilton Avenue, Suite 300, Palo Alto, CA, 94301. The system is used to support DHS/ICE HSI Special Agents, Criminal Research Analysts, Intelligence Analysts, and other support personnel in their investigative operations and gives ICE operational elements the ability to communicate with each other and collaborate on missions.

This software is currently in use within HSI, and the procurement will be for O&M support of the software to include training, desk side support, remote engineering support, onsite engineering support, rapid turnaround, incident submission and resolution through help desk support, simple data integration, configuration, analyst support, program management, and updates to the Palantir Government software package.

The base period of performance is from June 14, 2013 through March 13, 2014 with four (4) option periods of 1 year each. The option to extend services, per FAR 52.217-8, will be evaluated at time of award.

The Independent Government Cost Estimate (IGCE) value, based on the current GSA contract pricing, is as follows:

Base (9 months)	\$1,184,531.04
Option year 1.....	\$3,592,664.84
Option year 2.....	\$3,818,289.48
Option year 3.....	\$4,043,914.12
Option year 4.....	\$4,269,538.76
FAR 52.217-8 (6-month extension)....	\$1,128,123.24
Total.....	\$ 18,037,061.48

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

ICE requires software licenses peculiar to Palantir Technologies IAW 41 U.S.C. 3102 et. seq, as implemented under Federal Acquisition Regulation (FAR) Subpart FAR 8.405- 6(b)(1). ICE also requires software maintenance services, O&M services, and training, on existing software from Palantir Technologies IAW 41 U.S.C. 3102 et. seq., as implemented in FAR 8.405-6(a)(1)(i)(B), only one source is capable of providing the supplies or services required because the supplies or services are unique or highly specialized.

Currently, ICE/HSI has approximately 1600 plus agents and analysts using the Palantir Gotham system for numerous on-going investigations and workflow applications. Palantir Gotham has been modified for ICE’s specific requirements and has been internally renamed as FALCON. FALCON provides HSI Special Agents a highly useful tool which (a) contributes to employee safety by keeping field operatives and supervisors continually aware of one another’s physical locations and (b) heightens investigative effectiveness and efficiency in the field by allowing for instantaneous sharing of photographs and other information regarding persons, vehicles, and locations of interest and which allows for more effective planning and reporting of field operations. Continued support and maintenance is vital to seamlessly providing users with a

fully operational system and the support they require to deliver effective support to the HSI mission.

Continued software maintenance support (Software Maintenance as a Service, which is priced in the GSA Schedule per installed server core) is needed for the underlying Palantir software. Without updates to the software, there is an increased risk that the FALCON system could stop working properly or could be made unstable or compromised by invasive software viruses or other malware. In addition, failure to acquire Software Maintenance as a Service would severely limit HSI's ability to access additional data sets which have been requested by the ICE user base and limit the FALCON system's utility as an investigative tool. At present, FALCON contains data ingested from TECS, SEACATS, SEN, TLS, and HSI tip line. The 56 server cores/Palantir Gotham Perpetual Licenses already purchased give HSI the technical capacity to provide access to these sets of data for the existing user base of 1500 to 1600, plus a small amount of growth in the user base for the full application (users of the slimmed-down version of Gotham, PGWeb, will place a much smaller drain on the system's resources than users of the full application do). However, access to the current data sets listed above is only the beginning of the planned utilization of the FALCON system. The value of Gotham as a product is the logical linkages which can be made between various bits of data (information about persons, locations, events, vehicles, and other items of law enforcement interest) residing in vast data sets which would be otherwise unconnected. The utility of the system and the value it adds to law enforcement investigations increases exponentially as more data sets are added.

Use of Palantir Gotham and FALCON system is intended to increase over the life of the order. The FALCON Integrated Program Team (IPT) is currently vetting requests from the HSI user base for the addition of a dozen more ICE, CBP, and law enforcement-related data sets to FALCON. Growth in the numbers of users of the full application, number of data sets ingested within FALCON, and use of the Phoenix service to access remote data sets (due to the fact that Phoenix builds indexes which will reside on FALCON servers) will require the purchase of additional server cores/Palantir Gotham Perpetual Licenses. These additional licenses will also require annual Maintenance and Support services to allow for updates to the Gotham software, software patches to prevent malicious code/security incidents, and provision of Help Desk and desk-side support services for the user base (Maintenance and Support for the initial year/year of purchase is included in the purchase of a Palantir Gotham Perpetual License).

Additional software licenses to support the increase in users and data sets can only be purchased by Palantir. Palantir is the only supplier that can provide the licenses since only they have access to the system's source components. The additional Palantir Gotham licenses will allow ICE to maintain and update current databases with the most accurate information for the additional end users. In addition to purchasing additional Palantir Gotham licenses to account for an increase in users and data sets, HSI is pilot-testing two plug-ins made available by Palantir Technologies; Phoenix and Palantir Mobile. The Phoenix service is a data-extending utility which allows users of a Gotham instance (such as FALCON) to access remote data sets which are housed on another organization's physical servers. Phoenix then builds and maintains an index of this remote data on the FALCON servers. This process requires less server core capacity, which should allow ICE HSI ingest more data sets than it could normally do using traditional methods. Palantir Mobile will allow Special Agents working on field investigations and operations to track in real-

time the physical locations of their team members on a map on their handheld devices, supervisors at a base of operations to track the physical locations of field operatives, field operatives to instantly share photos taken in the field with their supervisors for additional analysis, field operatives to share real-time operations reports with their supervisors, and for more efficient and accurate after-action reporting. Phoenix and Palantir Mobile are plug-in services for Gotham which are only available from Palantir Technologies; also, Palantir Technologies has made the business decision to include enterprise-wide access to these plug-in services as part of ICE's purchase of Palantir Gotham Perpetual Licenses. As HSI also already procured 56 server core perpetual licenses, these costs cannot be recouped should HSI have to compete its requirement and obtain licenses for a different software product. Nor could HSI compete its requirement for additional software licenses because Palantir has proprietary rights in the software and does not distribute or provide the underlying source code to any other vendor.

Within the services provided under Palantir's Software Maintenance as a Service, HSI receives help desk support as well as regular O&M support services. Without Palantir's O&M support, approximately 1600 HSI Special Agents and Intel analysts would lose access to one of their key intelligence gathering and intelligence evaluation tools, subjecting a wide range of agency law enforcement missions to failure. ICE does not have the in-house technical expertise to be able to provide the necessary O&M support services for FALCON. Additionally, thousands more HSI Special Agents are projected to utilize a slimmed-down, mobile version of FALCON called PGWeb. Without continued O&M support, these agents would lose access to this vital search and linkage tool and would not be able to operate these mobile versions for on-going investigations. The FALCON system houses essential, mission-supporting workflow applications for the HSI Tip Line, Undercover Operations, and Confidential Informants units. The agents and analysts who work in those three critical units would be unable to perform their daily work or would suffer major work flow slowdowns if the FALCON system were to be rendered unavailable. Although the Help Desk services could be provided by another contractor, ICE is already paying for these services through the purchase of Software Maintenance as a Service. If another vendor was contracted for the Help Desk services, the Government would be paying twice for these services. Since the Palantir software products are proprietary, Palantir has stated that only Palantir is the authorized seller and distributor of its software products and provider of any required maintenance services for its software. Palantir has also not authorized any other vendor to provide training services on Palantir or FALCON.

Therefore, HSI is seeking approval to acquire brand name licenses, operations support and maintenance, and training from Palantir as the single available source under the authority of the Multiple-Award Schedule Program.

5 Determination by the Ordering Activity Contracting Officer that the Order Represents the Best Value.

In accordance with FAR 8.404(d) Use of Federal Supply Schedules –Pricing, supplies offered on the schedule are listed at fixed prices. Services offered on the schedule are priced either at hourly rates, or at a fixed price for performance of a specific task (e.g., training, installation, maintenance, and repair). GSA has already determined the prices of supplies and fixed-price services for Palantir Software, under Palantir schedule GS-35F-0086U, to be fair and reasonable.

Therefore, ordering activities are not required to make a separate determination of fair and reasonable pricing, except for a price evaluation as required by FAR 8.405-2(d). By placing an order against a schedule contract using the procedures in FAR 8.405, the ordering activity has concluded that the order represents the best value (as defined in FAR 2.101) and results in the lowest overall cost alternative (considering price, special features, administrative costs, etc.) to meet the Government's needs.

Although GSA has already negotiated fair and reasonable pricing, the Office of Acquisition (OAQ), Information Technology Architecture and Development (ITAD) division shall seek additional discounts prior to placing an order.

Outlined below is a breakout of the pricing of each period of performance.

Base Year (9 Months) (6/14/2013-3/13/2014)						
SIN / Part Number	Description	FTEs	Unit of Measurement	Quantity	9 month rate	Total (9 Months)
132-34 / PT-PG-100001	Palantir Annual Support & Maintenance for 6/14/2013 to 3/13/2014 per installed core		EACH	56	\$21,152.34	\$1,184,531.04
Estimated Contract Total, Base Year (9 Months)						\$1,184,531.04

Option Period 1 (6/14/2014-6/13/2015)						
SIN / Part Number	Description	FTEs	Unit of Measurement	Quantity	Annual Rate	Total
132-34 / PT-PG-100001	Palantir Annual Support & Maintenance per installed core		EACH	56	\$28,203.08	\$1,579,372.48
132-33 / PT-PG-000001 (Optional CLIN)	Palantir Gotham Perpetual License, per server core		EACH	8	\$141,015.42	\$1,128,123.36
132-50 / PBT (Optional CLIN)	Palantir Bootcamp (Basic) Training, per Employee		EACH	500	\$960.72	\$480,360.00
132-50 / PWT (Optional CLIN)	Palantir Workshop (Advanced) Training, per Employee		EACH	100	\$1,548.09	\$154,809.00
ODC	Travel		NTE	1	\$250,000.00	\$250,000.00
Estimated Contract Total, Option Period 1						\$3,592,664.84

Option Period 2 (6/14/2015-6/13/2016)						
SIN / Part Number	Description	FTEs	Unit of Measurement	Quantity	Annual Rate	Total

132-34 / PT-PG-100001	Palantir Annual Support & Maintenance per installed core		EACH	64	\$28,203.08	\$1,804,997.12
132-33 / PT-PG-000001 (Optional CLIN)	Palantir Gotham Perpetual License, per server core		EACH	8	\$141,015.42	\$1,128,123.36
132-50 / PBT (Optional CLIN)	Palantir Bootcamp (Basic) Training, per Employee		EACH	500	\$960.72	\$480,360.00
132-50 / PWT (Optional CLIN)	Palantir Workshop (Advanced) Training, per Employee		EACH	100	\$1,548.09	\$154,809.00
ODC	Travel		NTE	1	\$250,000.00	\$250,000.00
Estimated Contract Total, Option Period 2						\$3,818,289.48

Option Period 3 (6/14/2016-6/13/2017)						
SIN / Part Number	Description	FTEs	Unit of Measurement	Quantity	Annual Rate	Total
132-34 / PT-PG-100001	Palantir Annual Support & Maintenance per installed core		EACH	72	\$28,203.08	\$2,030,621.76
132-33 / PT-PG-000001 (Optional CLIN)	Palantir Gotham Perpetual License, per server core		EACH	8	\$141,015.42	\$1,128,123.36
132-50 / PBT (Optional CLIN)	Palantir Bootcamp (Basic) Training, per Employee		EACH	500	\$960.72	\$480,360.00
132-50 / PWT (Optional CLIN)	Palantir Workshop (Advanced) Training, per Employee		EACH	100	\$1,548.09	\$154,809.00
ODC	Travel		NTE	1	\$250,000.00	\$250,000.00
Estimated Contract Total, Option Period 3						\$4,043,914.12

Option Period 4 (6/14/2017-6/13/2018)						
SIN / Part Number	Description	FTEs	Unit of Measurement	Quantity	Annual Rate	Total
132-34 / PT-PG-100001	Palantir Annual Support & Maintenance per installed core		EACH	80	\$28,203.08	\$2,256,246.40
132-33 / PT-PG-000001 (Optional CLIN)	Palantir Gotham Perpetual License, per server core		EACH	8	\$141,015.42	\$1,128,123.36

132-50 / PBT (Optional CLIN)	Palantir Bootcamp (Basic) Training, per Employee		EACH	500	\$960.72	\$480,360.00
132-50 / PWT (Optional CLIN)	Palantir Workshop (Advanced) Training, per Employee		EACH	100	\$1,548.09	\$154,809.00
ODC	Travel		NTE	1	\$250,000.00	\$250,000.00
Estimated Contract Total, Option Period 4						\$4,269,538.76
Estimated Contract Total, Base and all Option Periods						\$16,908,938.24

An evaluation of current support & maintenance pricing on Contract HSCETC-13-F-00010 has shown that the estimated support & maintenance pricing outlined above is fair and reasonable. Additionally, GSA has determined that the pricing outlined on Palantir's GSA Schedule 70 is fair and reasonable. Therefore, it has been determined that the pricing for each period of performance and for the overall contract period of performance (to include the option to extend services per FAR 52.217-8) has been deemed fair and reasonable.

6 Efforts to Obtain Competition and Market Research

Historically, the Government issued a Sources Sought Notice detailing program requirements for a comprehensive software solution and related support and requested that interested vendors submit technical capability documentation in response. As a result Palantir software was undertaken with the results of a fixed price award HSCETE-11-F-00125 followed by a maintenance support bridge contract award number HSCETC-13-F-00010, that was highly successful. The purpose of this limited source justification is to ensure the continuance of Palantir's software maintenance support for HSI currently in place. A sources sought notice was previously issued and determined that Palantir is the sole source for the proprietary software outlined in the document.

Market research revealed that Palantir is the Original Equipment Manufacturer (OEM) and owner of the source code information of the original Palantir licenses being utilized by ICE. Palantir is the only manufacturer that can provide the required annual maintenance support for these licenses. Palantir is not sold by third party resellers; therefore does not offer any additional discounts or special pricing through third party resellers.

The market research techniques used included:

- Reviewed internal ICE documentation (previous contract, PWS, and market research)
- Researched to see if other Federal Agencies used the same system we did. It was determined that CBP and the FBI use FALCON
- Internet research of products, standards, and industry practices (Google, DHS sites)
- O&M support for services to an installation of Palantir Government Licenses

- Researched the General Services Administration (GSA) e-Library

In accordance with FAR 5.201, OAQ will synopsise this requirement to the Federal Business Opportunities (FBO) website, which is the Government-wide Point of Entry (GPE).

7 Other Facts Supporting Limited Source Justification

Palantir enables ICE/HSI to secure information sharing with other law enforcement agencies in real-time to include Transportation Security Administration (TSA), Custom & Border Protection (CBP), the United States Coast Guard (USCG), Federal Bureau of Investigations (FBI), National Counterterrorism Center (NCC), Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA). This will give ICE an open platform that will be interoperable and have the ability to cross use capabilities such as federated search, mapping and geospatial capability, unstructured search function, visual linking with these agencies and also have the capability to fully scale the solution to enable large entity exchange (e.g., petabytes of data) between other agencies.

Several other Government agencies including the Department of Defense (DOD), United States Army, Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) use Palantir software for a seamless integration of structured and unstructured data, advanced searching and discovery capabilities, enterprise-wide common operating picture capability, and enterprise-wide collaboration. This ability gives our agents and analysts the ability to conduct consolidated searches and perform quantitative analytics.

8 Statement of Actions

In order to meet the mission needs of HSI, ICE needs to retain the Palantir capabilities by potentially expanding the functionality and user base of the product.

It is the Government's intention to eventually develop the in-house capability to provide user consultative support, deliver new user training and extend solution integration independently beyond the life of the contract. This training will involve users and technicians at all levels, to include advanced "train the trainer" and "train the developer" education of ICE agents and analysts. While this will limit ICE's reliance on contractor support to some extent, product maintenance support will continue to be available only from the vendor. ICE/HSI/MS/LESIM shall continue to monitor available software products and review HSI operating procedures to determine if any additional software products become available that more effectively and efficiently meet functional requirements.

9 CERTIFICATIONS

In accordance with FAR 8.404 and FAR 8.405-6, the signatures below certify that a task order resulting from this LSJ represents the best value and results in the lowest overall price alternative to meet the Government's needs.

Requirements/Technical Personnel:

Andrew Fox
Contracting Officer Representative

Date

Contracting Officer:

This justification is accurate and complete to the best of my knowledge and belief.

Harold J Honegger
Contracting Officer

Date

REVIEW:

M L McDaniel
Deputy Assistant Director

Date

REVIEW:

David Sander
Acting Competition Advocate
[Required for actions over \$650,000
but not exceeding \$12.5 million]

Date

APPROVAL:

Cheryl Tyner
Acting Head of Contracting Activity
[Required for actions over \$12.5 million]

Date



**U.S. Immigration
and Customs
Enforcement**

For Official Use Only

FALCON OPERATIONS & MAINTENANCE SUPPORT Performance Work Statement

July ~~29~~, 2013

Homeland Security Investigations (HSI)

Mission Support



**Homeland
Security**

Page 1891

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1892

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1893

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1894

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1895

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1896

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1897

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1898

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1899

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1900

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1901

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1902

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1903

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1904

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1905

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1906

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1907

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1908

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1909

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1910

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1911

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1912

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1913

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1914

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1915

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1916

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1917

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1918

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1919

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1920

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1921

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1922

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1923

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1924

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1925

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1926

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1927

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1928

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1929

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1930

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 1931

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act



U.S. Immigration
and Customs
Enforcement

~~For Official Use Only~~

FALCON OPERATIONS & MAINTENANCE SUPPORT Performance Work Statement

July 22, 2013

Homeland Security Investigations (HSI)

Mission Support



Homeland
Security

FALCON (Palantir Government) System Operations & Maintenance Support Services
Performance Work Statement

1.0 PROJECT TITLE

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

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. FALCON is HSI's implementation of a commercial, off-the-shelf (COTS) product, Palantir Government (aka Gotham). It provides HSI's agents and analysts with a key investigative resource: a wholly integrated, consolidated platform performing federated search, analytics, geospatial referencing, reporting and situational awareness capabilities across a broadly diverse universe of structured and unstructured law enforcement data residing in numerous, disparate source environments.

The FALCON system is comprised of several sub-components. The largest of these is FALCON-SA (Search and Analysis), used by the entire community of FALCON users. FALCON also provides a hosting environment for several specialized workflow applications, which are limited to specific subsets of the user community; these include FALCON-Tip Line (the workflow application for employees of the HSI Tip Line Unit), FALCON-UC Ops (the workflow application for employees of the HSI Undercover Operations Unit), and FALCON-CI (the workflow application for employees of the HSI Confidential Informants Unit).

The base Period of Performance for this contract will entail the integration of a new extension to FALCON's existing front-end interface, FALCON-DARTTS (Data Analysis and Research for Trade Transparency System), which will replace a stand-alone, legacy system, DARTTS, currently used by the Trade Transparency Unit (TTU) of ICE. This extension of FALCON's existing front-end interface will act as a workflow management module which will support the management and sharing of information regarding international trade transactions; it will allow employees of the TTU and their foreign partners to analyze trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other

import-export crimes. HSI Agents and analysts assigned to the TTU must understand the relationship between importers and exporters and the financing for a set of trade transactions to determine which transactions are suspicious and warrant investigation. FALCON-DARTTS will be specifically designed to make this investigative process more efficient by automating the analysis and identification of anomalies for the investigator.

3.0 SCOPE

Current and future releases of FALCON are required to have System Maintenance and Services support for the purpose of applying adaptive, perfective and corrective maintenance to the application as well as operating and maintaining the FALCON infrastructure, authoring and delivering training, supporting the end user community and delivering small-to medium-scale enhancements to the existing application.

(b)(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

FALCON Operations & Maintenance Support

Performance Work Statement

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)
 - Guidelines
 - Special Publications
 - 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 General Services Administration (GSA) Schedule 70 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:
 - simple requests such as password resets and account unlocks
 - basic network and application troubleshooting
 - application usage and operational feature questions and issues;
- Monitoring the tickets created to ensure users are updated on tickets' status and progress;
- Providing reports to ICE management and System / Application Program Management as required or requested.

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

At the governments 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

FALCON Operations & Maintenance Support

Performance Work Statement

and the COR will come to mutual agreement over which changes to the system constitute SCRs, as opposed to every day System Tuning (Section 5.2.3) and System Administration (Section 5.2.4) actions not requiring the SCR process.

- All maintenance activities that reach this level shall have an SCR opened and be reported using Atlassian Jira;
- SCRs will be prioritized and agreed to by the authorized government personnel and entered into the ICE approved management tracking tool. SCRs will be approved in writing by the government;
- Prior to commencing a system modification, the Contractor and the Office of the Chief Information Officer (OCIO) Information Technology (IT) project manager shall agree on the degree of the modification as minor, moderate, or major (see table below for classification);
- The Contractor shall 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 and shall fall under Section 5.5 Optional System Enhancement Support.

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

FALCON Operations & Maintenance Support
Performance Work Statement

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	2

SCRs for FALCON may include requirements analysis, design, development, integration & testing, and implementation, including any updates needed to product documentation. Typically, these activities involve the development of Palantir helper applications, interfacing programs communicating with FALCON via the common operating APIs and the mapping and integration of additional data sources.

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

Table 2. FALCON System Hardware

(b)(7)(E)

(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

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

5.2.3 Operational Support – System Tuning

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

5.2.4 Operational Support – System Administration

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

5.3 Configuration Management

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

5.4 Training Support Included in Operations and Maintenance Services

The Contractor shall maintain and update training materials to include User Guides, Training Plans, and System Administration and Operations Manuals when an enhancement, or other significant Software O&M release, occurs. The Contractor shall provide an electronic copy of all training material. The Contractor shall also coordinate with and FALCON PMO and IPT to insure that all members understand the updates to the application. The Contractor shall provide training to Special agents and analyst groups meeting the established, written criteria for successful Strategic training classes as approved by the FALCON PMO and agreed to by the Contractor, to include such services as classroom training, desk-side support of individual ICE Agents, Special Agents, Group Supervisors, or other employees involved in directly supporting active investigations, or small groups of such employees (6 or fewer), with desk-side support training pursued on a strategic basis targeting only users with a clear, operational use for the Palantir/FALCON system. Additionally, Contractor staff will work with the Office of Training Development (OTD) and Federal Law Enforcement Training Center (FLETC) staff to productively include Palantir/FALCON training in their regular programs as requested. There is no explicit training goal by user count. While the above specified training is included in O&M, any significant expansion beyond the Strategic Training program, or any broad solicitation of new training requests across substantially the whole of ICE's organization must be discussed and agreed to with the Contractor staff to avoid logistically, or financially prohibitive training commitments.

5.5 Optional Software Enhancement Support

In the event that the hour estimate for an individual SCR is identified as exceeding 250 hours, the Contractor may be tasked to develop additional IT solutions as components of the current application via task order modification. This is an optional requirement, not to be

priced at this time, as the actual requirements for this type of work are not known at this time. The Contracting Officer will request a proposal regarding such a SCR when this task is utilized. Should a major SCR result in a feature change or enhancement which the Contractor will then offer to other customers of their Gotham product as part of Gotham's included/core functionality, the Contractor will absorb the cost of this SCR; the government will not be charged for the labor hours expended.

5.6 Optional Classroom Training

As requests for either Palantir Bootcamp Training or Palantir Workshop Training are made, 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.

5.7 Optional Palantir Gotham Appliance Cores

If called upon, the Contractor shall propose additional Palantir Gotham Appliance cores to meet customer specifications. This includes Palantir Phoenix functionality, and Palantir Mobile functionality. Pricing will be based on the software line items in Palantir's GSA Schedule 70 Pricing. If the proposal is approved by the FALCON PMO and the COR, the additional Gotham cores will be put into production, and a change order will be definitized on the task order within 2 weeks.

5.8 Conversion of Legacy DARTTS to FALCON-DARTTS

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

(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.
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.

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	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.
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) (Software includes updates/new versions of the primary Gotham platform; new workflow applications and updated versions of existing workflow applications; data ingestions; and customized versions of Gotham Mobile and the Phoenix and Raptor plug-ins)	As Required	Electronic copy - PM, Electronic Library Management System (ELMS) Software (SW): ICE source control repository (Subversion); OCIO representative on FALCON PMO (either (b)(6);(b)(7) 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

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

(b)(7)(E)

FALCON Operations & Maintenance Support
Performance Work Statement

(b)(7)(E)

DHS Enterprise Architecture Compliance

(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 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.

FALCON Operations & Maintenance Support
Performance Work Statement

Items of GFE which are inventoried and tracked in Sunflower include the following twelve laptops and two Blackberry handheld devices:

(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.

13.0 SECURITY

Contractor personnel performing work under this task order may be required to obtain a security clearance. Levels of security may range from Sensitive but Unclassified (SBU) to Secret and Top-Secret, or the handling of Secret Compartmentalized Information (SCI), dependent upon whether specific efforts conducted during the duration of the contract include establishing and managing a classified FALCON instance in addition to the current unclassified environment. The security level required will be specified in the task order.

13.1 Section 508 Compliance

If applicable, Section 508 compliance information on the services in this task order is available in Electronic and Information Technology (EIT) at the following website:
<http://www.section508.gov/>. Please reference Section 3.10, Attachment #3 of RFQ # HSCETC-11-Q-00017.

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 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

FALCON Operations & Maintenance Support
Performance Work Statement

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.

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
AIDW	Automated Information Data Warehouse
AJAX	Asynchronous Java and XML
API	Application Programming Interface
C&A	Certification and Accreditation
CCB	Change Control Board
CFR	Code of Federal Regulation
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
EIT	Electronic and Information Technology
EIU	Executive Information Unit
ELMS	Electronic Library Management System
ENFORCE	Enforcement Case Tracking System
EOD	Entry on Duty
ETL	Extract, Transfer and Load
E-VERIFY	Eligibility Verification

FALCON Operations & Maintenance Support
Performance Work Statement

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
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
KITE	Palantir Data Ingestion
LECAD	Law Enforcement Centralized Access Development
LEISS	Law Enforcement Information Sharing System
LESC	Law Enforcement Support Center
LPR	Lawful Permanent Residents
MCC	Mobile Command Center
MD	Management Directive

FALCON Operations & Maintenance Support
Performance Work Statement

MS	Microsoft
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
PCN	Potomac Center North
PCTS	Parole Case Tracking System
PHOENIX	Palantir Big Data Platform
PM	Program Manager
PMO	Program Management Office
PMP	Project Management Professional
POP	Period of Performance
PSU	Personnel Security Unit
QAP	Quality Assurance Plan
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Plan
RAPTOR	Palantir Data Index Tool
RELRES	Relationship Resolution
RFD	Request for Deviation
ROI	Records of Investigation
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCR	System Change Request
SDA	System Design Alternative
SDD	Systems Development Division
SEACATS	Seized Asset and Case Tracking System
SELC	System Enterprise Lifecycle
SEN	Significant Event Notification

FALCON Operations & Maintenance Support
Performance Work Statement

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
VPN	Virtual Private Network



FALCON New Contract Deliverables



(b)(5)



FALCON New Contract Deliverables



(b)(5)



FALCON New Contract Deliverables



(b)(5)



FALCON New Contract Deliverables



(b)(5)