Palantir

LICENSE AND SERVICES AGREEMENT

Incorporated herein is Palantir's License and Services Agreement ("Agreement"), by and between Contractor ("Palantir Technologies Inc." or "Palantir") and the ordering entity ("Customer"). This Agreement sets forth the terms and conditions pursuant to which Customer will license certain Palantir software products and contract for certain services from Palantir and pursuant to which Palantir will provide such products and services to Customer.

## PALANTIR LICENSING TERMS AND CONDITIONS

1. Certain Definitions. Capitalized terms will have the meaning indicated above unless otherwise specifically defined in these Terms and Conditions or in any Exhibits hereto.

1.1 "Palantir Gotham FFP License" means a license to the Products to be used in perpetuity on the ICE Falcon enterprise instance of Palantir for an unlimited number of server cores on the terms and subject to the conditions set forth in this Agreement and pursuant to the applicable mutually agreed upon Performance Work Statement ("PWS"). For the avoidance of doubt, the PWS takes precedence over this agreement with respect to the required scope of work.

1.2 "Product" means Palantir's proprietary commercial Palantir Gotham software product(s) specified in the Order (and any related purchase orders, statements of work, or amendments, in each case incorporated into this Agreement) or provided in connection with this Agreement.

1.3 "Upgrades" mean any helpers, extensions, plug-ins, and add-ons, in any format, including any improvements, modifications, derivative works, patches, updates, and upgrades thereto that Palantir provides to Customer or that is deployed in connection with this Agreement.

2. Grant of License. Subject to Customer's continued and full compliance with all of the terms and conditions of this Agreement, Palantir hereby grants to Customer a non-transferable, non-exclusive license, without any right to sublicense, to install, execute and use the Products and Upgrades solely for its mission-related purposes, and only (i) in accordance with the technical specification documentation provided to Customer by Palantir ("Documentation"); and (ii) on the ICE FALCON system as specified in an annual statement of work to be mutually agreed to by the parties and any modifications thereto. The annual statements of work will specify any deliverables Palantir will provide during the applicable period. For the avoidance of doubt, if the Customer declines to obtain annual support services/Operations and Maintenance ("O&M") at any time, the Customer shall have a perpetual license to the Products (as of the date annual support services/O&M terminated) in accordance with the terms and conditions of this Agreement, but Palantir shall have no further obligations to provide any additional Upgrades or O&M to Customer. Unless otherwise stated in an applicable Performance Work Statement, Customer will be responsible, at its own cost and expense, for the procurement and maintenance of all necessary hardware, including, without limitation, servers needed to fully operate and support the Product. Unless otherwise agreed to in writing by the parties in an applicable Statement of Work, database licenses are not included and Customer will be responsible for payment and licensing of any required Oracle database licenses.

3. Ownership. Except for the license rights expressly provided herein, Palantir retains all rights, title and interest in and to the Products, Upgrades, Documentation, and any other related documentation, software, or materials provided by Palantir hereunder (including, without limitation, all patent, copyright, trademark, trade secret and other intellectual or industrial property rights embodied in any of the foregoing). Customer acknowledges that it is obtaining only a limited right to the Products and Upgrades, notwithstanding any reference to the terms "purchase", "customer", or "unlimited" herein. The Products and Upgrades are licensed and not sold, and no ownership rights are being conveyed to Customer under this Agreement. Customer will maintain the copyright notice and any other notices or product identifications that appear on or in any Products and any associated media.

4. Restrictions. Customer will not (and will not allow any third party to): (i) reverse engineer or attempt to discover any source code or underlying ideas or algorithms of any Product or Upgrade (except to the extent that applicable law expressly prohibits such a reverse engineering restriction); (ii) provide, lease, lend, or otherwise use or allow others to use a Product or Upgrades for the benefit of any third party, who is not authorized by the Customer for access to the ICE FALCON system; (iii) list or otherwise display or copy any object code of any Product or Upgrade; (iv) copy any Product or Upgrade (or component thereof), except that Customer may make a reasonable number of copies of the Products and/or Documentation solely for backup, archival or disaster recovery purposes; (v) develop any

improvement, modification or derivative work thereof or include a portion thereof in any other equipment or item; (vi) for the purposes of ITAR and EAR allow the transfer, transmission, export, or re-export of any Product or Upgrade (or any portion thereof) or any Palantir technical data without a license or other authorization from the responsible United States Government export control agency where required; or (vii) perform benchmark tests without the prior written consent of Palantir (any results of such permitted benchmark testing shall be deemed Confidential Information of Palantir). Notwithstanding these restrictions, nothing shall prevent Customer from development of software that interfaces with Palantir's public Application Program Interface ("APIs"). All the limitations and restrictions on Products in this Agreement also apply to Documentation.

5. Confidentiality. To the extent allowed under applicable law (e.g. The Freedom of Information Act, 5 USC 552), Customer shall treat as confidential all Confidential Information (as defined below) of Palantir, and shall not use such Confidential Information except to exercise its rights and perform its obligations herein, and shall not disclose such Confidential Information to any third party other than disclosure on a need to know basis to a party's own advisors, attorneys, and/or bankers whom are each subject to obligations of confidentiality at least as restrictive as those stated herein. Without limiting the foregoing, Customer shall use at least the same degree of care as it uses to prevent the disclosure of its own confidential information of like importance, but in no event less than reasonable care. Customer shall promptly notify Palantir of any actual or suspected misuse or unauthorized disclosure of Palantir's Confidential Information. "Confidential Information" shall mean (i) Products and Upgrades, (ii) Documentation and (iii) any other business, technical or engineering information provided by Palantir to Customer, including third party information, disclosed by Palantir to Customer, in any form and marked or otherwise designated as "Confidential" or "Proprietary" or in any form and by the nature of its disclosure would be understood by a reasonable person to be confidential and proprietary. Notwithstanding the foregoing, Confidential Information shall not include any information that (a) is or becomes part of the public domain through no act or omission of Customer in breach of this Agreement, (b) is known to Customer at the time of disclosure without an obligation to keep it confidential, (c) becomes rightfully disclosed to Customer from another source without restriction on disclosure or use, or (d) Customer can document by written evidence that such information is independently developed by Customer without the use of or any reference or access to Confidential Information, by persons who did not have access to the relevant Confidential Information. Customer is responsible for any breaches of this Section by its employees and agents. Customer's obligations with respect to Palantir's Confidential Information survives termination of this Agreement for a period of five (5) years; *provided*, that Customer's obligations hereunder shall survive and continue in perpetuity after termination with respect to any Confidential Information that is a trade secret under applicable law.

6. Payment and Delivery. Customer shall pay Palantir the total amount set forth in the applicable Task Order. Subject to the Prompt Payment Act, 5 C.F.R. 1315, payment shall be made in the currency set forth on the invoice via check or wire transfer to an account designated by Palantir and shall be due within thirty (30) days after the date of issuance of Palantir's invoice. Products and Upgrades are deemed delivered upon Palantir's initial e-mail communication providing Customer with access to Palantir's electronic support portal, through which Customer may download Products and Documentation.

7. Operations and Maintenance Services. Subject to payment of the applicable Task Order, Palantir shall use commercially reasonable efforts to provide Customer with O&M Services (as provided for in Attachment A) in accordance with and subject to Palantir's standard O&M services terms and conditions ("O&M Services") for the period of time specified in the applicable Task Order ("O&M Services Period"). If Customer fails to pay by the end of the then-current O&M Period, Customer shall be deemed to have cancelled O&M Services and Palantir shall no longer provide Customer with O&M Services (including Upgrades) and shall have no further obligations to the Customer regarding the Palantir Gotham FFP License. Customer may reinstate O&M Services after a period in which it was cancelled, provided (i) Palantir then offers O&M Services, and (ii) in order to receive Upgrades which Customer had not received due to cancellation, Customer pays Palantir the current year's O&M Services fee and any O&M Services fees that would have been payable during the period during which O&M Services were cancelled.

8. Professional Services. In addition to the O&M Services discussed above, if specified in the applicable task order or performance work statement, Palantir may provide Customer with additional services specified thereon ("Professional Services").

9. Government Matters. The Product, Upgrades, O&M Services and Professional Services created by Palantir are "commercial items" as defined at 48 C.F.R. 2.101, consisting of commercial computer software, commercial computer software documentation and commercial services. Since Customer or end user is a U.S. governmental entity, then Customer acknowledges and agrees that its (i) use, duplication, reproduction, release, modification, disclosure, or transfer of the Products, Upgrades and any related documentation of any kind, including, without limitation, technical data and manuals, will be subject to the terms and conditions of this Agreement in accordance with Federal Acquisition Regulation ("FAR") Parts 52.212-4 and 52.227-19 as applicable; (ii) the Products, Upgrades and documentation were developed fully at private expense and (iii) all other use of the Products, Upgrades and documentation except in accordance with the license grant provided herein is strictly prohibited.

10. Term and Termination. This Agreement shall begin on the Effective Date and remain in effect for the period of time specified as set forth below or as otherwise provided for in the Order ("Term"), unless otherwise terminated as provided herein.

10.1 This Agreement will remain in effect in perpetuity, including in the event Palantir is subject to a change in ownership through acquisition, merger, or any other corporate event, unless otherwise terminated as provided herein. This Agreement may be terminated by Customer without cause upon at least thirty (30) days prior written notice to Palantir.

10.2 Termination or expiration does not affect either party's rights or obligations that accrued prior to the effective date of termination or expiration (including without limitation, payment obligations). Sections 3, 4, 5 (but only for the period of time specified therein), 6, 9, 10.2, 10.3, 11, 12.2, 13 and 14 shall survive any termination or expiration of this Agreement. Termination is not an exclusive remedy and all other remedies will remain available.

11. Indemnification. Palantir shall indemnify and hold harmless Customer from and against damages, costs, and attorneys' fees, if any, finally awarded against Customer from any claim of infringement or violation of any U.S. patent, copyright, or trademark asserted against Customer by a third party based upon Customer's use of the Products in accordance with the terms of this Agreement, provided that Palantir shall have received from Customer: (i) notice of such claim within twenty (20) days of Customer receiving notice of such claim. For the avoidance of doubt, the US Government attorneys shall solely control any litigation covered under this clause. If Customer's use of any of the Products are, or in Palantir's opinion is likely to be, enjoined due to the type of infringement specified above, or if required by settlement, Palantir may, in its sole discretion: (a) substitute for the Products substantially functionally similar programs and documentation; (b) procure for Customer the right to continue using the Products; or (c) if Palantir reasonably determines that options (a) and (b) are commercially impracticable, terminate this Agreement and refund to Customer for Palantir licenses, the license fee paid hereunder by Customer as reduced to reflect a four-year, straight-line amortization from the date on which such Products were first delivered by Palantir, or, Palantir Cloud and Term licenses, refund to Customer a pro-rated portion of the license fee paid that reflects the remaining portion of the Term at the time of termination. The foregoing indemnification obligation of Palantir shall not apply: (1) if the Products are modified by any party other than Palantir, but only to the extent the alleged infringement would not have occurred but for such modification; (2) if the Products are modified by Palantir at the request of Customer, but only to the extent the alleged infringement would not have occurred but for such modification; (3) if the Products are combined with other non-Palantir products or processes not authorized by Palantir, but only to the extent the alleged infringement would not have occurred but for such combination; (4) to any unauthorized use of the Products; (5) to any superseded release of the Products if the infringement would have been avoided by the use of a current release of the Products that Palantir has provided to Customer prior to the date of the alleged infringement; or (6) to any third party software code contained within the Products. THIS SECTION SETS FORTH PALANTIR'S SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

12. Palantir Limited Warranty and Disclaimer.

12.1 In addition to any warranties or obligations included in the PWS, Palantir warrants for a period of one hundred twenty days (120) days from the date the initial Products were delivered by Palantir, the Products will substantially conform to Palantir's then current Documentation for such Products. This warranty covers problems reported to Palantir in writing (including a test case or procedure that recreates the failure and by full documentation of the failure) during the warranty period. In the event of a failure of the Products to perform substantially in accordance with the specifications during the warranty period ("Defect"), Palantir shall use reasonable efforts to correct the Defect or provide a suitable work around as soon as reasonably practical after receipt of Customer's written notice as specified above. A Defect shall not include any defect or failure attributable to improper installation, operation, misuse or abuse of the Products or any modification thereof by any person other than Palantir. If Palantir has not remedied the Defect within thirty (30) days of its receipt of Customer's written notice, Customer may give Palantir written notice of termination of this Agreement, which termination will be effective ten (10) days after Palantir's receipt of the notice, unless Palantir is able to remedy the Defect prior to the effective date of termination. In the event of the termination of this Agreement pursuant to Customer's exercise of its right under this Section, Customer shall be entitled to receive from Palantir, as its sole and exclusive remedy, a refund of all amounts paid to Palantir hereunder.

12.2 ALL SALES ARE FINAL. NO PURCHASES OF PRODUCTS ARE REFUNDABLE, EXCHANGEABLE OR OFFSETTABLE EXCEPT AS SET FORTH IN SECTION 12.1. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 12.1 of this Agreement, THE PRODUCTS AND SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY OTHER WARRANTIES OF ANY KIND AND PALANTIR AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, ORAL OR WRITTEN, RELATING TO THE PRODUCTS AND ANY SERVICES PROVIDED HEREUNDER OR SUBJECT MATTER OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, TITLE OR FITNESS FOR A PARTICULAR PURPOSE. .

13. Limitations of Liability.

13.1 EXCEPT FOR ANY AMOUNTS AWARDED TO THIRD PARTIES ARISING UNDER SECTION 11 OF THIS AGREEMENT, AND EXCEPT FOR BODILY INJURY, TO THE

MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, PALANTIR SHALL NOT BE LIABLE TO CUSTOMER OR TO ANY THIRD PARTY WITH RESPECT TO ANY PRODUCT, SERVICE OR OTHER SUBJECT MATTER OF THIS AGREEMENT FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF USE, LOSS OR ALTERATION OF DATA, COST OF REPLACEMENT, DELAYS, LOST PROFITS, OR SAVINGS ARISING OUT OF PERFORMANCE OR BREACH OF THIS AGREEMENT OR THE USE OR INABILITY TO USE THE PRODUCTS, OR FOR ANY MATTER BEYOND PALANTIR'S REASONABLE CONTROL, EVEN IF SUCH PARTY HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Contract under any federal fraud statue, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

13.2 EXCEPT FOR ANY AMOUNTS AWARDED TO THIRD PARTIES ARISING UNDER SECTION 11 OF THIS AGREEMENT, AND EXCEPT FOR BODILY INJURY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY AGREES THAT THE MAXIMUM AGGREGATE LIABILITY OF PALANTIR ON ANY CLAIM OF ANY KIND, WHETHER BASED ON CONTRACT, TORT (INCLUDING BUT NOT LIMITED TO, STRICT LIABILITY, PRODUCT LIABILITY OR NEGLIGENCE) OR ANY OTHER LEGAL OR EQUITABLE THEORY OR RESULTING FROM THIS AGREEMENT OR ANY PRODUCTS OR SERVICES FURNISHED HEREUNDER SHALL NOT EXCEED THE SUMS PAID TO PALANTIR BY CUSTOMER HEREUNDER. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Contract under any federal fraud statue, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

14.Miscellaneous. Neither this Agreement nor the licenses granted hereunder are assignable or transferable by Customer; any attempt to do so shall be void. Palantir may assign this Agreement in whole or in part with notice to and approval of the Customer. Any notice, report, approval or consent required or permitted hereunder shall be in writing and sent by first class U.S. mail, confirmed facsimile, a U.S. government email system with Read Receipt or major commercial rapid delivery courier service to the address specified in the Order. If any provision of this Agreement shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and be enforceable. Any and all modifications, waivers or amendments must be made by mutual agreement and shall be effective only if made in writing and signed by each party. No waiver of any breach shall be deemed a waiver of any subsequent breach. Customer's obligations under this Agreement are subject to compliance with all applicable export control laws and regulations. This Agreement is incorporated into the Government contract documents. Palantir is in no way affiliated with, or endorsed or sponsored by, The Saul Zaentz Company d.b.a. Tolkien Enterprises or the Estate of J.R.R. Tolkien.

## Attachment A- PALANTIR O&M/SUPPORT SERVICES

1a. For the avoidance of doubt, this Attachment A supplements the PWS O&M requirements, and does not replace it. The services referenced herein are provided by Palantir's general technical support team, which supplement the O&M provided by Palantir under the ICE PWS.

1b. SUPPORT SERVICES. Support Services consist of (a) Error Correction and Technical Support provided to the Customer's technical support contact concerning the installation and use of the then-current release of the applicable Product and the Previous Sequential Release and (b) Product Major Releases that Palantir in its discretion makes generally available without additional charge to a Customer that is up to date on all fees due under its current License and Services Agreement (any such update will be subject to the Agreement as though it were the applicable Product).

2. ERROR PRIORITY LEVELS. Palantir shall exercise commercially reasonable efforts to correct any Error reported by Customer in the current unmodified release of Product in accordance with the priority level reasonably assigned to such Error by Palantir.

- P0 Errors - Palantir shall promptly commence the following procedures: (i) assigning Palantir engineers or other Palantir-trained personnel to correct the Error(s); (ii) notifying Palantir management that such Errors have been reported and of steps being taken to correct such Error(s); (iii) providing Customer with periodic reports on the status of the corrections; (iv) initiating work to provide Customer with a Hotfix; and (v) if appropriate, providing Palantir engineers or other trained personnel, on site at Customer's facilities.
- P1 Errors - Palantir shall promptly commence the following procedures: (i) assigning Palantir engineers or other Palantir-trained personnel to correct the Error; (ii) notifying Palantir management that such Errors have been reported and of steps being taken to correct such Error(s); (iii) providing Customer with periodic reports on the status of the corrections; (iv) initiating work to provide Customer with a Hotfix; and (v) if appropriate, providing Palantir engineers or other trained personnel on site at Customer's facilities.
- P2 Errors - Palantir may include the Fix for the Error in the next Major Release.
- P3 Errors - Palantir may include the Fix for the Error in the next Major Release.

3. RESPONSE TIMES. Palantir will use diligent efforts to meet the following response times:

| Severity | Response Time | Targeted Resolution Service Level |
|---|---|---|
| **P0** | **12 clock hours, 365 days a year** | **Onsite if appropriate within 24 clock hours of issue until Error is resolved** |
| **P1** | **12 Business Hours** | **Onsite if appropriate within 36 business hours of issue until Error is resolved** |
| **P2** | **24 Business Hours** | **Error resolved with Major Release** |
| **P3** | **60 Business Hours** | **Error resolved at Palantir's discretion** |

4. EXCLUSIONS. Palantir shall have no obligation to support: (i) altered or damaged Product or any portion of a Product incorporated with or into other software; (ii) Product that is not the then-current release or immediately Previous Sequential Release; (iii) Product problems caused by Customer's negligence, abuse or misapplication, use of Product other than as specified in the Palantir's user manual, or other causes beyond the control of Palantir; (iv) Product installed on any hardware that is not supported by Palantir; or (v) any Product for which Palantir has released a Hotfix or Major Release that has not been implemented by Customer within six (6) months after the date first made available by Palantir. Palantir shall have no liability for any changes in Customer's hardware which may be necessary to use Product due to a Workaround or maintenance release.

5. CUSTOMER OBLIGATIONS. As a prerequisite to Palantir's obligations hereunder, Customer agrees to the following obligations.

In addition, this support team must be generally available and able to collect data and report it back to Palantir within 24 to 48 hours of requests made by Palantir.

5.1 Customer will back up Palantir files and associated databases regularly.

5.2 Customer will follow the Upgrade Guide and other instructions provided by Palantir when upgrading Product.

5.3 Customer will test Major Releases, Minor Releases and Hotfixes in a staging environment before deploying the Major Release, Minor Release or Hotfix to a production environment.

6. DEFINITIONS.

- "Business Hours" means hours occurring during the period of each day in which Palantir offers Support Services, 8 A.M.-4 P.M. Pacific Time.
- "Error" means an error in a Product that is reproduced by Palantir and which significantly degrades such Product as compared to the Palantir's published performance specifications.
- "Error Correction" means the use of reasonable commercial efforts to correct Errors.
- "Fix" means the repair or replacement of object or executable code versions of a Product to remedy an Error.
- "Hotfix" means a single, cumulative package that includes one or more files containing Fixes or Workarounds that are used to address P0 or P1 Errors. "Hotfixes" address a specific customer situation and may not be distributed outside the customer organization.
- "Major Release" means a Product update that represents incremental improved features, functionality, and usability and is released during the normal course of development. An update is indicated as an increment to the major version number in the software (version 1.2 can be updated to version 1.3).
- "Previous Sequential Release" means the release of a Product which has been replaced by a subsequent release of the same Product. Notwithstanding anything else, a Previous Sequential Release will be supported by Palantir only for a period of twelve (12) months after release of the subsequent release.
- "P0 Error" means an Error which renders a Product inoperative or causes such Product to fail catastrophically.
- "P1 Error" means an Error which substantially degrades the performance of a Product or materially restricts Customer's use of such Product.
- "P2 Error" means an Error which causes only a minor impact on the Customer's use of Product functionality.
- "P3 Error" means an Error which causes only a very minor impact on the Customer's use of a Product, such as documentation typos or handled error messages.
- "Support Services" means Palantir support services as described in Section 1.
- "Technical Support" means technical support assistance provided by Palantir via email, telephone or other means provided by Palantir in its discretion to the Technical Support Contact during Palantir's normal business hours concerning the installation and use of the then current release of a Product and the Previous Sequential Release.
- "Upgrade Guide" means the documentation provided by Palantir specifying appropriate procedure for upgrading Product.
- "Workaround" means a change in the procedures followed or data supplied by Customer to avoid an Error without substantially impairing Customer's use of a Product.

THESE TERMS AND CONDITIONS CONSTITUTE A SERVICE CONTRACT AND NOT A PRODUCT WARRANTY. ALL PRODUCTS AND MATERIALS RELATED THERETO ARE SUBJECT EXCLUSIVELY TO THE WARRANTIES SET FORTH IN THE AGREEMENT. THIS ATTACHMENT IS AN ADDITIONAL PART OF THE AGREEMENT AND DOES NOT CHANGE OR SUPERSEDE ANY TERM OF THE AGREEMENT EXCEPT TO THE EXTENT UNAMBIGUOUSLY CONTRARY THERETO.

U.S. Immigration and Customs Enforcement

~~For Official Use Only~~

# FALCON OPERATIONS & MAINTENANCE SUPPORT & SYSTEM ENHANCEMENT

(b)(4)

## 5/14/2015 – 5/13/2016

*(Performance Work Statement Appendix B)*

*May11, 2015*

Homeland Security Investigations (HSI)

Mission Support

Homeland Security

# (b)(4) – FALCON OPERATIONS & MAINTENANCE SUPPORT & SYSTEM ENHANCEMENT Contract

## (Appendix B)

## Period of Performance - 5/14/2015-5/13/2016

### 1.0 BACKGROUND

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

During the twelve-month period 5/14/2015 to 5/13/2016, or longer if mutually agreed to by the parties, the Contractor shall perform development, integration, and training services for the following projects, which are not presented in priority order. The parties shall mutually agree to the list priorities and project timelines.

### 2.0 PROJECT PLANS AND SCHEDULES

The Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten work days after the beginning of a contract year a (b)(4) listing the planned start dates of (b)(4) Based upon this (b)(4) (b)(4) the Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten working days prior to the initiation of work on a (b)(4) (b)(4) a Project Plan and a Project Schedule. The one exception shall be for the (b)(4) for which a Project Plan and a Project Schedule shall be delivered by the Contractor concurrently with delivery of the (b)(4)

Project Plans, mutually agreed to by HSI and the Contractor, shall identify specific user groups, workflows and discrete tasks. The Project Plans will define the (b)(4) (b)(4) – any and all changes to the Project Plans must be mutually agreed upon by the parties and documented in weekly and/or monthly reports. Specifically, any addition of a new task within the Project Plan must be mutually agreed upon by the parties, and counterbalanced with the deletion or delay of an existing task of equal effort, as documented in weekly and/or monthly reports. Project Schedules shall list high-level tasks for (b)(4) Project Plans and Schedules may be amended by the two parties' mutual agreement.

### 3.0 PROJECT MANAGEMENT

As part of the Draft Project Plan for (b)(4) Contractor shall identify a project lead, who will (a) coordinate all Contractor work on that (b)(4) (b)(4) (b) manage the Project Plan and Project Schedule; and (c) report on progress and achievement of project milestones at weekly meetings with the FALCON PMO Team and to

inquiries made by the FALCON Program Manager or other HSI authorities. At the Contractor's discretion, a particular employee may be assigned as project lead for more than (b)(4) (b)(4)

In addition to weekly progress meetings, the Contractor shall provide (a) quarterly briefings at the Unit Chief level and (b) twice yearly briefings to the Executive Steering Committee on progress and achievement of project milestones (b)(4)

The FALCON Program Manager shall identify a governmental project lead for (b)(4) (b)(4) This governmental project lead will (a) identify governmental Subject Matter Experts (SMEs) as necessary for requirements gathering, user feedback, and user testing; (b) facilitate meetings between governmental SMEs and Contractor staff; (c) coordinate agreements between the FALCON PMO and other bodies within ICE or other governmental agencies required for exchanges of data necessary for the accomplishment of the (b)(4) (b)(4); (d) review/approve all changes to the Project Plan and/or Project Schedule proposed by the Contractor; and (d) alert the FALCON Program Manager and the FALCON COR/ACOR whenever schedule breeches are anticipated to occur or other problems arise which may adversely impact either project quality or the achievement of project deadlines.

All training activities conducted in support of (b)(4) must be coordinated, in advance, with the FALCON Program Management Office (PMO).

## 4.0 LIST OF (b)(4)

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

Page 010 of 101

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

## 5.0 ESCALATION

At the beginning of each year of contract performance, the AD and DAD over the FALCON program, with the input of the ESC and of the Contractor will agree upon the addition of (b)(4) (b)(4) to be completed during the upcoming year (b)(4) may be higher if both parties agree). If ICE and the Contractor are unable to agree upon (b)(4) (b)(4) the Contractor will provide a detailed technical rationale as to why (b)(4) falls outside the scope of PWS. This written rationale shall include the level of effort and why this level of effort is not attainable and shall be presented to the ICE FALCON Program Manager and COR/ACOR within five (5) business days of the Contractor's initial announcement of lack of agreement on (b)(4) In this scenario, HSI management and the Contractor's management will use this information to reach a final agreement on the (b)(4) Contractor will provide the implementation support for all tasks listed in an (b)(4) to which both HSI and the Contractor agree.

Should the provision by the Contractor of a technical rationale for the non-feasibility of an (b)(4) fail to result in agreement between HSI management and the Contractor's management on the contents of the (b)(4) either party may request adjudication from the assigned ICE Contracting Officer (CO), who shall make a determination within five (5) business days of receipt of the adjudication request as to whether or not the

(b)(4) shall be included in the (b)(4) In the event that HSI's priorities change during the period of time covered by a (b)(4) and HSI requests that the (b)(4) be amended, and the Contractor determines that this new request for work does not clearly fall within the scope of the (b)(4) (b)(4) the Contractor may present the change request to the CO, who shall review the request to determine whether HSI's request falls within the scope of that document. Such determinations must be made within five (5) business days of the escalation request. The Contractor will not be obligated to take any action on the new request for work unless and until the CO, in coordination with the Contractor, approves the request and determines that such request falls within the scope of an (b)(4) or otherwise amends such document to include the new request for work. In the event the CO and Contractor are unable to reach an agreement, the matter will be referred to ICE's Head of Contracting Authority (HCA) for final adjudication. For any priority tasks outside the scope of the existing (b)(4) HSI may request a level of effort from Contractor; Contractor shall not be obligated to perform such tasks unless (i) the task consists of high priority case work and is specifically requested by the Executive Assistant Director of HSI (or his/her designee); and (ii) a required task of a comparable level of effort is explicitly postponed or eliminated.

Changes to the (b)(4) shall be incorporated into the contract through bilateral modification.

U.S. Immigration and Customs Enforcement

~~For Official Use Only~~

# FALCON OPERATIONS & MAINTENANCE SUPPORT & SYSTEM ENHANCEMENT

# Performance Work Statement

*May 11, 2015*

Homeland Security Investigations (HSI)

Mission Support

Homeland Security

## FALCON System Operations & Maintenance Support Services and System Enhancement

### 1.0 PROJECT TITLE

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

### 2.0 BACKGROUND

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

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

In order to support current and future system maintenance and system enhancement needs, ICE HSI has purchased from Palantir Technologies, Inc., beginning as of September 22, 2014. This is a (b)(4) which requires the Contractor to provide ICE with:

- Include provisions for mutually agreed upon projects through bi-lateral modification of the contract (the inclusion of the (b)(4) within the PWS), i.e.: migration of Telecommunications Linking System (TLS) off of the TECS Mainframe into a FALCON supported system;
- Increase FALCON Mobile users;
- During the initial Period of Performance (POP) and option years 1-2, adding up to (b)(4) (b)(4) aligned with HSI's (b)(4) (the (b)(4) (b)(4) may be higher if both parties agree); the Contractor will provide the technical and implementation support for all tasks listed in (b)(4) to which both HSI and the Contractor agree; and
- Unforeseen needs could be accommodated, with a newly identified, (b)(4) (b)(4) taking the place of one of the (b)(4) (see Section 3 below which describes this process).

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

## 3.0 SCOPE

FALCON uses commercial software sold by Palantir Technologies, Inc., called Palantir

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

The initial Period of Performance (POP) of this contract will entail the completion of the migration of TLS (Telecommunications Linking System) from TECS mainframe, which is being decommissioned on September, 2015, to FALCON. Additionally, the initial POP will entail the completion of the addition of significant enhancements and new features to FALCON-DARTTS within the (b)(4) (b)(4) The initial POP and Option Years 1-2 of this contract will entail the execution of up to (b)(4) (b)(4) (b)(4) is marked by the increased ability of users to act in support of ICE's mandate and is measured by the successful (b)(4) The Assistant Director (AD) and Deputy Assistant Director (DAD) over the FALCON program and the Contractor will agree upon five outcomes at the beginning of each contract year, with the input of the Executive Steering Committee (ESC). (b)(4) (b)(4) represent major projects. (b)(4) (b)(4) which can include but are not limited to additional feature roll out, implementation and documentation of new workflows, targeted trainings, and the integration of new data sets. The Contractor will ensure that these data sets, if not directly ingested within the FALCON system, can be remotely accessed and searched by users of the FALCON system, and that end users will not experience any significant degradation of performance while searching/manipulating data accessed remotely versus searching/manipulating data ingested directly into the FALCON system.

At the beginning of each year of contract performance, the AD and DAD over the FALCON program, with the input of the ESC and of the Contractor will agree upon the (b)(4) (b)(4) to be completed during the upcoming year (b)(4) may be (b)(4) ). If ICE and the Contractor are unable to agree upon the scope of a (b)(4) the Contractor will provide a detailed technical rationale as to why the (b)(4) This written rationale shall include the level of effort and why this level of effort is not attainable and shall be presented to the ICE FALCON Program Manager and COR/ACOR within five (5) business days of the Contractor's initial announcement of lack of agreement on the (b)(4) In this scenario, HSI management and the Contractor's management will use this information to reach a final agreement on the (b)(4) Contractor will provide the implementation support for all tasks listed in (b)(4) to which both HSI and the Contractor agree.

The Contractor will provide the (b)(4) shall be incorporated into the contract through bilateral modification.

Should the provision by the Contractor of a technical rationale for the non-feasibility of an (b)(4) (b)(4) to result in agreement between HSI management and the Contractor's management on the (b)(4) either party may request adjudication from the assigned

ICE Contracting Officer (CO), who shall make a determination within five (5) business days of receipt of the adjudication request as to whether or not (b)(4) s) shall be included in (b)(4) In the event that HSI's priorities change during the period of time covered by a (b)(4) and HSI requests that the (b)(4) and the Contractor determines that this new request for work does not clearly fall within the scope of the (b)(4) the Contractor may present the change request to the CO, who shall review the request to determine whether HSI's request falls within the scope of that document. Such determinations must be made within five (5) business days of the escalation request. The Contractor will not be obligated to take any action on the new request for work unless and until the CO, in coordination with the Contractor, approves the request and determines that such request falls within the scope of an (b)(4) or otherwise amends such document to include the new request for work. In the event the CO and Contractor are unable to reach an agreement, the matter will be referred to ICE's Informational Technology Division Assistant Director for final adjudication. For any priority tasks outside the scope of (b)(4) (b)(4) HSI may request a level of effort from Contractor; Contractor shall not be obligated to perform such tasks unless (i) the task consists of high priority case work and is specifically requested by the Executive Assistant Director of HSI (or his/her designee); and (ii) a required task of a comparable level of effort is explicitly postponed or eliminated.

Changes to (b)(4) shall be incorporated into the contract through bilateral modification.

## 4.0 APPLICABLE DOCUMENTS

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

- DHS Acquisition Management Directive 102-01 Handbook
- ICE Enterprise Systems Assurance Plan
- ICE System Lifecycle Management (SLM) Handbook, Version 1.4, January, 2012
- ICE Technical Architecture Guidebook
- ICE Technical Reference Model (TRM) (Standards Profile)
    - The Offeror shall identify any hardware, software, and/or licenses required for its proposed solution. The Government is prepared to provide any hardware and software items that are included within the ICE TRM that would reasonably be utilized by Offerors for the system development. Test and evaluation tools listed within the TRM are not provided as Government Furnished Equipment (GFE).
- 4300A DHS Information Security Policy
- 4300A Sensitive Systems Handbook

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

- International Information Systems Security Certification Consortium ($ISC^2$) Standards
- National Industrial Security Program Operating Manual (NISPOM), February 28, 2006
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)
    - o Guidelines
    - o Special Publications
    - o Standards
- NIST Special Publication 800-37, Guide for the Certification and Accreditation of Federal Information Systems
- Federal Information Processing Standard (FIPS) 199
- Federal Information Security Management Act (FISMA), November 22, 2002
- Federal Information Technology Security Assessment Framework (FITSAF), November 28, 2000
- Federal OMB Circular A-130, Management of Federal Information Resources
- Federal Privacy Act of 1974 (As Amended)
- Federal Records Act
- DHS 4300A, Sensitive Systems Policy Directive, Version 6.1.1, October 31, 2008
- DHS Management Directive (MD) 4300.1, Information Technology Systems Security, November 03, 2008
- DHS MD Volume 11000 – Security
- DHS Office of Chief Information Officer (OCIO) E-Government Act Report 2008

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

## 5.0 TASKS

The Contractor shall provide:

### 5.1 Tier 1 – Help Desk Support

Help Desk Support consists of the following responsibilities:

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

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

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

**Tier 2 System Maintenance and Support**

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

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

**Tier 3 - System Maintenance and Support**

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

- All maintenance activities that reach this level shall have an SCR opened and be reported using Atlassian Jira;
- SCRs will be prioritized and agreed to by the authorized government personnel and entered into the ICE approved management tracking tool. SCRs will be approved in writing by the government;
- Prior to commencing a system modification, the Contractor and the Office of the

Chief Information Officer (OCIO) Information Technology (IT) project manager shall agree on the degree of the modification as minor, moderate, or major (see table below for classification);

- The Contractor shall implement an application feedback loop, whereas systemic issues identified during common Tier 1, 2, and 3 escalation procedures are routinely evaluated and reviewed with the IT Project Manager to assess the need for a SCR in future release.
- The Contractor shall respond to all Tier 3 System Maintenance Support tickets in accordance with the contract;
- Software changes to applications are based upon the submission of an SCR, and are classified as minor, moderate, or major changes, where:

Table 1: Change Requests

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

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

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

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

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

SCRs for FALCON may include Contractor's assistance with requirements analysis for

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

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

### 5.2 Operational Support

The Contractor shall provide Operational Support for the FALCON system. Table 2 and Table 3 detail the hardware and software infrastructure currently in place for FALCON. The hardware and software listed below is subject to change based on future expansion requirements and datacenter moves as requested by FALCON PMO. PCN-Potomac Center North, 500 12th St SW, Washington, DC 20536

**Table 4. FALCON System Firmware**

| Hardware Device | Firmware | Remarks |
|---|---|---|
| | | |

Operational support shall include the activities below:

#### 5.2.1 Operational Support - Interfaces and Data Sources

The Contractor shall support interfaces that feed into and out of the FALCON System. The Contractor shall provide on-going support for all FALCON components which provide data to the tool's databases. Data currently housed within FALCON and synchronized with external 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 implementation of database scripts to update or query information in the database as required. The Contractor shall support ad-hoc queries as requested by the HSI FALCON program management office (PMO) and/or perform data analysis as requested.

### 5.2.3 Operational Support – System Tuning

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

### 5.2.4 Operational Support – System Administration

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

## 5.3 Configuration Management

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

## 5.4 Training Support Included in Operations and Maintenance Services

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

## 5.5 Support of FALCON Mobile Technology

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

(b)(7)(E)

Contractor shall have access to FALCON Mobile by March 13, 2016 and shall ensure there will be no degradation of overall system performance from current levels.

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

At the beginning of each year of contract performance, the AD and DAD over the FALCON program, with the input of the ESC and of the Contractor will agree upon the addition of (b)(4) (b)(4) to be completed during the upcoming year ( (b)(4) may be higher if both parties agree). If ICE and the Contractor are unable to agree upon the (b)(4) (b)(4) the Contractor will provide a detailed technical rationale as to why (b)(4) This written rationale shall include the level of effort and why this level of effort is not attainable and shall be presented to the ICE FALCON Program Manager and COR/ACOR within five (5) business days of the Contractor's initial announcement of lack of agreement on the (b)(4) In this scenario, HSI management and the Contractor's management will use this information to reach a final agreement on the (b)(4) Contractor will provide the implementation support for all tasks listed in (b)(4) to which both HSI and the Contractor agree.

(b)(4) shall be incorporated into the contract through bilateral modification.

The performance period of this task order may entail the integration of potentially 15 other data sets each of which must be aligned with and designated as a subtask of (b)(4) listed in the

(b)(4) agreed on by HSI management and the Contractor for inclusion in the FALCON system before those data sets may be made accessible to FALCON users. The data sets (this list is not exhaustive, as currently unforeseen needs may arise) are listed below.

(b)(7)(E)

Contingent upon the decisions of FALCON PMO and applicable ICE oversight bodies, these data sets may be directly ingested within the FALCON system or accessed from an external data store. The Contractor shall ensure that these data sets, if not directly ingested within the FALCON system, can be remotely accessed and searched by users of the FALCON system, and that end users will not experience any significant degradation of performance while searching data accessed remotely versus searching data ingested directly into the FALCON system. This performance requirement is subject to limitations imposed by the source system. (b)(4) approved by HSI management and the Contractor's management in the (b)(4) for inclusion within the FALCON system must be made accessible to end users in a Production environment by the end of the same contract Option Year in which that data set or feature was first approved, unless HSI management approves an extension into the following Option Year.

Should the optional six-month extension from March 14, 2018 to September 13, 2018 be exercised, the management of HSI and of the Contractor will agree upon (b)(4) (b)(4) to be accomplished during the six month period. If (b)(4) cannot be identified by HSI management, then an equivalent combination of smaller data sets or program enhancements shall be proposed.

### 5.6.1 Project Plans and Schedules

The Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten work days after the beginning of a contract year a (b)(4) listing the planned start dates of (b)(4) Based upon this (b)(4) the Contractor shall submit to the FALCON Program Manager and the FALCON COR/ACOR no later than ten working days prior to the initiation of work on a (b)(4) a Project Plan and a Project Schedule. The one exception shall be for the (b)(4) for which a Project Plan and a Project Schedule shall be delivered by the Contractor concurrently with delivery of (b)(4) (b)(4)

Project Plans, mutually agreed to by HSI and the Contractor, shall identify specific user groups, workflows and discrete tasks. The Project Plans will define the agreed upon (b)(4) (b)(4) – any and all changes to the Project Plans must be mutually agreed upon by the parties and documented in weekly and/or monthly reports. Specifically, any addition of a new task within the Project Plan must be mutually agreed upon by the parties, and counterbalanced with the deletion or delay of an existing task of equal effort, as documented in weekly and/or monthly reports. Project Schedules shall list high-level tasks for a (b)(4) (b)(4) Project Plans and Schedules may be amended by the two parties' mutual agreement.

### 5.6.2 Escalations / Resolutions of Disagreements Concerning Project Scope

As described in Section 5.6.1 above, at the beginning of each year of contract performance, the AD and DAD over the FALCON program, with the input of the ESC and of the Contractor will agree upon the addition of (b)(4) to be completed during the upcoming year (b)(4) . If ICE and the Contractor are unable to agree upon (b)(4) the Contractor will provide a detailed technical rationale as to why the (b)(4) This written rationale shall include the level of effort and why this level of effort is not attainable and shall be presented to the ICE FALCON Program Manager and COR/ACOR within five (5) business days of the Contractor's initial announcement of lack of agreement on (b)(4) In this scenario, HSI management and the Contractor's management will use this information to reach a final agreement on the (b)(4) (b)(4) Contractor will provide the implementation support for all tasks listed in an (b)(4) (b)(4) to which both HSI and the Contractor agree.

Should the provision by the Contractor of a technical rationale for the non-feasibility of an (b)(4) to result in agreement between HSI management and the Contractor's management on the contents of the (b)(4) either party may request adjudication from the assigned ICE Contracting Officer (CO), who shall make a determination within five (5) business days of receipt of the adjudication request as to whether or not the (b)(4) shall be included in (b)(4) In the event that HSI's priorities change during the

period of time covered by a (b)(4) and HSI requests that the (b)(4) (b)(4) be amended, and the Contractor determines that this new request for work does not clearly fall within the scope of the (b)(4) the Contractor may present the change request to the CO, who shall review the request to determine whether HSI's request falls within the scope of that document. Such determinations must be made within five (5) business days of the escalation request. The Contractor will not be obligated to take any action on the new request for work unless and until the CO, in coordination with the Contractor, approves the request and determines that such request falls within the scope of (b)(4) (b)(4) or otherwise amends such document to include the new request for work. In the event the CO and Contractor are unable to reach an agreement, the matter will be referred to ICE's Informational Technology Division Assistant Director for final adjudication. For any priority tasks outside the scope of (b)(4) HSI may request a level of effort from Contractor; Contractor shall not be obligated to perform such tasks unless (i) the task consists of high priority case work and is specifically requested by the Executive Assistant Director of HSI (or his/her designee); and (ii) a required task of a comparable level of effort is explicitly postponed or eliminated.

Changes to (b)(4) shall be incorporated into the contract through bilateral modification.

## 6.0 PERFORMANCE STANDARDS

| | | | |
|---|---|---|---|
| | | | |
| | | | |

## 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 quarterly at the Unit Chief level and twice per year to the Executive Steering Committee. The initial report is due forty-five

calendar days after start of the task and shall cover the first calendar month of performance. Subsequent reports shall be provided quarterly y 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.

- 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

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

| Deliverable | Frequency | Recipients |
|---|---|---|

| | | |
|---|---|---|
| (b)(4) | 10 working days after beginning of contract year | Electronic copy - PM, Contracting Officer, COR/ACOR |
| Project Plan for first of (b)(4) (b)(4) | 0 working days after beginning of contract year | Electronic copy - PM, Contracting Officer, COR/ACOR |
| Project Plans for subsequent (b)(4) (b)(4) | 10 working days prior to the initiation of work according to Schedule of | Electronic copy - PM, Contracting Officer, COR/ACOR |
| Project Schedule for first (b)(4) | 10 working days after beginning of contract year | Electronic copy - PM, Contracting Officer, COR/ACOR |
| Project Schedules for subsequent (b)(4) (b)(4) | 10 working days prior to the initiation of work according to Schedule of | Electronic copy - PM, Contracting Officer, COR/ACOR |
| Quarterly Progress Report | Quarterly, within 15 calendar days of the end of the quarter being reviewed | Electronic copy: PM, Contracting Officer, COR/ACOR |
| Certification and Accreditation Documentation | As Required | Electronic copy: PM, COR/ACOR |
| Transition In Plan- Final | 15 calendar days after award | Electronic copy: PM, Contracting Officer, COR/ACOR |
| Transition Out Plan | 120 calendar days before the end of the POP | Electronic copy: PM, Contracting Officer, COR/ACOR |

| | | |
|---|---|---|
| QASP- Final | 15 calendar days after award | Electronic copy: PM, Contracting Officer, COR/ACOR |
| | | |

### 7.6 Delivery Instructions

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

### 7.7 Draft Deliverables

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

### 7.8 Written Acceptance/Rejection by the Government

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

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

### 7.9 Non-Conforming Products or Services

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

### 7.10 Notice Regarding Late Delivery

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

## 8.0 CONSTRAINTS

### 8.1 General Constraints

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

- Changes to source databases TECS and the Enforcement Case Tracking System (ENFORCE) are being planned under TECS Modernization and E3;
- Existing FALCON system is a version of a Commercial, Off the Shelf (COTS) product sold by Palantir Technologies, Inc., called Palantir Gotham that has been specifically configure to meet HSI's needs;
- FALCON will be primarily accessed from the existing ICE standard desktop;
- ICE-OCIO must approve in writing any exceptions to the established ICE-OCIO System Lifecycle Management (SLM) processes;
- The Contractor will support and coordinate with ICE HSI's move from PCN to ICE-OCIO approved alternate data centers ;
- The Contractor shall comply with all DHS information security regulations for all Law Enforcement sensitive data;
- The Contractor shall comply with all applicable technology standards and architecture policies, processes, and procedures defined in ICE OCIO Architecture Division publications;
- The Contractor shall comply with the FALCON specific configuration management plan for all design and development artifacts in accordance with guidelines set forth in the Plan;
- ICE will provide Government Furnished Equipment as necessary to support all FALCON System Maintenance and Services activities.

### 8.2 DHS Enterprise Architecture Compliance

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

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

• All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

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

• Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
• Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special 8 ITAR Quick Essentials Guide 2011 v2.0 Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

## 8.3 Maintenance of Existing FALCON System Functionality

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

### 8.3.1 Continuation of Existing FALCON System Functionality

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

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

All data sets made newly accessible to the FALCON system under this contract shall be searchable along with previously existing FALCON data sets, both those data sets ingested within the FALCON system and those data sets remotely accessed. Contractor shall ensure that end users will continue to utilize a single, comprehensive front-end interface to search and manipulate all data accessible by FALCON, both data sets predating this contract and data sets made accessible within the scope of this contract.

Contractor shall ensure that previously existing FALCON system workflow applications (those (b)(7)(E) and FALCON-DARTTS) shall maintain all existing functionality and shall retain their existing "look and feel" for end users, such that no retraining of end users (or extremely minimal retraining, in the form of brief, on-line guides to changes which can be reviewed in less than an hour) is required.

Contractor shall ensure that all new work performed under this contract shall be compatible with the following application helpers previously deployed to assist end users with common, repetitive system tasks; these application helpers shall retain their existing "look and feel" for end users, such that no retraining of end users (or extremely minimal retraining, in the form of brief, on-line guides to changes which can be reviewed in less than an hour) is required unless mutually agreed to:

(b)(7)(E)

### 8.4 Level of Service

Contractor shall ensure that the FALCON system shall be able to accommodate the following minimum levels of service, with no diminishment of performance levels from performance levels met by the system prior to the initiation of this contract.

## 9.0 GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION

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

Items of GFE which are inventoried and tracked in Sunflower include the following seventeen laptops and four i-Phone handheld devices:

| Model Number | Serial Number | Laptop/VPN/i-Phone |
|---|---|---|
| Dell 6500 | (b)(7)(E) | |
| Dell 6500 | | |
| Dell Latitude E4310 | | |
| Dell Latitude D630 | | |
| Dell Latitude D630 | | |

| | | |
|---|---|---|
| Dell Latitude D620 | (b)(7)(E) | |
| HP Elitebook 8540p | | |
| Dell Latitude D620 | | |
| Dell Latitude D620 | | |
| Dell Latitude D630 | | |
| Dell M 6500 | | |
| HP Probook | | |
| HP Probook | | |
| HP Probook | | |
| HP Probook | | |
| HP Probook | | |
| HP Probook | | |
| HP Probook | | |
| HP Probook | | |
| HP Probook | | |
| iPhone5s | (b)(7)(E) | iPhone |
| iPhone4s | | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |

| | | |
|---|---|---|
| iPhone5s | (b)(7)(E) | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |
| iPhone5s | | iPhone |

### 9.1 Remote Access

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

## 10.0 OTHER DIRECT COSTS (ODCs)

Travel outside the local metropolitan Washington, DC area may be expected during performance of the resulting task order. Therefore, travel will be undertaken following the General Services Administration Field Travel Regulation. Reimbursement for allowable costs will be made. Any travel and training expenditures shall be pre-approved by the COR. Costs for transportation, lodging, meals and incidental expenses incurred by Contractor personnel on official company business are allowable subject to FAR 31.205-46, Travel Costs. These costs will be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the Federal Travel Regulations. The Contractor will not be reimbursed for travel and per diem within a 50-mile radius of the worksite where a Contractor has an office. Local travel expenses within the Washington Metropolitan area will not be reimbursed (this includes parking). All travel outside the Washington Metropolitan area must be approved by the COR in advance. No travel will be reimbursed without prior approval from the COR.

## 11.0 PLACE OF PERFORMANCE

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

## 12.0 PERIOD OF PERFORMANCE

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

## 13.0 SECURITY

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

### 13.1 Section 508 Compliance

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

### 13.2 General Clause

To ensure the security of the DHS/ICE information in their charge, ICE Contractors and Sub-contractors shall adhere to the same computer security rules and regulations as Federal Government employees unless an exception to policy is agreed to by the prime Contractors, ICE Information Systems Security Manager (ISSM) and Contracting Officer and detailed in the contract. Non-DHS Federal employees or Contractors who fail to comply with DHS/ICE security policies are subject to having their access to DHS/ICE IT systems and facilities terminated, whether or not the failure results in criminal prosecution. The DHS Rules of Behavior document applies to DHS/ICE support Contractors and Sub-contractors.

### 13.3 Security Policy References Clause

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

☐ DHS 4300A, Sensitive Systems Policy Directive

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

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

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

### 13.3.2 Protection of Sensitive Information

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

### 13.3.3 Information Technology Security Program

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

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

### 13.3.4 Handling of Sensitive Information and IT Resources

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

- **Media Protection**. The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive information stored on media to be surplused, 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 it's 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. Note that these procedures may be wavied by the COR, contingent upon approval of a follow-on contract with the current Contractor.

### 13.3.12 Personnel Security

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

All Contractor personnel (including Sub-contractor personnel) shall have favorably adjudicated background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/ICE sensitive information.

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

The Contractor shall ensure appropriate controls have been implemented to prevent Contractor personnel from obtaining access to DHS/ICE sensitive information before a favorably adjudicated

background investigation has been completed and appropriate clearances have been issued. At the option of the Government, interim access may be granted pending completion of a pre-employment check. Final access may be granted only upon favorable completion of an appropriate background investigation based on the risk level assigned to this contract by the Contracting Officer.

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

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

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

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

### 13.3.13 Physical Security

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

## 13.4 ISO Terms and Conditions for Sensitive but Unclassified Requests

### 13.4.1 DHS Security Policy Requirement

The following terms and conditions should be included in all acquisition documents.
All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

#### 13.4.1.1 Encryption Compliance Requirement

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

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.

2. National Security Agency (NSA) (b)(7)(E)
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

#### 13.4.1.2 Security Review Requirement

The following requirements should be included in all acquisition documents.

##### 13.4.1.2.1 Security Review

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

#### 13.4.1.3 Interconnection Security Agreement (ISA)

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

##### 13.4.1.3.1 Interconnection Security Agreement Requirements

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

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

The following requirements should be included in acquisition documents for information systems which are hosted, operated, maintained, and used on behalf of DHS at non-DHS facilities. Contractors are fully responsible and accountable for ensuring compliance with all Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) and related DHS security control requirements (to include configuration guides, hardening guidance, DHS Security Policy, Procedures, and Architectural guidance). The contractor security procedures shall be the same or

greater than those that are provided by DHS Enterprise Data Center(s). Please note that all of the subsections from **Security Authorization** to **Log Retention** are included in this requirement.

### 13.4.3 Security Authorization

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

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

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these requirements. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

### 13.4.4 Enterprise Security Architecture

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

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

Control Board (ICCB) process)
5. Performance of activities per continuous monitoring requirements

### 13.4.5 Continuous Monitoring

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

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

### 13.4.6 Specific Protections

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

#### 13.4.6.1 Security Operations

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

#### 13.4.6.2 Computer Incident Response Services

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

#### 13.4.6.3 Firewall Management and Monitoring

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

#### 13.4.6.4 Intrusion Detection Systems and Monitoring

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

#### 13.4.6.5 Physical and Information Security and Monitoring

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

#### 13.4.6.6 Vulnerability Assessments

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

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

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

#### 13.4.6.8 Patch Management

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

#### 13.4.6.9 Log Retention

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

#### 13.4.6.10 Supply Chain Risk Management Requirement

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

**Authorities:**
Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management
Department of Homeland Security, Security Policy for Sensitive Systems 4300A
Homeland Security Presidential Directive 23, Cyber Security and Monitoring, 8 January 2008
Office of Budget and Management Circulation A-130, Appendix III
•National Institute of Standards and Technology, Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

#### 13.4.6.10.1 Supply Chain Risk Management

The following requirements should be included in all hardware and software requests to ensure the confidentiality, integrity, and availability of government information.
The Contractors supplying the Government hardware and software shall provide the manufacture's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state and/or domain of registration and DUNs number of those suppliers must also be provided.
Subcontractors are subject to the same general requirements and standards as prime contractors.

Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.
The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.
Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.
The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.
The Supply Chain Risk Management Plan shall address the following elements:

1. How risks from the supply chain will be identified,
2. What processes and security measures will be adopted to manage these risks to the system or system components, and
3. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Technical Representative (COTR) 30 days post award.
The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.
The Contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.
The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.
The Contractor shall be excused from using new OEM (i.e. “grey market,” previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.
For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e. until the “end of life.”). Software updates and patches must be made available to the government for all products procured under this contract.
Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.
All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.
These records must be readily available for inspection by any agent designated by the US Government as having the authority to examine them.
This transit process shall minimize the number of times en route components undergo a change of

custody and make use tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit. The Contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

#### 13.4.6.11 Personal Identification Verification (PIV) Credential Compliance

Authorities:

- HSPD-12 "Policies for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 "Acquisition of Products and Services for Implementation of HSPD-12"
- NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- NIST SP 800-63 "Electronic Authentication Guideline"
- OMB M-10-15 "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

#### 13.4.6.11.1 Personal Identification Verification (PIV) Credential Compliance Requirement

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.
Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.
PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.
If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

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

**requirements for unclassified information technology resources.)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the

Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

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

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

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

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

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

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

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

the CSO and the CIO or their designees. In order for a waiver to be granted:

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

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

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

## 14.4 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

### 14.4.1 General

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

### 14.4.2 Fitness Determination

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

contract.

### 14.4.3 Background Investigations

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

1. Standard Form 85P (SF 85P) "Questionnaire for Public Trust Positions" Form shall be submitted via e-QIP (electronic Questionnaires for Investigation Processing) (Original and One Copy)

2. Three signed eQip Signature forms: Signature Page, Release of Information and Release of Medical Information (Originals and One Copy)

3. Two FD 258, "Fingerprint Card"

4. Foreign National Relatives or Associates Statement (Original and One Copy)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (Original and One Copy)

6. Optional Form 306 Declaration for Federal Employment (applies to contractors as well) (Original and One Copy)

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

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

Required forms will be provided by ICE at the time of award of the contract. Only complete

packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

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

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

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

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

**SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS**
*OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30*

| 1. REQUISITION NUMBER | PAGE | OF |
|---|---|---|
| 192115VHQ6ISI0017 | 1 | 115 |

| 2. CONTRACT NO. | 3. AWARD/ EFFECTIVE DATE | 4. ORDER NUMBER | 5. SOLICITATION NUMBER | 6. SOLICITATION ISSUE DATE |
|---|---|---|---|---|
| HSCETC-15-C-00001 | | | HSCETC-15-Q-00010 | 05/08/2015 |

7. FOR SOLICITATION INFORMATION CALL: a. NAME (b)(6),(b)(7)(C) b. TELEPHONE NUMBER (No collect calls) 202-732-(b)(6),(b)(7)(C) 8. OFFER DUE DATE/LOCAL TIME ES

9. ISSUED BY CODE ICE/ITD

ICE/Information Technology Division
Immigration and Customs Enforcement
Office of Acquisition Management
801 I Street NW, Suite (b)(6),(b)(7)(C)
Washington DC 20536

10. THIS ACQUISITION IS X UNRESTRICTED OR SET ASIDE % FOR:
SMALL BUSINESS
WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
HUBZONE SMALL BUSINESS
EDWOSB
SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
8(A)
NAICS: 511210
SIZE STANDARD: (b)(4)

| 11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED | 12. DISCOUNT TERMS | 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) | 13b. RATING |
|---|---|---|---|
| SEE SCHEDULE | Net 30 | | 14. METHOD OF SOLICITATION: X RFQ IFB RFP |

15. DELIVER TO CODE ICE/HSI/HQ-D6

ICE Hmlnd Sec Inv HQ Div. 6
Immigration and Customs Enforcement
500 12th Street SW
Washington DC 20024

16. ADMINISTERED BY CODE ICE/ITD

ICE/Information Technology Division
Immigration and Customs Enforcement
Office of Acquisition Management
801 I Street NW, Suite (b)(6),(b)(7)(C)
Washington DC 20536

17a. CONTRACTOR/ OFFEROR CODE 3621309520000 FACILITY CODE

PALANTIR TECHNOLOGIES INC
ATTN (b)(6),(b)(7)(C)
100 HAMILTON AVENUE
SUITE (b)(6),(b)(7)(C)
PALO ALTO CA 943011650

TELEPHONE NO.

17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE ICE-HSI-HQ-DIV 6

DHS, ICE
Burlington Finance Center
P.O. Box (b)(6),(b)(7)
Attn: ICE-HSI-HQ-DIV 6
Williston VT 05495-1620

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED X SEE ADDENDUM

| 19 ITEM NO. | 20. SCHEDULE OF SUPPLIES/SERVICES | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|---|---|---|---|---|---|
| | DUNS Number: 362130952<br>This is a Firm-Fixed Price (FFP) contract for FALCON Operations and Maintenance (O&M) Support and System Enhancement Services. The contractor shall provide the supplies and services in accorance with the Performance Work Statement (PWS) dated May 11, 2015, (b)(4) dated May 11, 2015, Safeguading of Sensitive Information and as outlined in this contract award document.<br>Exempt Action: N<br>*(Use Reverse and/or Attach Additional Sheets as Necessary)* | | | | |

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$9,900,000.00

27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ARE ARE NOT ATTACHED.
X 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4 FAR 52.212-5 IS ATTACHED. ADDENDA X ARE ARE NOT ATTACHED.

X 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

X 29. AWARD OF CONTRACT: REF Palantir Inc. OFFER DATED 05/11/2015 YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR
(b)(6),(b)(7)(C)

30c. DATE SIGNED
May 27, 2015

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
(b)(6),(b)(7)(C)

31c. DATE SIGNED
05/27/2015

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

**STANDARD FORM 1449 (REV. 2/2012)**
**Prescribed by GSA - FAR (48 CFR) 53.212**

| 19. ITEM NO. | 20. SCHEDULE OF SUPPLIES/SERVICES | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|---|---|---|---|---|---|
| | Delivery: 05/28/2015<br>Period of Performance: 05/28/2015 to 05/27/2018 | | | | |
| 0001 | BASE PERIOD:<br>GOTHAM UNLIMITED LICENSE<br>(Conversion of processor core licenses previously purchased under HSCETC-13-F-00030 to an unlimited license; also includes operation and maintenance support and other services indentifed in the PWS)<br>Obligated Amount: (b)(4)<br><br>Accounting Info:<br>(b)(7)(E)<br>Funded: (b)(4)<br>Accounting Info:<br>(b)(7)(E)<br>Funded: (b)(4)<br>Accounting Info:<br>(b)(7)(E)<br>Funded: (b)(4)<br>Accounting Info:<br>(b)(7)(E)<br>Funded: (b)(4)<br>Period of Performance: 05/28/2015 to 05/27/2016<br><br>Continued ... | (b)(4) | MO | (b)(4) | (b)(4) |

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

| 32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE | 32c. DATE | 32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE |
|---|---|---|
| 32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE | | 32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE<br>32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE |

| 33. SHIP NUMBER<br>☐ PARTIAL ☐ FINAL | 34. VOUCHER NUMBER | 35. AMOUNT VERIFIED CORRECT FOR | 36. PAYMENT<br>☐ COMPLETE ☐ PARTIAL ☐ FINAL | 37. CHECK NUMBER |
|---|---|---|---|---|
| 38. S/R ACCOUNT NUMBER | 39. S/R VOUCHER NUMBER | 40. PAID BY | | |

| 41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT | | 42a. RECEIVED BY *(Print)* | |
|---|---|---|---|
| 41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER | 41c. DATE | 42b. RECEIVED AT *(Location)* | |
| | | 42c. DATE REC'D *(YY/MM/DD)* | 42d. TOTAL CONTAINERS |

STANDARD FORM 1449 (REV. 2/2012) BACK

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|---|---|---|---|---|---|
| 1001 | OPTION PERIOD ONE:<br>GOTHAM OPERATION AND MAINTENANCE SUPPORT SERVICES<br>(Operation and maintenance of unlimited license; operation and maintenance support and other services identified in the PWS)<br>Amount: (b)(4) (Option Line Item)<br>05/27/2016<br>Period of Performance: 05/28/2016 to 05/27/2017 | (b)(4) | | | 0.00 |
| 2001 | OPTION PERIOD TWO:<br>GOTHAM OPERATION AND MAINTENANCE SUPPORT SERVICES<br>(Operation and maintenance of unlimited license; operation and maintenance support and other services identified in the PWS)<br>Amount: (b)(4) (Option Line Item)<br>05/27/2017<br>Period of Performance: 05/28/2017 to 05/27/2018 | (b)(4) | | | 0.00 |
| 3001 | FAR 52.217-8:<br>GOTHAM OPERATION AND MAINTENANCE SUPPORT SERVICES<br>(Optional six month extension for Operations and Management Services for previously acquired Palantir Gotham licenses/server cores; maintaining processing power.)<br>Amount: (b)(4) (Option Line Item)<br>05/27/2018<br>Period of Performance: 05/28/2018 to 11/27/2018 | (b)(4) | | | 0.00 |

For questions concerning this contract, please contact:

Contract Officer:
(b)(6),(b)(7)(C)
DHS/ICE/ITD
801 I Street, NW
Washington, DC 20536
Office: 202-732 (b)(6),(b)(7)(C)
Email: (b)(6),(b)(7)(C)

Contract Specialist:
(b)(6),(b)(7)(C)
DHS/ICE/ITD
801 I Street, NW
Washington, DC 20536
Office: 202-732 (b)(6),(b)(7)(C)
Continued ...

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|---|---|---|---|---|---|

Email: (b)(6),(b)(7)(C)

Contract Officer Representative:
(b)(6),(b)(7)(C)
Management and Program Analyst
DHS/ICE/HSI/IS&M
500 12th Street, NW
Washington, DC 20024
Office: 202-422-(b)(6),(b)(7)(C) or 202-732-(b)(6),(b)(7)(C)
Email: (b)(6),(b)(7)(C)

Alternate Contract Offier Representative:
(b)(6),(b)(7)(C)
Management and Program Analyst
DHS/ICE/HSI/IS&M
500 12th Street, NW
Washington, DC 20024
Office: 202-732-(b)(6),(b)(7)
Email: (b)(6),(b)(7)(C)

Vendor:
Palantir Technologies, (b)(6),(b)(7)(C)
Office: 703.270.(b)(6),(b)(7)(C)
Mobile: 781.248.
Fax: 650.618.2665
Email: (b)(6),(b)(7)(C)

The total amount of award: $34,650,000.00. The obligation for this award is shown in box 26.

**52.212-4 Contract Terms and Conditions -- Commercial Items (May 2015)**

(a) *Inspection/Acceptance.* The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights --

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C.3727). However, when a third party makes payment (*e.g.,* use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes.* Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes.* This contract is subject to 41 U.S.C. chapter 71,Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions.* The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays.* The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) *Invoice.*

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include --

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, contract line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (*e.g.*, 52.232-33, Payment by Electronic Funds Transfer— System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) *Patent indemnity*. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or

copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) Payment.

(1) Items accepted. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) Prompt Payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR Part 1315.

(3) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) *Discount*. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) *Overpayments*. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall—

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—

(A) Circumstances of the overpayment (*e.g.*, duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected contract line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6) Interest.

(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period at fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) Final decisions. The Contracting Officer will issue a final decision as required by 33.211 if—

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on—

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(j) *Risk of loss*. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes*. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience*. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause*. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title*. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty*. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability*. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances*. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts.* The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. 4712 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

(s) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause.

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments.

(9) The specification.

(t) System for Award Management (SAM).

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the SAM database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the SAM database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the SAM database to ensure it is current, accurate and complete. Updating information in the SAM does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)

(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in Subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to:

(A) Change the name in the SAM database;

(B) Comply with the requirements of Subpart 42.12 of the FAR;

(C) Agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name

agreement, the SAM information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the SAM record to reflect an assignee for the purpose of assignment of claims (see FAR Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the SAM database. Information provided to the Contractor's SAM record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via SAM accessed through https://www.acquisition.gov.

(u) Unauthorized Obligations.

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End Use License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(i) Any such clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(v) *Incorporation by reference*. The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of Clause)

**52.203-3** **GRATUITIES** (APR 1984)
(IAW FAR 3.202)

**52.203-17** **CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS** (APR 2014)
(IAW FAR 3.908-9)

**52.204-2** **SECURITY REQUIREMENTS** (AUG 1996)
(IAW FAR 4.404(a))

**52.204-9** **PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL** (JAN 2011)
(IAW FAR 4.1303)

**52.204-18** **COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE** (NOV 2014)
(IAW FAR 4.1804(c), FAR 12.301(d))

**52.204-19** **INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS** (DEC 2014)
(IAW FAR 4.1202(b))

**52.227-17** **RIGHTS IN DATA—SPECIAL WORKS (DEC2007)**

(This is only applicable to ICE generated information, ICE training information, and ICE Personally Identifiable Information (PII) in the system.)

(a) Definitions. As used in this clause-

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of Rights.

(1) The Government shall have-

(i) Unlimited rights in all data delivered under this contract, and in all data first produced in the performance of this contract, except as provided in paragraph (c) of this clause.

(ii) The right to limit assertion of copyright in data first produced in the performance of this contract, and to obtain assignment of copyright in that data, in accordance with paragraph (c)(1) of this clause.

(iii) The right to limit the release and use of certain data in accordance with paragraph (d) of this clause.

(2) The Contractor shall have, to the extent permission is granted in accordance with paragraph (c)(1) of this clause, the right to assert claim to copyright subsisting in data first produced in the performance of this contract.

(c) Copyright-

(1) Data first produced in the performance of this contract.

(i) The Contractor shall not assert or authorize others to assert any claim to copyright subsisting in any data first produced in the performance of this contract without prior written permission of the Contracting Officer. When copyright is asserted, the Contractor shall affix the appropriate copyright notice of 17 U.S.C. 401 or 402 and acknowledgment of Government sponsorship (including contract number) to the data when delivered to the Government, as well as when the data are published or deposited for registration as a published work in the U.S. Copyright Office. The Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license for all delivered data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

(ii) If the Government desires to obtain copyright in data first produced in the performance of this contract and permission has not been granted as set forth in paragraph (c)(1)(i) of this clause, the Contracting Officer shall direct the Contractor to assign (with or without registration), or obtain the assignment of, the copyright to the Government or its designated assignee.

(2) Data not first produced in the performance of this contract. The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract and that contain the copyright notice of 17 U.S.C. 401 or 402, unless the Contractor identifies such data and grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause.

(d) Release and use restrictions. Except as otherwise specifically provided for in this contract, the Contractor shall not use, release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer.

(e) Indemnity. The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data. The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to material furnished to the Contractor by the Government and incorporated in data to which this clause applies.

(End of Clause)

**52.227-19-- Commercial Computer Software License (Dec 2007)**

(a) Notwithstanding any contrary provisions contained in the Contractor's standard commercial license or lease agreement, the Contractor agrees that the Government will have the rights that are set forth in paragraph (b) of this clause to use, duplicate or disclose any commercial computer software delivered under this contract. The terms and provisions of this contract shall comply with Federal laws and the Federal Acquisition Regulation.

(1) The commercial computer software delivered under this contract may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b)(2) of this clause or as expressly stated otherwise in this contract.

(2) The commercial computer software may be—

(i) Used or copied for use with the computer(s) for which it was acquired, including use at any Government installation to which the computer(s) may be transferred;

(ii) Used or copied for use with a backup computer if any computer for which it was acquired is inoperative;

(iii) Reproduced for safekeeping (archives) or backup purposes;

(iv) Modified, adapted, or combined with other computer software, provided that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, commercial computer software shall be subject to same restrictions set forth in this contract;

(v) Disclosed to and reproduced for use by support service Contractors or their subcontractors, subject to the same restrictions set forth in this contract; and

(vi) Used or copied for use with a replacement computer.

(3) If the commercial computer software is otherwise available without disclosure restrictions, the Contractor licenses it to the Government without disclosure restrictions.

(c) The Contractor shall affix a notice substantially as follows to any commercial computer software delivered under this contract:

Notice--Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction and disclosure are as set forth in Government Contract No. _____.

(End of Clause)

**3052.204-71 CONTRACTOR EMPLOYEE ACCESS (SEP 2012)**

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under

section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

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

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

background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

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

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

(End of clause)

**ALTERNATE I (SEP 2012)**

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

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

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

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

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

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

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

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

(End of clause)

**52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT**
(MAR 2000)
(IAW FAR 17.208(g))

(a) The Government may extend the term of this contract by written notice to the Contractor within **30 calendar days**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **60** days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **three (3) years and six (6) months**.

**THE FOLLOWING IS FILL-IN DATA FOR CLAUSE 52.212-5 PARA (b)(25):**

**52.219-28 POST-AWARD SMALL BUSINESS PROGRAM REREPRESENTATION** (JUL 2013)

(g) If the Contractor does not have representations and certifications in SAM, or does not have a representation in SAM for the NAICS code applicable to this contract, the Contractor is required to complete the following rerepresentation and submit it to the contracting office, along with the contract number and the date on which the rerepresentation was completed:

The Contractor represents that it **[ ] is, [ ] is not** a small business concern under NAICS Code **511210** assigned to contract number _____.

[*Contractor to sign and date and insert authorized signer's name and title*].

**52.224-1** **PRIVACY ACT NOTIFICATION** (APR 1984)
(IAW FAR 24.104(a))

**52.224-2** **PRIVACY ACT** (APR 1984)
(IAW FAR 24.104(b))

**52.227-19** **COMMERCIAL COMPUTER SOFTWARE LICENSE** (DEC 2007)
(IAW FAR 27.409(g)

**52.229-4** **FEDERAL, STATE, AND LOCAL TAXES (STATE AND LOCAL ADJUSTMENTS)** (FEB 2013)
(IAW FAR 29.401-3(b))

**52.232-25** **PROMPT PAYMENT** (JUL 2013)
(IAW FAR 32.908(c)

**52.232-39** **UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS** (JUN 2013)
(IAW FAR 32.706-3)

**52.232-40** **PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS** (DEC 2013)
(IAW FAR 32.009-2)

**3052.242-71** **DISSEMINATION OF CONTRACT INFORMATION** (DEC 2003)
(IAW HSARFARS 3042.202-70)

**3052.242-72** **CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE** (DEC 2003)
(IAW HSARFARS 3042.7000)

**52.243-7** **NOTIFICATION OF CHANGES** (APR 1984)
(IAW FAR 43.107)

(b) the Contractor shall notify the Administrative Contracting Officer in writing promptly, within **30** calendar days

(d) The Contracting Officer shall promptly, within **15** calendar days

**3052.245-70** **GOVERNMENT PROPERTY REPORTS** (JUN 2006)
(IAW HSARFARS 3045.505-70)

**52.247-68** **REPORT OF SHIPMENT (REPSHIP)** (FEB 2006)
(IAW FAR 47.208-2)

**52.252-4** **ALTERATIONS IN CONTRACT** (APR 1984)
(IAW FAR 52.107(d))

Portions of this contract are altered as follows:

**********
**********
**********
**********

**ICE PRIVACY REVIEW CLAUSES**

**PRIV 1.4: Separation Checklist for Contractor Employees**: Contractors shall enact a protocol to use a separation checklist before its employees, Subcontractor employees, or independent Contractors terminate working on the contract. The separation checklist must cover areas such as: (1) return of any Government-furnished equipment; (2) return or proper disposal of Sensitive PII (paper or electronic) in the custody of the Contractor/Subcontractor employee or independent Contractor, including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to Sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee, Subcontractor employee, or independent Contractor, the Contractor shall notify the Contract Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

(End of clause)

**PRIV 1.7: Privacy Act Information: In accordance with FAR 52.224-1, PRIVACY ACT**

**NOTIFICATION (APR 1984), and FAR 52.224-2, PRIVACY ACT (APR 1984),** this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974. The Agency advises that the relevant system of records notices (SORNs) applicable to this Privacy Act information include, but are not limited to, the following:

- All ICE SORNS
- DHS/CBP006 - Automated Targeting System
- DHS/CBP011 - U.S. Customs and Border Protection TECS
- DHS/CBP013 - Seized Assets and Case Tracking System
- DHS/CBP017- Analytical Framework for Intelligence (AFI) System of Records
- DHS/NPPD004 - DHS Automated Biometric Identification System (IDENT)
- DHS-USCIS007 - Benefits Information System
- DHS/USVISIT001- Arrival and Departure Information System (ADIS)
- FBI/001 - National Crime Information Center (NCIC)

These SORNs may be updated at any time. The most current DHS versions are publicly available at www.dhs.gov/privacy. SORNs of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System of the Government Publishing Office, available at http://www.gpo.gov/fdsys/.

(End of clause)

**PRIV 2.1: Restriction on Testing Using Real Data Containing PII**: The use of real data containing Sensitive PII from any source for testing purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing whenever feasible. ICE policy requires that any proposal to use real data or de-identified data for IT system testing be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

(End of clause)

**PRIV 2.2: Restriction on Training Using Real Data Containing PII**: The use of real data containing Sensitive PII from any source for training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for training whenever feasible. ICE policy requires that any proposal to use real data or de-identified data for IT system training be approved by the ICE Privacy Officer and Chief Information Security Officer in advance. In the event performance of the contract requires or necessitates the use of real data for training purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Agency program manager shall obtain approval from OCIO and the ICE Privacy Office and complete any required documentation.

(End of clause)

**REC: 1.1: Required DHS Basic Records Management Training**: The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to Sensitive PII as well as the creation, use, dissemination and/or destruction of Sensitive

PII at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site. The Agency may also make the training available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance. The Contractor must submit an annual e-mail notification to the Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

(End of clause)

**REC 1.2: Deliverables Property of the Agency Not Retained, Disseminated**: Except for the Palantir products cited in the approved License Service Agreement (LSA) as incorporated and referenced FAR Clauses herein, the Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable without the expressed permission of the Contracting Officer or Contracting Officer's Representative. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract. The Agency owns the rights to all data/records produced as part of this contract.

(End of clause)

**REC 1.3: Contractor Not Create or Maintain Any Records Not Tied to Contract**: The Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records. The Contractor shall not create or maintain any records containing any Government Agency data that are not specifically tied to or authorized by the contract.

(End of clause)

**REC 1.4: Agency Owns Rights to Electronic Information – Deliver Technical Requirements**: Except for the Palantir products cited in the approved License Service Agreement (LSA) as incorporated and referenced FAR Clauses herein, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation created as part of this contract. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the Agency to use the data.

(End of clause)

**REC 1.5: Comply With All Records Management Policies**: The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(End of clause)

**REC 1.6: No Disposition of Documents Without Prior Written Consent**: No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized

destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

(End of clause)

**REC 1.7: Contractor Obtain Approval Prior to Engaging Sub-Contractor Support**: The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(End of clause)

**SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)**

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under

criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of

the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

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

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

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits) (2) Date of birth (month, day, and year) (3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation

(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year) (8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of

Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to

safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems. (f) Sensitive Information Incident Reporting Requirements.
(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor

has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email); (vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved; (ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident. (g) Sensitive Information Incident Response Requirements.
(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies

and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means; (iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer: (1) Provide notification to affected individuals as described above; and/or
(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring; (ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period; (ii)

Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

(End of clause)

**INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)**

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e- mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

## CONTRACT TERMS AND CONDITIONS

**52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS** (DEC 2014)
(IAW FAR 12.301(b)(4))

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) **52.209-10,** Prohibition on Contracting with Inverted Domestic Corporations (Dec 2014).

(2) **52.222-50**, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).

___ **Alternate I** (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).

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

(4) **52.233-4**, Applicable Law for Breach of Contract Claim (Oct 2004)(Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

*[Contracting Officer check as appropriate.]*

| | | |
|---|---|---|
| X | (1) | **52.203-6**, Restrictions on Subcontractor Sales to the Government (Sep 2006), with **Alternate I** (Oct 1995)(41 U.S.C. 4704 and 10 U.S.C. 2402). |
| X | (2) | **52.203-13,** Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509). |
| ___ | (3) | **52.203-15**, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.) |
| ___ | (4) | **52.204-10**, Reporting Executive Compensation and First-Tier Subcontract Awards (Jul 2013) (Pub. L. 109-282) (31 U.S.C. 6101 note). |
| | (5) | [Reserved] |
| ___ | (6) | **52.204-14**, Service Contract Reporting Requirements (Jan 2014) (Pub. L. 111-117, section 743 of Div. C). |
| ___ | (7) | **52.204-15,** Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Jan 2014) (Pub. L. 111-117, section 743 of Div. C). |
| X | (8) | **52.209-6**, Protecting the Government's Interest When |

Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Aug 2013) (31 U.S.C. 6101 note).

X (9) **52.209-9,** Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

____ (10) [Reserved}

___ (11) (i) **52.219-3**, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011)(15 U.S.C. 657a).

__ (11) (ii) **Alternate I** (Nov 2011) of 52.219-3.

___ (12) (i) **52.219-4**, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

__ (12) (ii) **Alternate I** (Jan 2011) of 52.219-4.

(13) [Reserved]

___ (14) (i) **52.219-6**, Notice of Total Small Business Set-Aside (Nov 2011)(15 U.S.C. 644).

___ (14) (ii) **Alternate I** (Nov 2011).

___ (14) (iii) **Alternate II** (Nov 2011).

___ (15) (i) **52.219-7**, Notice of Partial Small Business Set-Aside (June 2003)(15 U.S.C. 644).

___ (15) (ii) **Alternate I** (Oct 1995) of 52.219-7.

___ (15) (iii) **Alternate II** (Mar 2004) of 52.219-7.

X (16) **52.219-8**, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)).

___ (17) (i) **52.219-9**, Small Business Subcontracting Plan (Oct 2014)(15 U.S.C. 637(d)(4)).

___ (17) (ii) **Alternate I** (Oct 2001) of 52.219-9.

___ (17) (iii) **Alternate II** (Oct 2001) of 52.219-9.

___ (17) (iv) **Alternate III** (Oct 2014) of 52.219-9.

___ (18) **52.219-13**, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).

___ (19) **52.219-14**, Limitations on Subcontracting (Nov 2011)(15 U.S.C. 637(a)(14)).

___ (20) **52.219-16**, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

___ (21) **52.219-27**, Notice of Total Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011)(15 U.S.C. 657 f).

X (22) **52.219-28**, Post Award Small Business Program Rerepresentation

(Jul 2013) (15 U.S.C. 632(a)(2)).

___ (23) **52.219-29,** Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (Jul 2013) (1 U.S.C. 637(m)).

___ (24) **52.219-30,** Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (Jul 2013) (15 U.S.C. 637(m)).

___ (25) **52.222-3**, Convict Labor (June 2003)(E.O. 11755).

X (26) **52.222-19**, Child Labor—Cooperation with Authorities and Remedies (Jan 2014)(E.O. 13126).

X (27) **52.222-21**, Prohibition of Segregated Facilities (Feb 1999).

X (28) **52.222-26**, Equal Opportunity (Mar 2007)(E.O. 11246).

X (29) **52.222-35**, Equal Opportunity for Veterans (Jul 2014)(38 U.S.C. 4212).

X (30) **52.222-36**, Equal Opportunity For Workers with Disabilities (Jul 2014)(29 U.S.C. 793).

X (31) **52.222-37**, Employment Reports on Veterans (Jul 2014)(38 U.S.C. 4212).

X (32) **52.222-40**, Notification of Employee Rights Under the National Labor relations Act (Dec 2010) E.O. 13496).

___ (33) **52.222-54**, Employment Eligibility Verification (Aug 2013). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

___ (34) (i) **52.223-9**, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008)(42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

___ (34) (ii) **Alternate I** (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

___ (35) (i) **52.223-13**, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

___ (35) (ii) **Alternate I** (Jun 2014) of 52.223-13.

___ (36) (i) **52.223-14**, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).

___ (36) (ii) **Alternate I** (Jun 2014) of 52.223-14.

___ (37) **52.223-15**, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42.U.S.C. 8259b).

___ (38) (i) **52.223-16**, Acquisition of EPEAT®-Registered Personal

Computer Products (Jun 2014) (E.O.s 13423 and 13514).

___ (38) (ii) **Alternate I** (Jun 2014) of 52.223-16.

X (39) **52.223-18**, Encouraging Contractor Policies to Ban Text Messaging While Driving (Aug 2011)(E.O.13513).

___ (40) **52.225-1**, Buy American--Supplies (May 2014)(41 U.S.C. chapter 83).

___ (41) (i) **52.225-3**, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

___ (41) (ii) **Alternate I** (May 2014) of 52.225-3.

___ (41) (iii) **Alternate II** (May 2014) of 52.225-3.

___ (41) (iv) **Alternate III** (May 2014) of 52.225-3.

___ (42) **52.225-5**, Trade Agreements (Nov 2013) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

X (43) **52.225-13**, Restriction on Certain Foreign Purchases (Jun 2008)(E.O.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of Treasury).

___ (44) **52.225-26**, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

___ (45) **52.226-4**, Notice of Disaster or Emergency Area Set-Aside (Nov 2007)(42 U.S.C. 5150).

___ (46) **52.226-5**, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007)(42 U.S.C. 5150).

___ (47) **52.232-29**, Terms for financing of Purchases of Commercial Items (Feb 2002)(41 U.S.C. 4505, 10 U.S.C. 2307(f)).

___ (48) **52.232-30**, Installment Payments for Commercial Items (Oct 1995)(41 U.S.C. 4505, 10 U.S.C. 2307(f)).

___ (49) **52.232-33**, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013)(31.U.S.C. 3332).

___ (50) **52.232-34**, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013)(31.U.S.C. 3332).

___ (51) **52.232-36**, Payment by Third Party (May 2014) (31 U.S.C. 3332).

___ (52) **52.239-1**, Privacy or Security Safeguards (Aug 1996)(5 U.S.C.

552a).

___ (53) (i) **52.247-64**, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

___ (53) (ii) **Alternate I** (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

*[Contracting Officer check as appropriate.]*

___ (1) **52.222-41**, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

___ (2) **52.222-42**, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (3) **52.222-43**, Fair Labor Standards Act and Service Contract Labor Standards--Price Adjustment (Multiple Year and Option Contracts) (May 2014)(29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (4) **52.222-44**, Fair Labor Standards Act and Service Contract Labor Standards - Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (5) **52.222-51**, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (May 2014) (41 U.S.C. chapter 67).

___ (6) **52.222-53**, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014)(41 U.S.C. chapter 67).

___ (7) **52.222-17**, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495).

___ (8) **52.226-6**, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

___ (9) **52.237-11**, Accepting and Dispensing of $1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).

___ (10) **52.222-55**, Minimum Wages Under Executive Order 13658 (Dec 2014)(Executive Order 13658).

(d) *Comptroller General Examination of Record.* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.
(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (e)(1) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) **52.203-13**, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509).
(ii) **52.219-8**, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
(iii) **52.222-17**, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow Down required in accordance with paragraph (l) of FAR clause 52.222-17.
(iv) **52.222-26**, Equal Opportunity (Mar 2007) (E.O. 11246).
(v) **52.222-35**, Equal Opportunity for Veterans (Jul 2014) (38 U.S.C. 4212).
(vi) **52.222-36**, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).
(vii) **52.222-37**, Employment Reports on Veterans (Jul 2014) (38 U.S.C. 4212).
(viii) **52.222-40**, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
(ix) **52.222-41**, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).
(x) **52.222-50**, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104 (g)).
_ Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).
(xi) **52.222-51**, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (May 2014) (41 U.S.C. chapter 67).

(xii) **52.222-53**, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014) (41 U.S.C. chapter 67).
(xiii) **52.222-54,** Employment Eligibility Verification (Aug 2013).
(xiv) **52.225-26,** Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
(xv) **52.226-6**, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraphs (e) of FAR clause 52.226-6.
(xvi) **52.247-64**, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.
(xvii) **52.222-55,** Minimum Wages Under Executive Order 13658 (Dec 2014) (Executive Order 13658).

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

Invoicing Instructions

1. Invoices shall be submitted on a monthly or quarterly basis as outlined below. The monthly invoice amount will be based on the total price of the base period divided by the period of performance of the base period. If an option period if exercised under this contract, the invoicing for the option period will be determined in the same manner.

2. Invoice Submission:

a. Primary method of submission is email. Invoices shall be submitted to:
(b)(7)(E)

Additional copies of all submitted invoices shall be emailed to the Contracting Officer (CO) and Contracting Officer Representative (COR). Each email shall be in a .pdf format; contain only one (1) invoice and the subject line of the email will annotate the invoice number.

b. Alternative method of submission is fax. Invoices shall be submitted to:
(800) 288-7658

Each fax shall have a cover sheet identifying point of contact, phone number and number of pages.

Contractor Taxpayer Identification Number (TIN) must be registered in the Central Contractor Registration (http://www.ccr.gov) prior to award and shall be notated on every invoice submitted to ICE/OAQ to ensure prompt payment provisions are met.

3. Content of Invoices: Each invoice submission shall contain the following information:

(i) Name and address of the Contractor;
(ii) Invoice date and number;
(iii) Contract number, contract line item number and, if applicable, the order number;
(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
(vi) Terms of any discount for prompt payment offered;
(vii) Name and address of official to whom payment is to be sent;
(viii) Name, title, and phone number of person to notify in event of defective invoice; and
(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract. (See paragraph 1 above.)
(x) Electronic funds transfer (EFT) banking information.
(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.
(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with 52.232-33, Payment by Electronic Funds Transfer; Central Contractor Registration.
(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

4. Payment Inquiries: Questions regarding invoice submission or payment, contact DHS/ICE Financial Operations – Burlington Customer Service Inquiry Center @ 1-877-491-6521 Monday through Friday 8:00 AM -5:30 PM EST or at e-mail address (b)(7)(E)