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

1. REQUISITION NUMBER	PAGE	OF
RSUP-20-00008	1	52

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
70RSAT19D00000003	06/07/2020	70RSAT20FR0000051	70RSAT20R00000004	03/13/2020

7. FOR SOLICITATION INFORMATION CALL: (b)(6)

8. OFFER DUE DATE/LOCAL TIME: ET

9. ISSUED BY — CODE: DHS/OPO/S&T/S

U.S. Dept. of Homeland Security
Office of Procurement Operations
S&T Acquisition Branch
245 Murray Lane, SW, #0115
Washington DC 20528-0115

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☐ 8(A)

NAICS: 541611
SIZE STANDARD: $15.0

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 / 14. METHOD OF SOLICITATION
☒ SEE SCHEDULE	Net 30	☐	☐RFQ ☐IFB ☐RFP

15. DELIVER TO — CODE: S&T MURRAY LANE

DHS S&T
245 Murray Lane
Building 410
Washington DC 20528

16. ADMINISTERED BY — CODE: DHS/OPO/S&T/S&T

U.S. Dept. of Homeland Security
Office of Procurement Operations
S&T Acquisition Branch
245 Murray Lane, SW, #0115
Washington DC 20528-0115

17a. CONTRACTOR/ OFFEROR — CODE: 9329023640000 — FACILITY CODE:

NOBLIS INC
2002 EDMUND HALLEY DR
RESTON VA 20191

TELEPHONE NO.

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

18a. PAYMENT WILL BE MADE BY — CODE: DHS-S&T-INV

DHS ICE
Burlington Finance Center
PO BOX 1000
Attn: S&T Division
Williston VT 05495-1000

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 932902364+0000 The Department of Homeland Security (DHS) issues a Time-and-Material Task Order to obtain program management, administrative and technical support services for the Science and Technology (S&T) Directorate, Office of University Programs (OUP) against the Science and Technology Systems Engineering and Technical Assistance III (SETA III) multiple-award Indefinite Quantity, Indefinite Delivery (IDIQ) contract in accordance with the attached Statement of Work (Attachment *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA: See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: $2,692,510.90

☐ 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.
☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☒ ARE ☐ ARE NOT ATTACHED.

☒ 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.

☐ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

(b)(6)

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
	J.1). All applicable terms and conditions flow down from the SETA III IDIQ and shall apply to this Task Order. Ceiling Price for this Task Order is (b)(4) If the Contractor exceeds the ceiling price, the Contractor does so at its own risk. Refer to Attachment 2 Pricing Schedule for detailed Labor Categories, rates and number of hours. The period of performance for this requirement is a one (1) 12-month Base Period, two (2) 12-month Option Periods. Period of Performance: 06/07/2020 to 06/06/2023				
0001	LABOR BASE PERIOD: June 7, 2020 - June 6, 2021 Product/Service Code: R408 Product/Service Description: SUPPORT-PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT Delivery: 06/06/2021 Accounting Info: NONE000-000-U0-40-96-01-000-37-05-0000-00-00-00-00 Continued ...				(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
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ 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

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	-GE-OE-25-50-000000 Funded: (b)(4) Accounting Info: NONE000-000-U8-40-01-02-001-37-05-0000-00-00-00-00 -GE-OE-25-50-000000 Funded: (b)(4) Accounting Info: NONE000-000-U9-40-01-02-001-37-05-0000-00-00-00-00 -GE-OE-25-50-000000 Funded: (b)(4)				
0002	TRAVEL - NTE BASE PERIOD: June 7, 2020 - June 6, 2021 Delivery: 06/06/2021 Accounting Info: NONE000-000-U9-40-01-02-001-37-05-0000-00-00-00-00 -GE-OE-25-50-000000 Funded: (b)(4)				(b)(4)
0003	ODC - NTE BASE PERIOD: June 7, 2020 - June 6, 2021 Delivery: 06/06/2021 Accounting Info: NONE000-000-U9-40-01-02-001-37-05-0000-00-00-00-00 -GE-OE-25-50-000000 Funded: (b)(4)				(b)(4)
0004	SURGE Labor Reference SOW and Pricing Sheet BASE PERIOD: June 7, 2020 - June 6, 2021 Amount: (b)(4) (Option Line Item)				(b)(4)
1001	LABOR OPTION PERIOD I: June 7, 2021 - June 6, 2022 Amount: (b)(4) Option Line Item)				(b)(4)
1002	TRAVEL - NTE Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	OPTION PERIOD I: June 7, 2021 - June 6, 2022 Amount: (b)(4) Option Line Item)				
1003	ODC - NTE OPTION PERIOD I - June 7, 2021 - June 6, 2022 Amount: (b)(4) (Option Line Item)				(b)(4)
1004	SURGE Labor Reference SOW and Pricing Sheet OPTION PERIOD I: June 7, 2021 - June 6, 2022 Amount: (b)(4) (Option Line Item) Product/Service Code: R408 Product/Service Description: SUPPORT-PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT				
2001	LABOR OPTION PERIOD II: June 7, 2022 - June 6, 2023 Amount: (b)(4) (Option Line Item)				
2002	TRAVEL - NTE OPTION PERIOD II: June 7, 2022 - June 6, 2023 Amount: (b)(4) (Option Line Item)				(b)(4)
2003	ODC - NTE OPTION PERIOD II: June 7, 2022 - June 6, 2023 Amount: (b)(4) Option Line Item)				
2004	SURGE Labor Reference SOW and Pricing Sheet OPTION PERIOD II: June 7, 2022 - June 6, 2023 Amount: (b)(4) Option Line Item)				

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	The total amount of award: (b)(4) The obligation for this award is shown in box 26.				

PIID: 70RSAT20FR0000051

SETA III TASK ORDER

SYSTEMS ENGINEERING AND TECHNICAL ASSISTANCE III INDEFINITE-DELIVERY/INDEFINITE-QUANTITY CONTRACT REQUIREMENT

1. REQUIREMENT TITLE:

Office of University Programs Programmatic Support Services

2. PROCUREMENT INSTRUMENT IDENTIFIER:

70RSAT20R0000004

3. ISSUING OFFICE:

U.S. Department of Homeland Security, Directorate for Management, Office of the Chief Procurement Officer, Office of Procurement Operations, Science and Technology Acquisitions Division

4. AGENCY CONTACTS:

Contracting Officer: (b)(6)

Contract Specialist: (b)(6)

Please include both contacts in communications related to this opportunity.

5. ISSUE DATE:

5.1. Notice Type: Request for Proposal (RFP)

5.2. Version (Check one, complete form field only for modifications):

☒ Base ☐ Modification/Amendment (Fill-in number (/P#####)):

5.3. Issuance Date: Friday, March 13, 2020

6. PERIOD OF PERFORMANCE

6.1. If this notice is an RFI, the duration here is an estimate only.

6.2. The period of performance for this requirement is 36 months from date of award.

6.3. This requirement includes two (2) option periods.

Option Period	Duration
Base Period	June 7, 2020-June 6, 2021
Option Period I	June 7, 2021-June 6, 2022
Option Period II	June7, 2022-June 6, 2023

6.4. The total anticipated period of performance for this requirement if all options are exercised is 36 months.

6.5. This section will be completed by the contracting officer at the time the Task order is awarded:

The full period performance is from June 7, 2020 through June 6, 2023.

7. INFORMATION

7.1. NAICS Code and Small Business Size Standard:

The principal nature of the requirements described in this solicitation is consistent with services performed by industries in the 541611 North American Industry Classification System code (Administrative Management and General Management Consulting Services) with a small business size standard of $15M in average annual receipts.

7.2. Product Service Code (PSC):

The services in this solicitation are best represented by PSC Code: R408 - Support-Professional: Program Management/Support

7.3. Type of Contract: This is a Time-and-Materials (T&M) type contract.

7.4. Telework for this requirement:

☒ Is permitted subject to the stipulations of § H.4 "Telework" of the SETA III IDIQ.

☐ Is not permitted since the contracting officer has determined, in writing, the requirements of the agency, including security requirements, cannot be met if teleworking is permitted.

7.5. Security:

This requirement is:

☐ Unclassified ☒ Classified ☐ Mix of Both

The Facility Clearance Level for this requirement is:

☐ Unclassified ☒ Secret ☐ Top Secret

7.6. The work will be performed at a site owned/controlled by:

☐ Government ☐ Contractor ☒ Mix of Both

7.7. The place(s) of performance for this requirement are:

1120 Vermont Avenue NW, Washington DC

DHS Facilities within the Washington, DC metropolitan area

The Contractor may at times, in collaboration with Government staff, temporarily perform work under this SOW at other federal government facilities, with appropriate authorization, and at their designated contractor locations as approved in advance by the CO, the S&T COR and S&T's Office of Security, should any sensitive or classified information be involved.

8. DESCRIPTION OF SERVICES

(Please refer to the Statement of Work.)

9. LABOR CATEGORIES AND DESCRIPTIONS

The successful Offeror's applicable labor categories and rates will be included as part of the awarded Task Order.

10. INVOICING INSTRUCTIONS

Invoices shall be submitted via email to InvoiceSAT.Consolidation@ice.dhs.gov with a courtesy copy (cc:) to the Contracting Officer's Representative (COR) and Contracting Officer (CO).

11. TASK ORDER CLAUSES

11.1. All Applicable and Required clauses set forth in Federal Acquisition Regulation (FAR) 52.301 automatically flow down to all SETA III task orders, based on their specific contract type, e.g. FFP, LH, or T&M.

11.2. The clause at FAR 52.212-4, "Contract Terms and Conditions - Commercial Items," applies to this acquisition.

11.3. The clause at FAR 52.212-5, "Contract Terms and Conditions Required to Implement Statutes or Executive Orders - Commercial Items," applies to this acquisition with all applicable additional FAR clauses cited therein.

11.4. Pursuant to paragraph (d)(2) of the Rights in Data-General clause, FAR 52.227-14, of this task order, the Contractor may not use data first produced in the performance of this task order for any purpose other than the performance of this task order without the prior, written permission of the Contracting Officer.

11.5. Representation and Certification provisions from the SETA III master contracts automatically flow down to all task orders.

11.6. The following additional clauses are applicable to this requirement if the boxes next to them are

SETA III TASK ORDER

checked (contracting officer must check and complete as applicable):

☒ **52.204-2 SECURITY REQUIREMENTS (AUG 1996)**

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with --

(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

(End of Clause)

☐ **52.211-11 LIQUIDATED DAMAGES-SUPPLIES, SERVICES, OR RESEARCH AND DEVELOPMENT (SEPT 2000)**

(a) If the Contractor fails to deliver the supplies or perform the services within the time specified in this contract, the Contractor shall, in place of actual damages, pay to the Government liquidated damages of $<INSERT DOLLAR AMOUNT> per calendar day of delay.

(b) If the Government terminates this contract in whole or in part under the Default-Fixed-Price Supply and Service clause, the Contractor is liable for liquidated damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These liquidated damages are in addition to excess costs of repurchase under the Termination clause.

(c) The Contractor will not be charged with liquidated damages when the delay in delivery or performance is beyond the control and without the fault or negligence of the Contractor as defined in the Default-Fixed-Price Supply and Service clause in this contract.

(End of clause)

☒ **52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor within one (1) day; provided that the Government gives the Contractor a preliminary written

notice of its intent to extend at least seven (7) 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 3 years.

(End of clause)

☒ **3052.215-70 KEY PERSONNEL OR FACILITIES (DEC 2003)**

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract:

(b)(6) - (b)(4)

(b)(6) - (b)(4)

(b)(6) (b)(4)

(End of clause)

3052.242-72 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

(b) The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

(End of clause)

11.7. CONTRACTING OFFICER'S REPRESENTATIVE (COR)

(a) The Contracting Officer's Representative (COR) that will be responsible for the day-to-day coordination of this Task Order. The COR for this Task Order is designated in accordance with Homeland Security Acquisition Regulation (HSAR) 3052.242-72 Contracting Officer's Technical Representative (DEC 2003) included in this Task Order.

(b) The COR for this Task Order is:

(b)(6)

(c) The COR will represent the Contracting Officer in the administration of technical details within the scope of the Task Order. The COR is also responsible for final inspection and acceptance of all Task Order deliverables and reports, and such other responsibilities as may be specified in this Task Order. The COR is not otherwise authorized to make any representations or commitments of any kind on behalf of the Contracting Officer or the Government that affect, price, quality, quantity, delivery, or other terms and conditions of this Task Order. If, as a result of technical discussions, it is desirable to modify Task Order obligations or specifications, changes will be issued in writing and signed by the Contracting Officer.

(d) The Alternate Contracting Officer's Representative (ACOR) will be responsible for the day-to-day coordination of this Task Order when the COR is unavailable. The ACOR for this Task Order is designated in accordance with Homeland Security Acquisition Regulation (HSAR) 3052.242-72 Contracting Officer's Technical Representative included in this Task Order.

(e) The ACOR for this Task Order is:

(b)(6)

(f) The ACOR will represent the Task Order Contracting Officer in the administration of technical details within the scope of the Task Order when the COR is unavailable. References in this Task Order to the COR shall be construed to mean the ACOR in the event the COR is unavailable.

11.8. CONTRACTING OFFICER AND CONTRACT SPECIALIST

(a) The Contracting Officer (CO) is the only person authorized to approve changes to any of the terms and conditions of this Task Order. In the event the Contractor effects any changes at the direction of any person other than the CO, the changes will be considered to have been made without authority and no adjustment will be made in the Task Order price to cover any increase in prices incurred as a result thereof. The CO shall be the only individual authorized to accept nonconforming work, waive any requirement of the Task Order, or to modify any term or condition of the Task Order. The CO is the only individual who can legally obligate government funds. No cost chargeable to the proposed Task Order can be incurred before receipt of a fully executed Task Order, which includes any subsequent modifications or other specific written authorization from the CO.

(b) The Contractor shall not comply with any order, direction or request of government personnel unless it is issued in writing and signed by the CO, or is pursuant to specific authority otherwise included as a part of this Task Order. No order, statement, or conduct of government personnel, other than the CO, who visit the Contractor's facilities or in any other manner communicate with Contractor personnel during the performance of this Task Order shall constitute a change under the Changes clause included in this Task Order.

(c) The Contracting Officer for this Task Order is:

(b)(6)

(d) The Contract Specialist for this Task Order is:

(b)(6)

12. OPTIONAL TASKS AND SURGE CLINS

This solicitation and the resulting task order contain optional tasks and surge CLINs as detailed in the Statement of Work and Pricing Table. These options may be exercised within their respective periods and shall not cross into another period of performance from the one in which they are exercised. Should the Government choose to exercise an optional task or Surge CLIN, that option will be exercised no later than the second to last month of the period in which it is exercised.

Surge and optional CLINs may be exercised in increments as little as one hour.

The Government will make all efforts to notify an awardee no later than 15 days before the exercise of an optional task or surge CLIN. This notice will be provided by e-mail. Optional tasks and surge CLINs will be exercised via formal modification to the task order. This modification

will be sent by the task order Contract Specialist or Contracting Officer. Surge CLINs will not and cannot be ordered by the Contracting Officer's Representative.

ATTACHMENTS

Number	Title	# of Pages
J-1	Statement of Work	27
J-2	Deliverables	6
J-3	Pricing Schedule	3
J-4	DHS Non-Disclosure Agreement	3

Attachment J-1

Statement of Work
for
Systems Engineering and Technical Assistance (SETA)
Indefinite Delivery Indefinite Quantity (IDIQ)

Science and Technology (S&T) Directorate
Research and Development (R&D) Program Support
Office of University Programs

1.0 GENERAL

1.1 Background and Introduction

In its continuing quest to make America secure, the U.S. Department of Homeland Security (DHS) is committed to advancing science, creating cutting-edge technology, and leveraging scientific and non-scientific talents in order to strengthen the domestic defensive posture against terrorism. As a result, the DHS Science and Technology Directorate (S&T) is dedicated to creating, promoting, encouraging and advancing a full range of research and development (R&D) efforts to drive innovation and efficient technological solutions to help guard the homeland and guide the nation to a better protected and resilient future.

To support DHS S&T's mission, a full range of Systems Engineering and Technical Assistance (SETA) services are needed. SETA services range from providing administrative assistance to providing expert technical assistance on national efforts that will contribute to maintaining and expanding the capabilities of homeland security. The program office within S&T that this task order shall support is the Office of University Program

SETA service for the Office of University Programs (OUP) requires providing technical knowledge, scientific information, advice, opinions, alternatives, analyses, feedback, and recommendations; providing administrative support to program and technical management; and providing assistance to program planning and oversight, exercise, development, execution and evaluation; system level analysis; system integration support inclusive of understanding of threats and vulnerability; technical assessment & evaluation to support and complement the Government's technical experts in applying research, development test & evaluation (RDT&E) towards accomplishing the DHS mission.

1.2 Scope

The scope of this requirement is to provide the DHS S&T, OUP currently with professional scientific, technical and programmatic assistance and relevant administrative assistance services to support efforts in research, development, test and evaluation (RDT&E). Scientific and technical services may include advisory assistance support in technology scouting; vulnerability and risk assessment and mitigation; project justification and defense; program planning; evaluation and analyses of programs, projects, budgets and performance; and project execution, transition and commercialization. This also includes providing programmatic support in the development and preparation of acquisition and procurement documents. Administrative assistance may include providing ancillary support to advance the overall mission of the program office, through its project objectives, and conducting support activities and functions in order to sustain the day-to-day business practices of an organization. These services are comprehensively categorized as Systems Engineering and Technical Assistance (SETA) support services. As such, SETA support must expeditiously acquire the fundamental understanding of the department's (DHS) and S&T's overall and respective program offices' mission, practices, policies, and procedures; and respond professionally and promptly to mission needs within a demanding, challenging, and evolving environment.

1.3 Objective

The objective of this requirement is to acquire professional SETA services for S&T OUP with sufficient scientific background and business administration expertise to effectively support a full range of programmatic initiatives, inclusive of research, development, test and evaluation, as well as executing underlying budget and acquisition functions. To achieve the objective, the contractor shall meet the following requirements (details provided in Section 2.0):

- SETA REQUIREMENTS AND SKILL SETS- All contractor personnel must be able to respond quickly to requirements and tasks with stringent deadlines in a demanding and evolving R&D environment. Contractor personnel shall present and project professionally in demeanor, comportment and dress. Contractor personnel shall independently and proactively execute the coordination/completion of a myriad of business matters and therefore each contractor personnel shall be flexible, multi-talented; possess strong critical thinking abilities and judgement skills; and shall be sufficiently knowledgeable within the required technical area(s) of expertise and background; and possess complementary administrative skills to help successfully accomplish all programmatic functions assigned, and provide a comprehensive 360 degree assistance support at all times. The requirements also necessitate the ability to interact with various levels of people within and outside of the organization to obtain information. Therefore, the contractor personnel shall be familiar with and have the ability to be effective in a challenging R&D working environment, diligently mastering and managing priorities, and accurately communicating the preferences and philosophies of the directorate and their various program offices and clients. Strong interpersonal, organizational, analytical and planning skills are required and must be able to work with minimal guidance as well as collaboratively. Contractor personnel shall successfully integrate and coordinate all activities needed with all respective parties to execute the requirements specified within each task order. An integral part of successful performance is not only the production of quality products and services specified at the task order level, but the responsiveness of contractor personnel in the day-to-day business at hand. The end progress report, product or deliverable is as much vital to successful performance as is client interaction and responsiveness. Therefore, contractor personnel shall seek to ensure customer satisfaction is achieved and professional and ethical behaviors are maintained at all times. This skill set is comprised of requirements related to Six Task Areas and Surge Support:
    - TASK AREA ONE. Task Order Leadership/ Management (Refer to 2.1.)
    - TASK AREA TWO. Portfolio, Program and Project Assistance Support (Refer to 2.2)
    - TASK AREA THREE. Technology Transfer, Transition and Commercialization (Refer to 2.3)
    - TASK AREA FOUR. Program Office Support (Refer to 2.4)
        - Executive Administrative Assistance/ OUP Knowledge Management (Refer to 2.4.1)
        - Technical Editor and Communication (Refer to 2.4.2)
        - Budget and Strategy Support (Refer to 2.4.3)
    - TASK AREA FIVE. General Contractual Requirements (Refer to 2.5)
        - :Contract Management-and Subcontract Management (Refer to 2.5.1)
        - Transition Plans (Refer to 2.5.2)
    - TASK AREA SIX. Quality Control and Implementation (Refer to 2.6)

- SURGE SUPPORT- Contractor shall provide Technical/ Functional Programmatic Support. (Refer to 2.7)

1.4 Applicable Documents

The Contractor shall comply with requirements described in DHS Policies, Directives, and Guidance Memoranda, S&T's SP2's, OUP's written Standard Operating Procedures (SOPs), and adhere to government wide policies contained in the Federal Acquisition Register as appropriate. In addition, the Contractor should adhere to requirements contained in the following documents, updated as needed:

- OMB Circular A-110, Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations, relocated to 2 CFR Part 215.
- 45 C.F.R. Part 46, Subparts A-D, the DHS Management Directive (MD) for the Protection of Human Subjects (MD 026-04)

The following program specific SOP documents and guides may be helpful to the Contractor in performing the work described in this document:

- Center of Excellence Program
- Minority Serving Institutions Program
- Establishing a Center of Excellence
- Biennial Review Process
- COE Evaluation and Selection process
- OUP BOA Ordering Guide

2.0 SPECIFIC REQUIREMENTS AND TASKS

2.1 Task Area One. Task Order Leadership/ Management

Contractor shall designate a manager to oversee the daily initiatives and activities at the task order level. The Task Order Manager shall serve as the single point of contact for all contractor employees and shall be the liaison between the task order contractor staff and the task order Contracting Officer Representative. The Task Order Manager is responsible for ensuring the deliverables are met, progress is achieved in a timely manner, resolving all task order performance issues and readily engaging the task order Contracting Officer Representative whenever necessary, and overall managing contractor personnel and their time. The Task Order Manager shall also ensure there is no disruption in the quality of services to the government at any time, ensure record keeping, provide for successful transitions, and track and aid the IDIQ Program Manager in filling vacant positions in a timely manner at the task order level. The Task Order Manager is responsible for ensuring all of the overall task order requirements are met in accordance with the task order statement of work or performance work statement.

The designated Task Order manager for this task shall also conduct efforts under task requirements 2.2.3 Quality Control. Specifically, the Task Order Manager shall be responsible for the quality of the work

performed and shall ensure that the deliverables meet the quality established in the Quality Control Plan. The Task Order Manager will ensure that the work maintains the quality, timeliness, responsiveness and customer satisfaction.

2.2 Task Area Two. Portfolio, Program and Project Assistance Support

The principal function of S&T is to support Research and Development, and Test and Evaluation services to expand the understanding of current and new solutions. The Office of University program supports this S&T function and manages a complex and broad portfolio of scientific investments focused on the investigation, experimentation and evaluation of emerging science and technology in response to DHS Component needs. S&T OUP is organized in three focus areas:

- Centers of Excellence (COEs)- OUP manages ten lead COEs that form a consortium of hundreds of universities conducting research to address homeland security challenges.
- Education and Workforce Development (Ed&WF)- OUP has initiatives to education and train the current and future homeland security workforce in science and engineering professions.
- Minority Serving Institutions (MSIs)- OUP MSI programs aim to diversify the academic institutions involved in the homeland security mission. MSI programs include grants and cooperative agreements for Scientific Leadership and Summer Research collaborations that engage early career faculty and students with the COEs

SETA support providing assistance in project management to OUP shall be well-rounded and possess a wide range of diverse skillsets to meet project and programmatic needs. Since OUP manages Centers of Excellence with wide range of disciplines supporting the homeland security mission, SETA support personnel providing direct assistance to government technical experts in any office must be experienced in accomplishing all portfolio, program, and project related functions.

For Task Area Two, the contractor shall provide COE Program Analysis and Execution for all three focus areas within OUP. The contractor shall advise OUP Program Managers (PMs) on the overall planning and strategic direction of COEs and other OUP-funded performers. To support OUP in these areas, the contractor shall:

a. Execute mission needs and workload, independently. Quickly understand where authority lies in given scenarios when working with various stakeholders when consensus is not reached.
b. Assist in communication with stakeholders and other government service providers. Therefore, shall be capable of quickly familiarizing oneself with programmatic policies, procedures, processes and mission needs to assist with the execution of tasks.
c. Provide input and assistance in preparing project briefs, composing project reports and documents, and other project related materials; scheduling and assisting in organizing logistical support and hosting project-related meetings, reviews, and video or teleconferences.
d. Work with minimal guidance and diligently with various stakeholder to gather necessary information and must be able to take direction from the Government and timely implement

the necessary changes or edits. For example, SETA staff will be required to work closely with various government officials, such as portfolio and program managers, executive management officials, contracting officers, and other stakeholders, and may be required to address necessary changes based upon their review and comments. Must also be able to work with challenging and conflicting information to meet mission needs.

e. Assemble acquisition documents for purchase request packages. Shall possess comprehensive familiarity with the acquisition and procurement process to include understanding different assisted acquisitions and contract types, grants/ cooperative agreements and their purposes and potential uses. Assist with requirements such as conducting market research and composing meaningful, comprehensive market research reports, providing assistance in composing independent cost estimates based on contract types and the actual need related to the program mission, assist with acquisition planning and producing meaningful and comprehensive acquisition plans, etc.
f. Quickly understand technical needs and synthesize them in a comprehensive requirements document such as statement of works, performance work statements, statement of objective, etc., in plain English. Hence, shall understand the different contract types and acquisition document types and their purposes (e.g. working knowledge of how to prepare and understand the purpose of Determination and Finding (D&F) and Justification and Approval (J&A), and other procurement related documents).
g. Prepare documentation for modifications, tasks related to project and contract execution. This includes facilitating and assisting with closing out projects or contracts and interagency agreements. Establishes and maintains program contract files and records.
h. Assist in portfolio, program, project planning and control including tracking technical and fiscal performance, schedules, and government assigned action items; creating funding and budget documents; preparing project plans and milestones, status reports, monitoring the execution of the tasks for quality and against planned timelines.
i. Coordinate and track progress of R&D funding actions that facilitate portfolios, programs, projects execution; obtain funds status (commitment, obligation, expenditures); and be capable of monitoring expenditures. Assist in funds management and budget planning.
j. Keep records of all documents at the project level. Develop, refine and make available an archivable, searchable, indexed repository comprising official portfolio, program, and project records. Independently or under minimal guidance identify, collect, distill, organize, and maintain files of all program documents with availability the program office. May also require capturing best practices and lessons learned, and maintain currency of all records so the documents can be transitioned efficiently within the office.

2.3 Task Area Three. Technology Transfer, Transition and Commercialization

Complementary to the experience and acquisition capabilities described above, the SETA staff is required to possess sufficient technical knowledge to successfully assist OUP Director and PMs within a specific area(s) of the acquisition process. Requirements and details for this task include:

a. The contractor's effort in this area encompasses technology transfer and commercialization support and aids transition of products to end users. The contractor shall develop formal technology transfer, transition and commercialization agreements; assist with patent applications and intellectual property tracking and management; and exploit technology

scouting and market analysis to assess the potential for absorption of new products into the market place.

b. The contractor shall demonstrate detailed understanding of current systems and how such systems can be improved by the injection of new technologies, procedures, etc. The contractor shall develop and use mathematical models, prototypes, or both, in simulated environments to describe and enhance understanding of a system in context. The contractor shall apply systems engineering techniques and methods in support of technology development and acquisition efforts at all stages of the life cycle management process.

c. The contractor shall evaluate the performance of technology and non- material solutions in their intended operational context or a simulation thereof. This may involve close collaboration with the user community to understand requirements, to identify most relevant operational environment, and provide assistance in determining the potential acceptance by the user. This may also include refinement of established performance criteria in conjunction with the user and making further recommendations on engineering changes as necessary to meet user requirements. Activities may include support for: advanced technology demonstrations and advanced concept technology demonstrations. The contractor may be required to advise and make recommendations on integrating solutions into concept of operations, development of standard procedures, training material, and like thereof.

2.3.1 Additionally, the contractor shall provide SETA Technical Support to provide related analytical and engineering by conducting the following sub-tasks:

a. The contractor shall support Technology Foraging and Scouting. The contractor shall examine potential discoveries and forecast technologies and products that can advance homeland security capabilities to help S&T capitalize on existing and developing markets. The contractor's analysis shall support S&T's strategic and tactical R&D investment decision-making through research and analysis of technology markets and the public-private innovation landscape.

b. The contractor shall conduct investigative activities with the intention of improving existing or developing new products or procedures. This may include the development of new concepts based on the understanding of eventual operational context, conduct of market surveys, analysis of alternative solutions, demonstration of concepts feasibility, development of prototype that implements feasible concept.

c. The contractor shall conduct analysis to determine the feasibility of a concept or a prototype through a rational series of tests that measure a maturation of a concept against a set of requirements for the eventual use within an operational context. This will include the development of test plans and defining test environments. Requires understanding of user requirements as well as key elements of concept under evaluation. Incorporates analysis of data against defined test criteria, development and provision of test reports. Make recommendations on adequacy of concept or further required development of concept.

d. The contractor shall aggregate and assimilate knowledge, data, or both to extract meaningful content for application to a specific need or a variety of mission needs. This may include the development of repositories, curation of reports, creation of searchable data bases, and synthesizing data into summary reports of various types. This will also include the fusion of data through appropriate algorithms to support and inform meaningful decisions, analyses,

and recommendations.

e. The contractor shall analyze projects and programs to identify critical risk elements and susceptibilities to failure through an application of numerical approaches. The contractor shall identify and prioritize options available to reduce, monitor and control the likelihood or impact of failure in a critical process element. This may also include identifying options to increase the resilience of systems to unmitigated risks.

2.4 Task Area Four. OUP Office Support

OUP requires SETA staff to support overall S&T operations and execution. Task Area Four include 3 specific Sub Tasks: Executive Administrative Assistance/ OUP Knowledge Management, Financial Budget and Metrics and Communications and Outreach. SETA is required to possess sufficient technical knowledge to successfully assist OUP Director and PMs for OUP Office Support. Requirements and sub-tasks for this effort include:

2.4.1 Executive Administrative Assistance/ OUP Knowledge Management.

Contractor shall provide support assistance in coordinating, organizing and scheduling meetings, taking meeting notes and attendance. Coordinate program level taskings to the program office. Such tasking's may include congressional responses, testimony reviews; program data calls; organizing and assisting with office drills, office filing; office correspondence; tracking system; coordinating office requests, (e.g. IT issues, etc.). Contractor shall lead knowledge management effort and be responsible for managing archivable, repository comprising official S&T records, such as technical reports, requirement documents, technology transition agreements, memoranda, and other formal management records. Independently or under minimal guidance ensure there is an organized repository with, files of critical program documents with rapid availability to the Government.

2.4.2 Technical Editor and Communications.

Contractor shall serve as OUP Lead Communication Administrator. The Lead OUP Communication Administrator shall assist with the development of communication strategies, plans, and outreach. The. Contractor shall originate new or refine draft briefings, posters, newsletters, websites and other communications devices in accordance with prevailing DHS polices, templates, and guidance. Contractor shall possess expertise in standard graphic tools such as Adobe Photoshop and other specialty tools within the area of expertise. Contractor may perform video recording and editing and support content management on networks and platforms such as Facebook, Twitter, and YouTube. Contractor shall coordinate with all respective offices and personnel such as the Office of Corporate Communications in order to accomplish such tasks. Contractor shall coordinate publication of documents with the respective program offices, maintain records of cleared documents and those in progress.

2.4.3 Budget and Strategy Support.

The contractor shall designate a Sr. Budget Analyst for Budget and Strategy Support. The Sr. Budget Analyst shall maintain current year budgets and spend plans and support the development of future year budget and plans such as resource allocation plan, development of the President's budget request and other related requests. Monitor budget, ensure execution of funding is consistent with spending plans, analysis to identify variance from plans and recommend remediation actions. Provide recommendation to minimize future variance from

plans and, as required, advise management on all budget and funding issues. Support development of program strategy and prioritization of objectives for future funding. Maintain the database which tracks historical data for funds allocation, distribution, and obligation. Work collaboratively to provide office support, as required; maintain and monitor contract files relating to budget activities; review PR packages and provide quality review of acquisition related documents.

Additionally, the contractor shall provide SETA support to provide related OUP Office Support by conducting the following sub-tasks

a. Web Portal and Application Development. In accordance with DHS policies, contractor shall provide maintenance for collaboration site and build new capabilities, functions and utilities on applications (e.g. SharePoint 2013 (or later versions, Office 365, etc.) to enhance communications, collaboration and operational functions. Contractor shall maintain expertise in current versions of application and coordinate with offices to share and implement best practices. Contractor shall coordinate user requirements, conduct requirements gathering and analysis, and provide documentation support. Contractor shall keep records of, update or develop technical documents as to what was customized and why; or develop end user documents and provide user training, advise and consultation. Contractor may also require web design and development experience.
b. Other Subject Matter Experts. OUP may require contractor to provide highly specialized knowledge and expertise required to support S&T requirements or issues related to threats and vulnerability, policy and regulations, intelligence, and optimizing organizational processes and needs. Such support, for example, may require contractor to assist in the formulation or a reformulation of an S&T program, assistance with studies to inform major policy initiatives related to S&T, and provide strategic perspective or critical advice on high priority concerns or matters related to the homeland security enterprise.

2.5 Task Area Five. General Contractual Requirements

2.5.1 Contract Management and Subcontract Management.

The Contractor shall designate an Task Order Manager who shall be responsible for all the Contractor work performed in paragraphs 2.5.1, 2.5.2 and 2.6 (Surge Support). The Task Order Manager shall be a single point of contact for the Contracting Officer and the COR.

The contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to this requirement. The contractor must maintain continuity between the support operations at S&T, designated alternative sites and the contractor's corporate offices.

The contractor shall establish processes and assign appropriate resources to effectively administer this contract. The contractor shall respond to government requests for contractual actions in a timely fashion. The contractor shall have a single point of contact between the government and contractor personnel assigned to each task order contract. The contractor shall assign work effort and maintain proper and accurate time keeping records of personnel assigned to work task order requirements.

The contractor shall be responsible for any subcontract management necessary to integrate work performed on task order requirements and shall be responsible and accountable for subcontractor performance on task order requirements.

The prime contractor will manage work distribution to ensure there are no Organizational Conflict of Interest (OCI) considerations. Contractors may add subcontractors to their team at the discretion of and after notification to the task order Contracting Officer and COR.

2.5.2 Transition Plans.

The transition-in and out plans shall incorporate an inventory of all documents, procedures, materials and any and all information that is required to fully perform the services provided under a contract. The contractor is responsible for logging daily activities and exchanges between all respective parties and as such the contractor shall work diligently and professionally during the entire phase to identify all information and materials to be transitioned. The contractor shall develop milestones to be able to achieve successful transition of the identified information and materials. Finally, the contractor is responsible for executing the milestones to achieve successful transition of all items identified. The contactor is also responsible for coordinating a weekly briefing inclusive of all relevant parties. The meeting shall summarize all actions completed and in progress, including all information exchanged for the week with dates and times. The contractor shall obtain documented evidence of all parties agreeing to the results achieved at the conclusion of each meeting. Overall, the transition plans should talk to the detailed transition methodology in logical sequence to ensure a smooth transition of all tasks and subtasks of a contract without interruption or degradation of service levels; identify key transition events and objectives with a corresponding completion timeline; identify the associated risks and issues with risk mitigation strategies; and finally, identify the key individuals participating in the transition. The same transition principles apply at the micro level when individual contractor personnel are replaced during an active contract. The transition documents should be considered live documents that can be revised as the actual execution takes place to provide for flexibility to achieve a successful transition by the final date of the transition period. At any point that the contractors are uncooperative or unprofessional towards one another or the Government, the behavior will be reported in CPARS. When transitioning-in the contractor is responsible for ensuring all information is learned, and knowledge of the processes, documents and materials identified is retained to successfully carry on duties without interruption to government services. When transitioning-out the contractor is responsible for ensuring all information, knowledge of processes and contract activities, and documents are passed on successfully.

2.5.2.1 Task Order Transition Phase-In Plan. The contractor shall generate a Task Order transition-in plan. The details of the plan shall be refined at the task order kick-off meeting. The kick-off meeting ideally should happen prior to the contract effective date to ensure a smooth onboarding. The contractor shall provide a phase-in transition plan that describes how the contractor will transition without disruption to government operations. The task order level transition-in plan should be consistent with the master transition plan

incorporated at the IDIQ level. The phase-in period shall not exceed 30 calendar days for the transition during which the contractor shall overlap with the current contract. During the phase-in period, the contractor shall become familiar with performance requirements, establish responsibilities for the management of the tasks, and finalize the required plan. The plan must be detailed and include all activities that may be required to transition to full operational capability to successfully assume all duties under the contract. A near final draft plan must be provided to the government by the 2nd week of the 30-day transition period, for initial government review. At least a week before the final expiration date of a contract the contractor shall set up a meeting with the outgoing contractor and the task order Contracting Officer Representative(s) and Contracting Officer(s) to ensure all parties are in agreement of all actions taken and a successful transition has transpired.

2.5.2.2 Task Order Transition Phase-Out Plan. The contractor shall generate a transition-out plan. The contractor shall provide a phase-out plan at the task order level no later than 60 days prior to expiration of the task order. This phase-out plan shall be consistent with the master phase-out plan incorporated at the IDIQ level. An effective transition will be facilitated by the maintenance throughout contract execution of an accurate, current and 100% government accessible set of records for the program office. The contractor shall overlap with the incoming contractor during transition for a nominal period of 30 days and, work with government personnel and the incoming contractor to transfer all knowledge, information and documentation for all projects and tasks related to the contract. At least a week before the final expiration date of a contract the contractor shall set up a meeting with the outgoing contractor and the task order Contracting Officer Representative(s) and Contracting Officer(s) to ensure all parties are in agreement of all actions taken and a successful transition has transpired.

2.6. Task Area Six. Quality Control Plan and Implementation (QCP)

2.6.1 The contractor has a fundamental responsibility for the control of the work they perform. As a result, the contractor shall submit a Task Order Quality Control Plan for the Task Order that articulates a quality control system that ensures that the work performed meets contract requirements. The plan shall articulate how the contractor will measure, track, report and analyze contract performance. At a minimum, the QCP must include a self-inspection and a follow-up inspection plan; methodology for identifying and correcting problems; composition of QC team with identification of individual roles and responsibilities; and an outline of the procedures that the Contractor will use to maintain quality, timeliness, responsiveness, customer satisfaction, and any other requirements set forth within the terms and conditions of this contract.

2.6.2 The contractor shall implement the Task Order Quality Control Plan. The contractor shall measure, track, report and analyze contract performance. Contractor shall conduct quality control of all deliverables per the plan provided in 2.6.1. Each quarter contractor shall provide OUP a report detailing the deliverable provided, any rework requirements and assessment of the quality. The designated Task Order Manager in task 2.1. shall support this task requirement.

NOTE: Contractor shall notify the government of any and all problems encountered within 24 hours from time of discovery.

2.7 Surge Support

For this task 2.7, OUP requires SETA Surge Support that provides Technical Portfolio, Program and Project Assistance similar to 2.3 requirements and subtasks and 2.4 OUP Office Support.

2.7.1 The contractor shall provide the following Surge Support related to the requirements in 2.3 Technical, Portfolio, Program and Project assistance:

a. The contractor shall support Technology Foraging and Scouting. Discovers and forecasts technologies and products that can advance homeland security capabilities to help S&T capitalize on existing and developing markets. Supports S&T's strategic and tactical R&D investment decision-making through research and analysis of technology markets and the public-private innovation landscape.
b. The contractor shall conduct investigative activities with the intention of improving existing or developing new products or procedures. This may include the development of new concepts based on the understanding of eventual operational context, conduct of market surveys, analysis of alternative solutions, demonstration of concepts feasibility, development of prototype that implements feasible concept.
c. The contractor shall conduct analysis to determine the feasibility of a concept or a prototype through a rational series of tests that measure a maturation of a concept against a set of requirements for the eventual use within an operational context. This will include the development of test plans and defining test environments. Requires understanding of user requirements as well as key elements of concept under evaluation. Incorporates analysis of data against defined test criteria, development and provision of test reports. Make recommendations on adequacy of concept or further required development of concept.
d. The contractor shall demonstrate detailed understanding of current systems and how such systems can be improved by the injection of new technologies, procedures, etc. May require development and use of mathematical models, prototyping, or both, in simulated environments to describe and enhance understanding of a system in context. Applies systems engineering techniques and methods in support of technology development and acquisition efforts at all stages of the life cycle management process.
e. The contractor shall aggregate and assimilate knowledge, data, or both to extract meaningful content for application to a specific need or a variety of mission needs. This may include the development of repositories, curation of reports, creation of searchable data bases, and synthesizing data into summary reports of various types. This will also include the fusion of data through appropriate algorithms to support and inform meaningful decisions, analyses, and recommendations.
f. The contractor shall evaluate the performance of technology and non- material solutions in their intended operational context or a simulation thereof. This may involve close collaboration with the user community to understand requirements, to identify most relevant operational environment, and provide assistance in determining the potential acceptance by the user. This may also include refinement of established performance criteria in conjunction with the user and making further recommendations on engineering changes as necessary to meet user requirements. Activities may include support for: advanced technology demonstrations and advanced concept technology demonstrations. The contractor may be

required to advise and make recommendations on integrating solutions into concept of operations, development of standard procedures, training material, and like thereof.

g. The contractor shall support OUP Technology Transfer, Transition and Commercialization. The contractor's effort in this area encompasses technology transfer and commercialization support and aids transition of products to end users. This may include developing formal technology transfer, transition and commercialization agreements; assisting with patent applications and intellectual property tracking and management; and exploiting technology scouting and market analysis to assess the potential for absorption of new products into the market place.

h. The contractor shall analyze projects and programs to identify critical risk elements and susceptibilities to failure through an application of numerical approaches. The contractor shall identify and prioritize options available to reduce, monitor and control the likelihood or impact of failure in a critical process element. This may also include identifying options to increase the resilience of systems to unmitigated risks.

2.7.2 The contractor shall provide the following Surge Support related to the requirements in 2.4 OUP Program Office:

a. Graphics and Communications. Contractor shall assist with the development of communication strategies, plans, and outreach. Contractor shall originate new or refine draft briefings, posters, newsletters, websites and other communications devices in accordance with prevailing DHS polices, templates, and guidance. Contractor shall possess expertise in standard graphic tools such as Adobe Photoshop and other specialty tools within the area of expertise. Contractor may perform video recording and editing and support content management on networks and platforms such as Facebook, Twitter, and YouTube. Contractor shall coordinate with all respective offices and personnel such as the Office of Corporate Communications in order to accomplish such tasks. Contractor shall coordinate publication of documents with the respective program offices, maintain records of cleared documents and those in progress.

b. Web Portal and Application Development**.** In accordance with DHS policies, contractor shall provide maintenance for collaboration site and build new capabilities, functions and utilities on applications (e.g. SharePoint 2013 (or later versions, Office 365, etc.) to enhance communications, collaboration and operational functions. Contractor shall maintain expertise in current versions of application and coordinate with offices to share and implement best practices. Contractor shall coordinate user requirements, conduct requirements gathering and analysis, and provide documentation support. Contractor shall keep records of, update or develop technical documents as to what was customized and why; or develop end user documents and provide user training, advise and consultation. Contractor may also require web design and development experience.

c. S&T Knowledge Management for OUP. Contractor shall develop, refine and make available an archivable, searchable, indexed repository comprising official S&T records, such as technical reports, requirement documents, technology transition agreements, memoranda, and other formal management records. Independently or under minimal guidance identify, collect, distill, organize, and maintain files of all critical program documents with rapid

availability to the Government. May also require capturing best practices and lessons learned, and connecting user with the information available.

d. Other Subject Matter Experts. OUP may require contractor to provide highly specialized knowledge and expertise required to support S&T requirements or issues related to threats and vulnerability, policy and regulations, intelligence, and optimizing organizational processes and needs. Such support, for example, may require contractor to assist in the formulation or a reformulation of an S&T program, assistance with studies to inform major policy initiatives related to S&T, and provide strategic perspective or critical advice on high priority concerns or matters related to the homeland security enterprise

3.0 CONTRACTOR PERSONNEL

3.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in the SOW.

3.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence. Otherwise the contractor shall provide a fully qualified replacement.

3.3 Key Personnel

Before replacing any individuals designated as KEY by the Government, the Contractor shall notify the Contracting Officer and the COR no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the KEY person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace KEY Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as KEY for this requirement. Note: The Government may designate additional Contractor personnel as KEY at the time of award.

Key Personnel for this Task Order are:

- (b)(6), (b)(4)
- (b)(6), (b)(4)
- (b)(6), (b)(4)

Contractor KEY personnel shall not be assigned by the Contractor to more than one position for this requirement.

3.4 Key Personnel Duties

3.4.1 (b)(4) The Contractor shall provide a (b)(4) who shall be responsible for the daily operations of the work performed under this SOW. The (b)(4) shall directly report to the IDIQ Program Manager. It is anticipated that the (b)(4) shall be one of the senior-level employees provided by the Contractor for this work effort. The name of the (b)(4) and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the (b)(4) shall be provided to the Government as part of the Contractor's proposal. The (b)(4) is further designated as KEY by the Government. During any absence of the (b)(4), only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The (b)(4) and al designated alternates shall be able to read, write, speak and understand English. Additional the Contractor shall not replace the (b)(4) without prior approval from the Contracting Officer. The (b)(4) (b)(4) shall be available to the COR via telephone between the hours of 8:30am and 5:30PM (ET), Monday through Friday and shall respond to a request for discussion or resolution of daily technical problems within 8 hours of notification.

3.4.2 (b)(4) The Contractor shall provide a (b)(4) who will serve as the primary.lead for supporting DHS OUP in financial and performance management. This includes providing direct support to OUP leadership in developing management spreadsheets to track financial processes, coordinating with the DHS S&T Finance and Budget Division and the DHS Office of Procurement Operations to support tracking and document processing, and coordinating the DHS OUP Contractor team prepare financial and milestone information. The Senior Budget Analyst shall work with all DHS OUP Program Managers and Contractor Team members in the development and implementation of standard financial and milestone reporting and tracking procedures. Paragraph 2.4.3 includes the task requirements for the (b)(4) (b)(4)

3.4.3 (b)(4) The Contractor shall provide a (b)(4) to serve as OUP Lead Communication Administrator. The OUP Lead Communication Administrator shall provide a mix of program support, marketing, and administrative duties that assist DHS OUP execute its mission. This includes building relationships with external scientific organizations to leverage funding, tracking performer's milestones, developing communication and marketing outreach strategies and implementing these communication and marketing outreach strategies. The Lead Communication Administrator shall coordinate publication of documents with the respective program offices, maintain records of cleared documents and those in progress and coordinate with all respective offices and personnel such as the Office of Corporate Communications in order to accomplish tasks. Paragraph 2.4.2 includes the task requirements for the Lead Communication Administrator.

4.0 OTHER APPLICABLE CONDITIONS

4.1 Security

Contractor access to sensitive information is required under this SOW. The contractor shall comply with the terms of HSAR Class Deviation 15-01.

Contractor access to classified information is required under this SOW. The maximum level of classification is **SECRET**. Classified storage is not required.

All on-site personnel that are supporting this SOW shall be able to obtain and maintain a **SECRET** clearance.

The Government reserves the right to approve or deny suitability of the Contractor's individual employees based on security risks, unsatisfactory performance, or disruptive influence to mission accomplishment.

All services provided under this TO must be compliant with DHS 4300B DHS National Security System Policy and the DHS 4300B National Security System Handbook. Additionally, where there is a requirement for encryption, all encryption shall be FIPS 197 Advanced Encryption Standard (AES) that has been FIPS 140-2 certified.

Requirements for Handling Sensitive and/or Proprietary Information. The Contractor shall comply with all Government standards for handling sensitive and/or proprietary information, as listed on the DD Form 254 and briefed by DHS/S&T. Contractor personnel may be required to access the Homeland Secure Data Network (HSDN) and/or the Joint Worldwide Intelligence Communications System (JWICS) to accomplish tasks in the SOW. Personnel will comply with all access policies for those networks.

DHS has and will exercise full control over granting, denying, withholding, or terminating unescorted Government facility, Government systems and/or sensitive Government information access for Contractor employees, based upon the results of a DHS fitness (suitability) investigation. DHS may, as it deems appropriate, authorize and make a favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the contactor to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment Contractor fitness (suitability) authorization will follow as a result thereof. The granting of a favorable EOD decision or a full Contractor fitness (suitability) authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order. No employee of the Contractor shall be allowed unescorted access to a Government facility, access to any sensitive information or access to DHS Systems without a favorable EOD decision or Contractor fitness (suitability) determination by the DHS Office of Security. Contract employees assigned to the task order not needing access to sensitive DHS information, DHS systems or access to DHS facilities will not be subject to

security Contractor fitness (suitability) screening. Contract employees waiting an EOD decision may not begin work on the task order. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings, nonrecurring meetings, and begin transition work. Classified information is Government information which requires protection in accordance with Executive Order 13526, National Security Information (NSI) as amended and supplemental directives. If the Contractor has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. If the Contractor is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

4.2 Protection of Information

Safeguarding of Sensitive Information (HSAR Deviation 15-01, March 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*.

VI. Information Technology Security and Privacy Training (HSAR Deviation 15-01, March 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. For purposes of this section, references to the "Contractor" shall mean START.

(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.

4.3 General Report Requirements

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications).

Attachment J-2

DELIVERABLES

It is up to the contractor to manage their resources to maximize value to meet the deliverables on the government's timeline.			
Name & Format	**Deliverable Description**	**Frequency of Deliverables**	**SOW Reference Number**
1) Task Order (TO) Deliverable. (electronic files)	The contractor shall provide electronic copies of the following: • all copies of current awards and modifications received during the reporting period. • task order chart – chart detailing all modifications made to date including: POP, funding and date of modification. • signed NDA agreements for personnel brought on during the reporting period to include form 11000-6, Supplemental Form SETA III NDA, Contractor disclosure of interests per FAR clause 52.203-16. • any known information on anticipated TO modifications	15th day of each month once contract awarded. If the 15th calendar day falls on a weekend or holiday, the report is due the following business day.	Section 2. Subsection 2.1. Task Order Manager Subsection 2.5 Contract and Subcontract Management
	• Excel worksheet compiling financial status aggregating information across all TOs and per TO by CLIN (or as requested) included (original) planned, actual expenditures to date and projected expenditures • summary of resolved, pending and emerging issues • status on vacancies, replacements and onboarding of staff per TO		

It is up to the contractor to manage their resources to maximize value to meet the deliverables on the government's timeline.			
Name & Format	**Deliverable Description**	**Frequency of Deliverables**	**SOW Reference Number**
	and across all TOs • Travel: SETA names, government beneficiary official, purpose of travel for SETA, location of travel, duration of travel, event location, and event name. List & corresponding information above must be provided in Excel worksheet for the reporting period. • ODCs: Itemized list of what was or will be purchased, purpose of purchase, name of government official authorizing the purchase, name of SETA purchaser. List & corresponding information above must be provided in Excel worksheet for the reporting period. • Point of contact chart with TO PM contact information including, e- mail and phone and IDIQ Manager contact information. The deliverable shall also include any other information concerning topics that affect the task depending on current events that transpire. • The TO contract deliverable shall be accompanied by a cover letter on company letterhead. The cover letter shall describe the contents of the complete package.		

It is up to the contractor to manage their resources to maximize value to meet the deliverables on the government's timeline.			
Name & Format	**Deliverable Description**	**Frequency of Deliverables**	**SOW Reference Number**
2) Meeting with TO COR	• Discuss information provided in deliverable #1. • Provide TO meeting agenda 24 hours in advance of meeting. • Provide meeting minutes to TO COR no later than 5 days after meeting.	2nd and 4th Wednesday of the month once contract awarded.	Section 2. Subsection 2.1. Task Order Manager
3) Task Order (TO) Transition Plans in Word Document	• Phase-In Transition Plan • Phase-Out Transition Plan	Transition In plan within one month of TO start date Transition Out plan within three months of planned TO end date.	Section 2. Subsection 2.5.2 Transition Plans
4) Quality Control Plan in Word Document	• Quality Control Plan that discusses a systematic approach to how services provided to the Government will be monitored, tracked and analyzed and improved.	Plan must be submitted within 15 days after TO award.	Section 2. Subsection 2.6 Quality Control Plan and Subsection 2.1 Task Order Manager
5) Report for OUP Portfolio, Program and Projects	• Technical/ scientific analysis comparing DHS requirements and needs and performer proposals including recommendations to improve the proposals	Report must be submitted within 3 weeks of request	Section 2. Sub-sections 2.2 and 2.3

It is up to the contractor to manage their resources to maximize value to meet the deliverables on the government's timeline.			
Name & Format	**Deliverable Description**	**Frequency of Deliverables**	**SOW Reference Number**
6) Acquisition and Procurement Request (PR) Documents for OUP Projects	• Documentation for OUP to support PRs and acquisition	Within 1 week of request	Section 2. Sub-sections 2.2, and 2.4
7) Report- White Paper	• Report analyzing COE annual reports submitted at the end of each fiscal year and project reports, including assessments of COE performance in all required areas identified in COE award terms and conditions	Within 2 weeks of request	Section 2. Sub-sections 2.2 and 2.3.
8) Portfolio, Program and Project Reports, Brief and Meeting Materials	• Presentation on DHS OUP initiatives, programs, and projects	Frequent throughout the year.	Section 2. Sub-sections 2.2, 2.3.and 2.4

It is up to the contractor to manage their resources to maximize value to meet the deliverables on the government's timeline.			
Name & Format	**Deliverable Description**	**Frequency of Deliverables**	**SOW Reference Number**
9) MS Word documents including list of attendees and their affiliation, highlights of meetings and action items	• Meeting minutes (Electronic)	Within 2 days of event	Section 2. Sub-sections 2.2, 2. 3.and 2.4
10) Program and Project Tracking/ Milestone and Status Reports and Recommendations for Corrective Actions	• DHS OUP Program Documents	Within 5 days of request	Section 2. Sub-sections 2.2, 2.3.and 2.4
11) OUP Portfolio Reporting for Senior Leadership, Congress and Public.	• Report on topics to include: finance, budget, metrics, accomplishments.	Within 5 days of requests	Section 2 Sub-section 2.4

It is up to the contractor to manage their resources to maximize value to meet the deliverables on the government's timeline.			
Name & Format	**Deliverable Description**	**Frequency of Deliverables**	**SOW Reference Number**
12) Tech Foraging/ Scouting Reports, Test and Evaluation Planning documents and Technology, Transition Reports	• Technical Reports and Material • .	Within 10 days of request	Section 2. Sub-sections 2.2 and 2.3, 2.7
13) Surge Support	• Technical reports providing Market Analysis, Analysis of Alternatives and other Studies analyzing emerging trends, risks, and future environments	Per Surge Schedule	Section 2 Subsection 2.7
14) Quality Control Report	• Report providing the metrics for deliverables per the Quality Control Plan submitted (see Deliverable #4).	Quarterly.	Section 2. Subsection 2.6 Quality Control Implementation and 2.1 Task Order Manager

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

I,_____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials:	**Protected Critical Infrastructure Information (PCII)**

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials:	**Sensitive Security Information (SSI)**

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.

Initials:	**Other Sensitive but Unclassified (SBU)**

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, 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 or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific c categories of information to which I am granted access.

3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific c categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.
(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.
(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.
(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Signature:

This form is not subject to the requirements of P.L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.