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

1. REQUISITION NUMBER	PAGE	OF
RSMC-20-00005	1	4

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
70RSAT19D00000003		70RSAT20FR0000048	70RSAT20R00000011	03/16/2020

7. FOR SOLICITATION INFORMATION CALL:	(b)(6)	8. OFFER DUE DATE/LOCAL TIME
		ET

9. ISSUED BY	CODE	10. THIS ACQUISITION IS
U.S. Dept. of Homeland Security Office of Procurement Operations S&T Acquisition Division 245 Murray Lane, SW, #0115 Washington DC 20528-0115	DHS/OPO/S&T/E	☒ 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
☒ SEE SCHEDULE	Net 30	☐	14. METHOD OF SOLICITATION ☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO	CODE	16. ADMINISTERED BY	CODE
		U.S. Dept. of Homeland Security Office of Procurement Operations S&T Acquisition Branch 245 Murray Lane, SW, #0115 Washington DC 20528-0115	DHS/OPO/S&T/S&T

17a. CONTRACTOR/ OFFEROR	CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
NOBLIS INC ATTN (b)(6) 2002 EDMUND HALLEY DR RESTON VA 20191 TELEPHONE NO. 7036102290	9329023640000		DHS ICE Burlington Finance Center PO BOX 1000 Attn: S&T Division Williston VT 05495-1000	DHS-S&T-INV

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

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 Division: Office of Mission and Capability Support Performer: Noblis, Inc. DHS Primary COR: (b)(6) DHS Alternate COR: (b)(6) The purpose of this action is to award a Time and Materials Task Order off of the SETA III IDIQ 70RSAT19D00000003 with Noblis. This task order will provide Systems Engineering and Technical Assistance (SETA) support services to the DHS S&T *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
See schedule	(b)(4)

☐ 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
	Office of Mission and Capability Support (MCS) for Front Office Support. The period of performance is a base period of twelve (12) months and two (2) twelve (12) month option periods. As a result of this action, the Base Period (CLINs 0001, 0002, and 0003) is fully funded. Base Period Optional CLIN 0004 is partially exercised in the amount of 5,760 hours. Option Periods 1 (CLINs 1001-1002) and 2 (CLINs 2001-2002) will remain unexercised and unfunded. The total obligated amount is (b)(4) Attachments: 1. Terms and Conditions (8 pages) 2. Statement of Work (13 pages) 3. Pricing Table (3 pages) 4. Task Order Clauses (12 pages) ---- Delivery: 1 Days After Award Period of Performance: 05/27/2020 to 05/26/2023				
0001	Base Period Tasks 1-4 12 Months 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	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

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)
	In accordance with the Pricing Table Accounting Info: NONE000-000-J0-63-96-07-100-35-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
0002	Base Period Travel and Other Direct Costs Travel NTE: (b)(4) ODCs NTE: (b)(4) 12 Months Accounting Info: NONE000-000-J0-63-96-07-100-35-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				(b)(4)
0003	Base Period Task 5 12 Months In accordance with the Pricing Table Accounting Info: NONE000-000-J0-63-96-07-100-35-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-65-04-13-001-36-01-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				(b)(4)
0004	Base Period Task 6 Surge Support - Optional 12 Months In accordance with the Pricing Table Base Period Exercise - (b)(4) hours total Senior Portfolio/Program/Project Analyst (b)(4) hours (b)(4) hours remains unexercised and unfunded Continued ...				(b)(4)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Total Line Item Value: (b)(4) Accounting Info: NONE000-000-J0-65-04-13-001-36-01-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
1001	Option Period 1 Tasks 1-4 12 Months In accordance with the Pricing Table Amount: (b)(4) (Option Line Item)				(b)(4)
1002	Option Period 1 Travel and Other Direct Costs Travel NTE (b)(4) ODCs NTE: (b)(4) 12 Months Amount: (b)(4) (Option Line Item)				(b)(4)
2001	Option Period 2 Tasks 1-4 12 Months In accordance with the Pricing Table Amount: (b)(4) (Option Line Item)				(b)(4)
2002	Option Period 2 Travel and Other Direct Costs Travel NTE: (b)(4) ODCs NTE: (b)(4) 12 Months Amount: (b)(4) (Option Line Item)				(b)(4)
	The total amount of award: $7,458,652.20. The obligation for this award is shown in box 26.				

SETA III SOLICITATION AND TASK ORDER TEMPLATE

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

1. REQUIREMENT TITLE:

Office of Mission and Capability Support Front Office Support

2. PROCUREMENT INSTRUMENT IDENTIFIER:

70RSAT20FR0000048

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:

Please include both contacts in communications related to this opportunity.

5. ISSUE DATE:

5.1. Notice Type: Task Order Award

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

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

5.3. Issuance Date: Thursday, May 21 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 12 months from date of award.

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

Option Period	Duration (in Months)
Option Period 1	12 months
Option Period 2	12 months

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 5/27/2020 through 5/26/2023.

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:

(b)(6)

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 (b)(6) 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 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 36 months.

(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:

Task Order Manager- (b)(6)

(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.

SETA III SOLICITATION AND TASK ORDER TEMPLATE

ATTACHMENTS

Number	Title	# of Pages
(1)	Statement of Work	13
(2)	Pricing Table	3
(3)	Task Order Clauses	12

DEPARTMENT OF HOMELAND SECURITY (DHS)

STATEMENT OF WORK (SOW)
FOR
Systems Engineering & Technical Assistance (SETA) Support to the Office of Mission and Capability Support (MCS) Front Office

1.0 GENERAL

1.1 BACKGROUND

In support of the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, the Office of Mission and Capability Support (MCS) executes Research, Development, Test and Evaluation (RDT&E) to transition technologies, knowledge products, and solution approaches in support of its DHS Component customers, Federal, State, Local Tribal and Territorial (FSLTT) first responders, and the larger Homeland Security Enterprise (HSE).

MCS is the S&T Office that executes Research, Development and Innovation (RD&I) funding to find or develop solutions to fulfill DHS component operational requirements. MCS covers all DHS mission areas, and serves 13 discrete customer portfolios. Programs and Projects managed by MCS Program Managers and supported by matrixed staff from throughout the other Offices of S&T often serve multiple customers. It is this matrixed nature of S&T's operations that highlights the value of a centralized R&D coordinating function for the Department.

S&T's Core Mission areas mirror the Department's, and the MCS Programs and Projects address customer requirements in those areas accordingly. They are:

- Counter Terrorism and Homeland Security Threats
- Secure U.S. Borders and Approaches
- Secure Cyberspace and Critical Infrastructure
- Preserve and Uphold the Nation's Prosperity and Economic Security
- Strengthen Preparedness and Resiliency
- Champion the DHS Workforce and strengthen the Department

1.2 SCOPE

The MCS Front Office requires support to conduct oversight and management of its RDT&E portfolio and facilitate its efforts to analyze, introduce, and enhance technological products, services, systems, and capabilities to S&Ts customers. This Statement of Work provides for Systems Engineering and Technical Assistance (SETA) to the MCS Front Office that includes strategy development, portfolio administration and oversight, stakeholder engagement and communications, reporting and data call management, property and records management support, and business operations and financial management support.

These support functions include program analysis, tracking, and reporting; program and communication coordination; high-level technology research and technical feasibility assessments; program budget assessment and analysis; and studies and analysis related to program management, engineering, and technical services for current and proposed MCS programs. A detailed breakdown of the tasks by functional areas is listed below

1.1 OBJECTIVE

The objective of this solicitation is to establish a task order for SETA support to the MCS Front Office (FO). The successful procurement of these services will support the efficient and effective execution of a matrixed portfolio of RDT&E in support of S&T customers and Homeland Security Enterprise.

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 TASK ONE. Task Order Management (Key Personnel)

The Contractor shall provide task order management functions, to include the planning, coordination, technical direction, and surveillance of the activities necessary to assure disciplined work performance and timely resources application to accomplish all tasks under this task order. The Contractor shall at a minimum perform the following tasks:

- Provide a Project Management Plan (PMP) to outline how the task order will be managed.
- Be responsible for maintaining communication with the Contracting Officer (CO) and Contracting Officer's Representative (COR), and to immediately notify both the CO and the COR of any problems that would prevent timely performance of all tasks.
- Establish, implement, and maintain technical management and oversight of all work performed under this SOW.
- Assure the technical excellence, cost effectiveness, and timeliness of all required work and deliverable products.
- The Contractor's Task Order Manager shall be act as the Contractor's single point of contact for all technical and administrative matters related to this task order and shall administer, manage and possess the necessary authorities over all contractor personnel including consultants and subcontractors and unfettered access to actual services performed and hours billed. The task order manager shall establish, implement and maintain management control systems required to plan, organize, direct, and control task order activities. The Contractor's management systems should track and monitor the status of all tasks assigned, from planning to completion, track deliverables, and record projected and actual resources expended on each task. This data should be presented in the Monthly Progress Report.
- Provide the overall management effort required to integrate operational and programmatic functions necessary to perform all tasks and effectively administer the task order. The contractor shall perform contract management duties including, but not limited to, meetings with the COR as deemed necessary regarding all aspects of the task order, establishing and maintaining staffing requirements, reviewing budget

estimates, contractor invoicing and activity reports, sub-contractor invoicing and monthly activity reports, management of task order level activities, development and revisions to spend plan, coordination on new requirements, scopes of work, and response to staffing needs.

- Provide a Task Order Transition In/Out Plan to manage a 90 day transition in/out. This plan shall be in accordance with Attachment I of the Contractor's SETA III IDIQ.

2.2 TASK TWO. Tasking & Records Management Coordination

MCS has a high volume of taskings, data calls, FOIA requests, Congressional Inquiries, Request for Information, Queries for the Record, and other communication streams for regular and ad hoc reporting throughout S&T, the Department, and the larger governmental apparatus. This task will maintain coordination of those information flows and will maintain MCS FO records, and a contractor under this task will serve as the MCS POC to attend Records Management (RM) meetings and coordination of RM requirements and information to MCS personnel. The contractor shall perform the following tasks.

- Support the review and clearance of internal and external S&T MCS communications including: briefs, meeting agendas and read-ahead's, white papers, program fact sheets and quad charts, senior leadership correspondence, year in review, and other artifacts.
- Assist in the review/clearance of inbound and outbound inquires, requests, and documents from the Office Executive Secretariat /or S&T Front Office that have MCS equities; responses to congressional questions for the record that convey the current status of projects within S&T to congress and other government representatives; review signed letters, memos, and plans from component heads or other agencies; taskers that commit the directorate to actions or dedicate resources; read-ahead items that will be used by DHS leadership (i.e., DHS Secretary, S&T USST) for upcoming meetings or briefings with key stakeholders/or customers. Such services are limited by the IDIQ's H.11 clause: Disclosure and Avoidance of Inherently Governmental Functions.
- Review MCS subject matter expert (SME) input for taskers; offer a concurrence or request that the SMEs expand on the subject or answer questions from leadership.
- Review between 10-20 daily action items with varying due dates and necessary approvals each week.
- Coordinate MCS RM requirements in support of the MCS Federal Records Management POC in accordance with Applicable DHS Management Directives (available at http://www.dhs.gov/department-homeland-security-management-directives)
- Communicate Records Management Policy and provide records management guidance to MCS personnel in coordination with the DHS S&T Records Management Officer.
- Host one-on-one and small-group training sessions, in-person or via electronic medium (webinar, Lync messenger, etc.) for MCS personnel regarding S&T Records Management processes and requirements.

- Attend the regularly-scheduled S&T Records Management meetings to remain current on RM policy, and report new policy information to the MCS Front Office and MCS Staff as it is published.
- Maintain DHS records (hardcopy and electronic) in accordance with applicable DHS Management Directives and S&T Standard Operating Procedure System (SP2s)
- Coordinate MCS Property Management requirements in support of the MCS Federal Property Management POC in accordance with Applicable DHS Property Directives (available at http://www.dhs.gov/department-homeland-security-management-directives)
- Communicate Property Management Policy and provide property management guidance to MCS personnel in coordination with the DHS S&T Property Management Officer. Host one-on-one and small-group training sessions, in-person or via electronic medium (webinar, Lync messenger, etc.) for MCS personnel regarding S&T Property Management processes and requirements.
- Attend the regularly-scheduled S&T Property Management meetings to remain current on Property Management policy, and report new policy information to the MCS Front Office and MCS Staff as it is published.
- Facilitate and/or conduct execution of the annual Accountable Property inventory.

2.3 TASK THREE. Executive Assistance

MCS Requires Executive Assistants to coordinate calendars, schedule meetings, book rooms, manage and coordinate travel, route documents for signature, liaise with S&T leadership support staff, and otherwise ensure the full functionality of MCS Front Office. The contractor shall perform the following tasks.

- Perform routine executive-level tasks for the MCS Front Office Staff to include but not limited to scheduling, drafting internal memos, filing, intranet website maintenance, and coordinating MCS Front Office daily operations.
- Manage and maintain MCS Front Office staff calendars, phones, and arrange meetings and conference calls to include scheduling with other attendees, scheduling conference rooms, and off-site meetings.
- Arrange travel for MCS Front Office staff to include domestic, international, and invitational travel.
- Support senior staff personnel in the development of organizational goals and implementation plans.
- Provide strategic analysis and support to the MCS Front Office staff supporting MCS outreach and strategic vision.

2.4 TASK FOUR. Business & Property Management Support

MCS requires support in maintaining and executing its business and financial processes. Support will be based around the coordination and communication of the annual MCS appropriation, and in supporting the oversight and tracking of MCS property management. The contractor shall perform the following tasks.

- Provide office administrative support for the MSC senior management team.
- Review MCS documents for grammar, structure and clarity.
- Provide analysis and preparation of financial reports, presentations, graphs, tables and charts and other documentation.
- Provide financial management support to the MCS FO, including coordinating all financial data calls and reviews between MCS and the Financial Budget Division. This also includes yearly budgets; spend plans; budget impact statements; mid-year reviews; Verification and Validation cycles, milestones and measurements, and other required budget cycle data calls and activities.
- Assist in managing data-calls to include coordinating all inputs from MCS staff and collating all required data for review and submission. Assist in the review/clearance of inbound and outbound inquires, requests, and documents from the S&T Executive Secretary, S&T Front Office or the Office of Legislative Affairs that have MCS enquiries; signed letters, memos, and plans from component heads or other agencies; actions or assigned tasks that commit the directorate to actions or dedicate resources; read-ahead items that will be used by DHS leadership (i.e., DHS Secretary, S&T USST) for upcoming meetings or briefings with key stakeholders/or customers. Such services are limited by the IDIQ's H.11 clause: Disclosure and Avoidance of Inherently Governmental Functions.
- Document and provide implementation support for strategies to effectively support MCS's integration with other key S&T stakeholders, private industry, national labs, university community, and other intergovernmental R&D organizations.
- Serve as a MCS web manager and Share Point administrator, posting various information such as technical documents, notices, bulletins, calendar items, and other documents, as needed. The contractor shall provide web support to MCS senior leadership and give recommendations on publishing web content to the both the internal and external facing IT systems.
- Support the MCS Front Office in its collaborative efforts with other S&T Offices to communicate, track, and ensure program management best practices are followed by S&T Program and Project managers as S&T continues to install and refine its revised business process flow. Support shall encompass:
    - Drafting and distributing meeting notes,
    - development and distribution of meeting agendas,
    - drafting required documentation, and
    - collection, organization and storage of program and office artifacts.

2.5 TASK FIVE. Strategic Mission Manager and Portfolio Manager Support BASE PERIOD ONLY

MCS requires support to allow the Strategic Mission Managers and S&T Portfolio Managers to integrate fluidly with MCS, other parts of S&T, and DHS at large. These administrative support personnel will help manage calendars, workloads, tasking and reporting, communication and similar endeavors. The contractor shall perform the following tasks.

- Provide office support.
- Provide analysis and preparation of reports, presentations, graphs, tables and charts.
- Review documents for grammar, structure and clarity.
- Assistance in managing and responding to S&T Executive Secretary data calls.
- Provide executive-level support to Strategic Mission Managers in planning, assessment, and advice in the following areas: strategic and operational planning, infrastructure enhancement, and conceptual development.
- Provide support to Portfolio Managers in their continued engagement with DHS S&T customers on the receipt, prioritization, and regular reporting of their operational capability gaps.
- Provide graphics design, printing, publishing, wide format imaging and photographic support services in support of S&T communications.
- Assist in maintaining records (hardcopy and electronic).

2.4 TASK SIX: Surge Support OPTIONAL

The Contractor may be required to provide additional support under Task Five as described in the base period, depending on the level of effort required. These tasks shall be reimbursed on a Time and Materials basis subject to the labor categories and hourly rates contained in the pricing schedule and the terms of the modification authorizing the work.

3.0 CONTRACTOR PERSONNEL

3.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this 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 individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 14 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.

Task Order Manager

3.4 Task Order Manager (Task 1)

The Contractor shall provide a Task Order Manager (TOM) who shall be responsible for all Contractor work performed under this SOW. The TOM shall be a single point of contact for the Contracting Officer and the COR. It is anticipated that the TOM shall be one of the senior level employees provided by the Contractor for this work effort. The name of the TOM, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the TOM, shall be provided to the Government as part of the Contractor's proposal. The TOM is further designated as *Key* by the Government. During any absence of the TOM, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The TOM and all designated alternates shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the TOM without prior approval from the Contracting Officer.

3.4.1 The Task Order shall be available to the COR via telephone between the hours of 0900 and 1700 EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification.

3.5 Employee Identification

3.5.1 Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

3.5.2 Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones,

in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

3.6 Employee Conduct
Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

3.7 Removing Employees for Misconduct or Security Reasons
The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

4.0 OTHER APPLICABLE CONDITIONS

4.1 SECURITY

Contractor access to classified information is required under this SOW. Contractor access to classified information is required under this SOW. The maximum level of classification is Top Secret. The details will be specified in a Department of Defense (DD) Form 254.

The following security clearances will be required.

Task	LCAT	Clearance Lvl	Time Needed
Task 1	Task Order Manager	Public Trust	Day 1
Task 5	Senior Portfolio/Program/Project Analyst	4 FTE @ TS	Day 90

4.2 PERIOD OF PERFORMANCE
The period of performance for this contract is a one-year base period with two one-year option periods as follows:

Base Period	*12 months*
Option Period One	*12 months from option exercise*
Option Period Two	*12 months from option exercise*

4.3 PLACE OF PERFORMANCE

The primary place of performance will be at the Department of Homeland Security at (b)(6) (b)(6) (hereby referred to as VTA). Telework will be allowed under this task order with prior COR approval.

4.4 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 0700 and 1730 EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

4.5 TRAVEL

Contractor travel shall be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

4.6 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 15 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held at the Government's facility, located at VTA or via teleconference.

4.7 PROJECT PLAN

The Contractor shall provide a draft Project Management Plan as part of their proposal for review as a factor within the evaluation process. The Contractor shall provide a final Project Plan to the COR not later than 30 business days after Award.

4.8 BUSINESS CONTINUITY PLAN

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 30 business days after the date of award, and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- How the Contractor will communicate with the Government during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
    - Telephone numbers
    - E-mail addresses

4.8.1 Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 24 hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life threatening emergency, the COR shall immediately make contact with the TOM to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, the TOM and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

4.8.2 The COR and TOM shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

4.9 PROGRESS REPORTS

The TOM shall provide a *monthly* progress report to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

4.10 PROGRESS MEETINGS

The TOM shall meet with the COR on a *monthly* basis to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at VTA.

4.11 TRANSITION IN/OUT PLANS

The Contractor shall provide a draft Transition In Plan with their proposal addressing the task order transition methodology, processes, staffing, key milestones, and schedule to assure a complete, effective and efficient transition of task order requirements from the incumbent within 90 days of task order award that is in accordance with Attachment I Master Transition Plan of the Contractor's SETA III IDIQ. The Contractor shall provide a final Transition In Plan to the COR no later than 5 business days following the Post Award Conference.

The Contractor shall support and cooperate with MCS and its designated agents. During the task order transition period, the Contractor shall coordinate and support daily status meetings with MCS to ensure transition is on track for timely completion. MCS expects the low-risk, phased-in, smooth and seamless transition to occur during non-peak hours with no disruption to its operations or those of other contractors supporting MCS. The COR shall coordinate transition

efforts among current service providers and the Contractor. MCS will provide the Contractor with the information and data to effect transition to the performance expectations under the task order.

Task Order transition shall be deemed successfully completed when the Contractor has demonstrated that it is prepared to assume full day-to-day performance of the task order. These activities may occur during normal business hours provided they are scheduled ahead of time to minimize interruptions to day-to-day work requirements. The Contractor shall provide a final transition checklist to the COR indicating that it has successfully completed all transition activities and it is ready to assume full performance of the task order.

The Contractor shall also provide a final Transition Out Plan to the COR to allow for a 90 day transition out at the end of the task order upon COR request.

4.12 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 10 and Microsoft Office Applications).

4.13 PROTECTION OF INFORMATION

Contractor access to information protected under the Privacy Act is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

4.14 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

5.0 GOVERNMENT TERMS & DEFINITIONS

5.1 COR – Contracting Officer's Representative
5.2 DHS – Department of Homeland Security
5.3 MCS – Office of Mission and Capability Support
5.4 S&T – Science and Technology (S&T) Directorate

6.0 GOVERNMENT FURNISHED RESOURCES

The Government will provide the workspace, equipment and supplies necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement.

The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this contract, and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear.

The Government will provide all necessary information, data and documents to the Contractor for work required under this contract.

The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract, and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

7.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in SOW 6.0.

8.0 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

8.1 The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

8.2 The COR will have 10 business days to review deliverables and make comments. The Contractor shall have 10 business days to make corrections and redeliver.

8.3 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

9.0 DELIVERABLES

The Contractor shall consider items in **BOLD** as having mandatory due dates.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	4.6	**Post Award Conference**	15 Days after award	N/A
3	4.7	**Final Contractor Project Plan**	30 Days after award	COR, Contracting Officer
4	4.8	**Original Business Continuity Plan**	30 Days after award	COR, Contracting Officer
5	4.8	**Updated Business Continuity Plan**	Annually	COR, Contracting Officer
6	4.9	**Progress Reports**	Monthly	COR, Contracting Officer
7	4.11	**Final Transition In Plan**	5 Business Days after Post Award Conference	COR, Contracting Officer
8	4.11	**Transition Out Plan**	Upon COR Request	COR, Contracting Officer

Task Order Clauses

Safeguarding of Sensitive Information (MAR 2015)

(a) Applicability. This clause applies to the Contractor and its contractors, its subcontractors, and their 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;
(xiii) 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.

Information Technology Security and Privacy Training [March 2015]

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

(b) Security Training Requirements.

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

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

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