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

1. REQUISITION NUMBER	PAGE	OF
RSUS-20-00009	1	45

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
70RSAT19D00000002		70RSAT20FR0000042	70RSAT20R00000024	03/31/2020

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
Contracting Officer/S. Buford Jr.
245 Murray Lane, SW
Washington DC 20528-0115

10. THIS ACQUISITION IS: [X] 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
[X] 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
Contracting Officer/(b)(6)
245 Murray Lane, SW
Washington DC 20528-0115

17a. CONTRACTOR/ OFFEROR — CODE: 0661830390000 — FACILITY CODE:

MANTECH SRS TECHNOLOGIES INC
ATTN (b)(6)
2251 CORPORATE PARK DRIVE
HERNDON VA 20171

TELEPHONE NO. (b)(6)

[ ] 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: 066183039+0000 The purpose of this Task Order is to provide funding to establish a new task under U.S. Department of Homeland Security (DHS) Indefinite Delivery, Indefinite Quantity ("IDIQ") Contract No. 70RSAT19D00000002. This Task Order is to procure Systems Engineering and Technical Assistance (SETA) III support services for the Department of Homeland Security (DHS), Science and Technology Directorate (S&T), *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: (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.
[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [X] ARE NOT ATTACHED.

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

[ ] 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 Enterprise Services (OES), Program Support Office (PSO). All work shall be conducted in accordance with the attached terms and conditions and Statement of Work (SOW). All applicable terms and conditions of DHS IDIQ Contract PIID 70RSAT19D00000002 apply to this Task Order. Period of Performance: 06/02/2020 to 06/01/2023				
0001	Base Period: Labor IAW SOW Section 5 (06/02/2020 - 06/01/2021) This is a Time and Materials (T&M) CLIN See Attachment 3: Pricing Table Product/Service Code: R408 Product/Service Description: SUPPORT-PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT Accounting Info: NONE000-000-J9-66-01-96-001-31-00-0000-00-00-00-00-GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J8-66-01-01-005-31-00-0000-00-00-00-00-GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: 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)
	NONE000-000-U9-40-96-05-000-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
	Accounting Info: NONE000-000-A0-50-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
	Accounting Info: NONE000-000-L0-37-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
0002	Base Period: Travel IAW SOW Section 9 (06/02/2020 - 06/01/2021) Not-to-Exceed (NTE) (b)(4) See Attachment 3: Pricing Table				(b)(4)
	Accounting Info: NONE000-000-L0-37-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
0003	Base Period: Surge Support Labor IAW SOW Section 5 (06/02/2020 - 06/01/2021) This is a Time and Materials (T&M) CLIN See Attachment 3: Pricing Table Amount: (b)(4) (Option Line Item) Product/Service Code: R408 Product/Service Description: SUPPORT-PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT				(b)(4)
	Accounting Info: Funded: (b)(4)				
1001	Option Period 1: Labor IAW SOW Section 5 (06/02/2021 - 06/01/2022) This is a Time and Materials (T&M) CLIN See Attachment 3: Pricing Table Amount: (b)(4) (Option Line Item) Product/Service Code: R408 Product/Service Description: SUPPORT-PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT				(b)(4)
	Accounting Info: NONE000-000-J8-66-01-01-005-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: NONE000-000-J9-66-01-96-001-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-U9-40-96-05-000-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-A0-50-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-L0-37-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-67-10-96-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-U0-40-96-05-000-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
1002	Option Period 1: Travel IAW SOW Section 9 (06/02/2021 - 06/01/2022) Not-to-Exceed (NTE) (b)(4) See Attachment 3: Pricing Table Amount: (b)(4) (Option Line Item) Accounting Info: NONE000-000-J8-66-01-01-005-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J9-66-01-96-001-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-U9-40-96-05-000-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-A0-50-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Continued ...				(b)(4)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: NONE000-000-L0-37-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-67-10-96-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-U0-40-96-05-000-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
1003	Option Period 1: Surge Support Labor IAW SOW Section 5 (06/02/2021 - 06/01/2022) This is a Time and Materials (T&M) CLIN See Attachment 3: Pricing Table Amount: (b)(4) (Option Line Item) Product/Service Code: R408 Product/Service Description: SUPPORT- PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT Accounting Info: NONE000-000-J8-66-01-01-005-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J9-66-01-96-001-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-U9-40-96-05-000-31-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-A0-50-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-L0-37-96-12-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-67-10-96-002-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: Continued ...				(b)(4)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	NONE000-000-U0-40-96-05-000-38-00-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4)				
2001	Option Period 2: Labor IAW SOW Section 5 (06/02/2022 - 06/01/2023) This is a Time and Materials (T&M) CLIN See Attachment 3: Pricing Table Amount: (b)(4) (Option Line Item) Product/Service Code: R408 Product/Service Description: SUPPORT- PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT Accounting Info: Funded: (b)(4)				(b)(4)
2002	Option Period 2: Travel IAW SOW Section 9 (06/02/2022 - 06/01/2023) Not-to-Exceed (NTE) $3,250.00 See Attachment 3: Pricing Table Amount: $(b)(4) (Option Line Item) Accounting Info: Funded: (b)(4)				(b)(4)
2003	Option Period 2: Surge Support Labor IAW SOW Section 5 (06/02/2022 - 06/01/2023) This is a Time and Materials (T&M) CLIN See Attachment 3: Pricing Table Amount: (b)(4) (Option Line Item) Product/Service Code: R408 Product/Service Description: SUPPORT- PROFESSIONAL: PROGRAM MANAGEMENT/SUPPORT Accounting Info: Funded: (b)(4) The total amount of award: (b)(4) The obligation for this award is shown in box 26.				(b)(4)

SETA III TASK ORDER

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

1. REQUIREMENT TITLE:

Office of Enterprise Services, Program Support Office (PSO) Systems Engineering and Technical Assistance (SETA) III Support Services

2. PROCUREMENT INSTRUMENT IDENTIFIER:

70RSAT20R00000042

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: 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: Tuesday, June 02, 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 (in Months)
Base Period	12 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 6/02/2020 through 6/01/2023.

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:

SETA III TASK ORDER

1120 Vermont Avenue, NW, Washington DC

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 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 thirty (30) day; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least sixty (60) days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 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) - Task Order Manager

TBD - Subject Matter Expert (SME) II

(b)(6) - Analyst

(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.

SETA III 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.

13. TIME AND MATERIALS CEILING

This is a Time and Materials (T&M) Task Order and the amount of funds obligated under the task order is a ceiling that the Contractor exceeds at its own risk.

SETA III TASK ORDER

ATTACHMENTS

Number	Title	# of Pages
1.	Statement of Work	25
2.	Pricing Table	3
3.	Non-Disclosure Agreement (NDA)	2

STATEMENT OF WORK

1. BACKGROUND

The U.S. Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The DHS Directorate of Science and Technology (S&T) is tasked with researching and organizing the scientific, engineering, and technological resources of the United States and leveraging these existing resources into technological tools to help protect the homeland. The mission of DHS S&T is to enable, "effective, efficient, and secure operations across all homeland security missions by applying scientific, engineering, analytic, and innovative approaches to deliver timely solutions and support departmental acquisitions."

In support of this mission, DHS S&T provides science and technology products and research, from development through transition, to Department components and first responders. These may include knowledge products, such as reports or briefing packages that document conclusions from a study or assessment conducted by an S&T project and delivered to a customer, or technology solutions such as designs or pilots to help demonstrate a candidate solution.

The Program Support Office (PSO) was established in the Office of Enterprise Services as a central hub within DHS S&T for all matters related to management of programs and projects. The PSO provides direct support to Program and Project Managers (PMs) and facilitates the development of common repeatable standards, guidance, and program/project management processes for the Directorate. The PSO supports the S&T mission through basic PM support services, guidance documentation and templates, skill development, information sharing and best practices. The PSO is also responsible for promoting collaboration, communication, consistency, alignment, transparency, and continuous process improvement to maximize the value S&T delivers to its customers. The PSO promotes a culture of program/project management that will reduce costs, risks, better estimate program/project costs, and improve program/project quality. Support is provided to the Directorate in the following core service areas:

- **Operations Support:** The PSO serves as an information hub for PM documentation, standard PM processes and procedures, and templates. The PSO maintains a central repository for processes, tools, methodologies, and techniques to ensure PMs have what is needed to successfully manage S&T programs/projects. Additional support to the Directorate include the facilitation of programmatic reviews, reporting, performance measurement, change management, and process improvement.

- **Consulting Services:** The PSO partners with PMs to address program/project management related activities, such as facilitate project team meetings (i.e., kickoff meeting, risk reviews, schedule reviews, etc.), and build materials needed for their programs and projects. Additional support to the Directorate include coaching, mentoring, and matrixed support to program/project teams.

- **Learning and Skill Development:** The PSO provides supplemental skill development opportunities for PMs to help bridge the gap between traditional PM practices and performing program/project management in a research and development (R&D) environment. These services include facilitation of workshops and training series. The goal of the PSO is to establish a Program/Project Management Community of Practice.

2. SCOPE

The Program Support Office seeks expert consultation and support on program and project management services, governance and administrative services, documentation, methodology, and professional development services that will support and enhance the S&T mission. Systems Engineering and Technical Assistance (SETA) services for the PSO will include support to programmatic and business operations

that is flexible, innovative, transformative, and responsive to the dynamic and evolving needs of the S&T Directorate. Support services include program analysis, tracking, and reporting; program and communication coordination; consultation services in the areas of effective project execution, monitoring and control; studies and analysis related to portfolio/program/project optimization, business process engineering and performance data modeling; and program/project management knowledge sharing and skill development services.

3. PLACE OF PERFORMANCE

The primary place of performance will be the Department of Homeland Security, Science and Technology (DHS/S&T) Directorate headquarters located at:

1120 Vermont Avenue NW
Washington, DC 20005 (VTA)

Work shall be performed at the Government site. 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 Contracting Officer's Representative (COR) and S&T's Office of Security, should any sensitive or classified information be involved.

4. PERIOD OF PERFORMANCE

The Government contemplates an overall period of performance of 36 months consisting of one (1) base period and two (2) 12-month options. The anticipated option periods are structured as follows:

Base Period	06/02/2020 – 06/01/2021
Option Period I	06/02/2021 – 06/01/2022
Option Period II	06/02/2022 – 06/01/2023

5. TASKS

The Contractor shall provide support for each of the tasks described below for every year of the contract. All positions are expected to be full-time (at least 40 hours per week), unless otherwise specified by the COR.

All contractor support staff shall have a working knowledge and understanding of Software Applications such as: MS Office (Excel, Word, PowerPoint, Outlook), Adobe Acrobat and others as needed to perform the tasks outlined below.

All contractor support staff shall have a Secret Clearance. The Contractor shall begin processing individuals for DHS Fitness for these positions, as soon as possible.

5.1 Post Award Conference & Planning

Upon contract award, the Contractor shall hold a post award conference with key stakeholders to review the terms of the task order. The Contractor shall be prepared to present a draft 60/90/120- day project plan for all tasks outlined in this section.

5.2 Monthly Status Report

The Contractor shall provide a monthly status report no later than the 10th day of the month following the reporting period. This monthly status report shall describe technical progress by each sub-task listed in this

SOW. It shall include: accomplishments for the month; status of personnel and timesheets; problems encountered; solutions recommended; anticipated travel; and actions for the upcoming month.

The financial status section shall consist of a funds expenditure graphic, the total current labor hours and associated total current costs by category and individual for the month and the cumulative totals (hours and cost) to date for the project; travel costs broken down by destination, date, duration, purpose, and costs for both monthly and cumulative to date. The monthly and cumulative financial data shall be reconcilable to labor hours, travel, burdens, and fee invoiced monthly and cumulatively to date. The Contractor shall be prepared to present the report at a monthly meet upon the request of DHS.

5.3 Program Support Office (PSO) Management Support

The Contractor shall support and advise the PSO Division Director in developing and executing the strategic and tactical vision for the PSO, which includes the following:

- Providing expert advice in the development of the PSO brand and providing value across the S&T organizational matrix through the core tenets of governance, guidance, tools, and training;
- Recommending and employing agile, innovative and cutting-edge techniques and methodologies, such as modular approaches, wardley mapping, and design thinking;
- Assisting in the distribution and communication of results and, assist in developing corrective action or continuous improvement plans for ongoing change initiatives;
- Interfacing with key stakeholders; establishing and maintaining communications, scheduling meetings, and managing correspondence;
- Updating and maintaining the PSO intranet site (referred to as S&T Connect Site), which includes the document repository (referred to as the process asset library) containing PM tools and templates, and the PM resource center where PM can access useful information related to program/project management.
- Assisting and participating in the development and maintenance of strategic and process documentation (e.g. Project Manager Guide, Portfolio/Program Review Plan(s), associated directives, policies, procedures, and instructions) and their implementation. This includes participating in the creation of training materials and associated communication strategies and products to ensure that the S&T staff understands and has the templates/tools to execute business processes and procedures, in accordance with program and project management best practices, relevant internal and external directives, and the Program Management Improvement Accountability Act (PMIAA).

5.4 Operations & Governance Support

The Contractor shall provide support to address the full scope of management activities for programs/projects on behalf of the PSO. This support shall align with the DHS/S&T Operational Model Blueprint and associated business processes. The Contractor shall provide one-on-one support to the PMs in the development of program/project documentation; facilitation of key project team working sessions such as risk reviews, and kickoff meetings.
The Contractor shall support the establishment and execution of the Program/Project Review Board,

Change Control Board and other Governance boards. This includes the following: planning, preparation and distribution of advance meeting materials, minute taking, facilitating the meetings (including logistics), planning, coordinating, and communicating the agenda, tracking action items, posting of information on the PSO Portal, and monitoring and disseminating information.

Additional responsibilities shall include the following:

- Assisting and providing lead support in the development, coordination, and execution of the in-depth independent reviews of S&T program and projects (e.g., rubric development, methodology development, management of information required to evaluate review quality).

- Providing support for logistics planning and execution of independent portfolio analysis and reviews; data curation and quality control; metric definition and tracking; and reporting for the S&T portfolio. Reviews may include participation by senior members of the S&T staff, senior leaders from DHS components and other equivalent functional offices, and senior stakeholders across the Homeland Security Enterprise (HSE). Results will be used to recommend data-driven decisions to the Under Secretary of S&T and other senior leadership within S&T and across DHS.

- Providing support and assistance in the development and execution of data-driven strategies and techniques that inform the effectiveness, relevance, usage and quality of PSO products and services. The Contractor shall provide recommendations to the PSO Division Director and be able to model innovative, effective, and proven data-driven techniques for collecting and analyzing business data to help inform decision-making, process and product improvements and customer satisfaction. PSO customers include S&T portfolio managers, program managers, project managers, and senior leadership.

5.5 Administrative & Branding Support

The Contractor shall provide administrative and branding support to the PSO. The Contractor shall provide graphics design support for presentations, communications, and training materials. Administrative tasks shall include, but not limited to the following: development and distribution of internal memos/correspondence, briefing, and spreadsheets, electronic filing, and records management; arrange meetings and conference calls to include scheduling with other attendees using DHS approved applications and tools; scheduling conference rooms; maintaining metrics for PSO efforts; and coordination of daily operations of the PSO.

Additional responsibilities shall include the following:

- Maintaining the PSO Outlook calendar activities by scheduling appointments, meetings, conferences, and teleconferences in compliance with PSO Division Director preferences and guidance. The Contractor shall schedule meetings that align with availability of participants and conference rooms. The Contractor shall have the ability to use all forms of virtual communication available such as teleconferencing, virtual meetings, desktop sharing, video teleconferencing (VTC), etc.

- Drafting, coordinating, finalizing and distributing meeting agendas and assembling all related background material for participants. The Contractor shall attend designated meetings, capture relevant information and action items, provide meeting summaries to participants within 24 hours, upon review and approval of the PSO Division Director

- Developing and reviewing written memos, letters, and briefings for internal and external audiences for grammatical accuracy. The Contractor shall ensure that information is appropriate and in compliance with S&T and the PSO Division Director preferences and guidance. The Contractor shall coordinate the distribution and response of official S&T Executive Secretariat (ExecSec) taskers. Quality control duties include editing correspondence for grammar, formatting, and content, ensuring that responses are complete, concise and clearly stated.

- Creating travel authorizations and generate travel vouchers for PSO staff using Concur Government (ConcurGov). Contractor shall maintain awareness of applicable travel policies, procedures, and documentation requirements and serve as an information resource for the traveler.

- Assisting the PSO Division Director by handling incoming calls; answering routine inquiries, tracking, forwarding, and/or taking messages as appropriate and ensuring that adequate coverage is maintained during official business hours.

- Serving as the primary point of contact for the PSO Outlook inbox. The Contractor will monitor, distribute and coordinate responses to inquiries received. The Contractor shall respond within 1 business day to customers in a courteous and professional manner.

- Tracking and monitoring day-to-day official communications including task traffic, deadlines and questions.

- Responding to information requests, including taskers and other reporting requirements on or before the determined due date, unless otherwise noted by the PSO Division Director.

- Independently research, resolve, or recommend solutions to routine issues in performing a variety of duties related to special projects involving administrative issues.

- Establishing and maintaining effective working relationships with internal and external personnel and maintaining a customer-centered focus, at all times.

- Absorbing, organizing, and communicating large quantities of information in a fast-paced environment in a clear, concise and accurate manner.

- Staying informed of the mission, organizational structure, key personnel, current activities, status of current projects, and any issues affecting the PSO, S&T and DHS.

- Communicating with staff and customers in a manner that is clear, concise, and professional.

- Managing a variety of functions simultaneously and with flexibility to work under competing demands and deadlines.

- Be able to operate independently and work collaboratively in a team environment.

5.6 PM Learning and Skill Development Support

The Contractor shall support the PSO in the development of innovative, transformative, and creative professional development opportunities for S&T Portfolio, Program and Project Managers. The Contractor shall develop education materials and execute skill development activities, to include: instructor-led training (in-person and virtual), self-guided training for self-certification, and informational documents.

The Contractor shall create engaging learning and skill development workshops and educational forums that considers adult learning theory and accounts for various learning styles. Skill development activities shall maximize participants' attention and knowledge retention by making the appropriate use of all educational tools available to include: periodic knowledge checks, positive and negative examples, group exercises, embedded videos, animations, and facilitating dialogue among participants.

The Contractor shall provide technical and administrative support in applying standard training concepts, adult learning theory, and principles and techniques for the S&T PM learning and skill development program.

The Contractor shall perform administrative tasks to facilitate the training program such as: serving as the primary point of contact for PM training inquiries, filing and maintaining documents electronically in Government systems, as appropriate.
The Contractor shall provide support to training events by drafting and distributing training announcements; managing registration when applicable; setting up webinar and/or meeting spaces; scheduling and communicating expectations to training facilitators; and developing and processing post-training evaluations.

The Contractor shall analyze and review course materials to determine the effectiveness of learning sessions with regard to content and trainer; take correction action as necessary to improve training effectiveness.

The Contractor shall communicate and collaborate with all necessary stakeholders to develop and maintain a timely and accurate master training task listing, guest speaker contact list, and other materials in accordance with guidance from the PSO Division Director.

5.7 Records and Knowledge Management

Records management is the organizational function devoted to the management of information in an organization throughout its life cycle, from the time of creation or inscription to its eventual disposition. The ISO 15489-1: 2001 standard and the Federal National Archives and Records Administration (NARA) regulation. ("ISO 15489-1:2001") defines records management as "[the] field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records".

The Contractor shall develop a PSO records management plan in accordance with all Federal Regulations governing records management and that aligns with the overall S&T Records Management Plan.

The Contractor shall serve as the Records Custodian and work in coordination with the S&T Records Manager and Records Liaison to ensure that the records management plan is in compliance with all Federal Regulations regarding records management.

The Contractor shall support the PSO Division Director by using concepts, processes, tools, and methodologies of knowledge management.

The Contractor shall assist with the development, design, implementation, and maintenance of a website/portal for knowledge dissemination. This includes creating documents and implementing knowledge management governance policies and procedures.

5.8 Staffing Plan

The Contractor shall provide a written staffing plan in accordance with the criteria specified in the task order. The staffing plan shall contain the following:

- Descriptions of all proposed labor categories; mapping of all employees to their assigned labor categories;
- Explanation of the process undertaken to ensure proposed employees staffed in each labor category meet the specific qualifications and have the requisite skills for the position; and
- Explanation of the due diligence performed to verify that employees meet the specified qualifications and requisite skills for the assigned labor category. The Contractor shall correctly and consistently perform proper due diligence to verify all newly hired or replacement employees meet the specified qualifications for their assigned labor categories.

The Contractor shall seek written approval from the Contracting Officer (CO) and the Contracting Officer's Representative (COR) prior to making any staffing changes (e.g. new hires, replacements, etc.).

6. SKILL and RELEVANT EXPERIENCE REQUIREMENT

The Contractor shall provide personnel for performing the activities identified in the Tasks Section under this contract who are fully qualified, trained (to include appropriate certifications), experienced, competent to perform their assigned work, and physically able to perform the work required. No trainee and/or apprentice shall be assigned. The Contractor shall make its best efforts to retain personnel who have gained experience on this contract, and to minimize turnover. All personnel assigned to perform activities under this contract must be United States citizens.

The Contractor shall provide qualified individuals* with the necessary skill sets to support project and program managers. The individuals should have full understanding of project management theory and practices. Individuals should possess leadership and expertise in business process improvement, change management, risk management, quality management, building partnerships between support service areas and programmatic/operational areas, and creating project management competency in the workforce.

The Contractor shall provide qualified individuals with the necessary skill sets to support schedule development and maintenance. Individuals should possess skilled and efficient schedule building methods and has demonstrated experience with collecting project status information and working with the project team and other stakeholders to track schedule and cost, identifying variances and proposing solutions to minimize deviations from the project plan, and identifying areas of risk and proposing solutions to mitigate or avoid risk. Individuals should also possess skill and have demonstrated experience preparing operations or procedural manuals, writing technical documentation, conducting research, and/or preparing technical reports. Knowledge and proficiency in the use of Microsoft Office and SharePoint is required.

The Contractor shall propose labor categories it believes are necessary for successful performance of the Government's requirement consistent with the terms and conditions of its SETA III IDIQ Contract.

**Staff fulfilling this experience level are required to have a Project Management Professional Certification and/or Certified ScrumMaster Certification. See staffing table in Staff Qualifications section (6.3) for list of qualified personnel.*

6.1 Key Personnel

Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer (CO) and the Contracting Officer's Representative (COR) no less than 15 business days in advance. The Contractor shall 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 CO.

The Contractor shall not replace Key Contractor personnel without approval from the CO. The Government may designate additional Contractor personnel as Key at the time of award or through a contract modification.

The key positions for this requirement are:

6.1.1 Senior Analyst

The Contractor shall provide a Senior Analyst who shall be responsible for all contractor work performed under this SOW. The Senior Analyst shall oversee and verify the hours worked by all personnel, considering flexible schedules, breaks, leave, telework, and off-site meetings. This support personnel shall be a single point of contact for the CO and the COR. The Contractor shall ensure the designated personnel has a minimum of ten (10) years of experience. The Contractor shall ensure that mandatory and recurring training requirements for contractors supporting this SOW are completed.

The name of the contract management personnel, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Senior Analyst, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Senior Analyst, only one alternate shall have full authority to act for the contractor on all matters relating to work performed under this contract. Additionally, the Contractor shall not replace the Senior Analyst without prior approval from the CO. The Senior Analyst shall be available to the COR via telephone between the hours of 7am and 5pm Eastern Standard Time (EST), Monday through Friday, and shall respond to a request for discussion or resolution of problems within eight hours of notification.

6.1.2 Senior Portfolio/Program/Project Analyst

The Contractor shall provide a Senior Portfolio/Program/Project Analyst who shall oversee and manage contractor personnel tasked with operations and governance support work performed under this SOW; which includes the establishment and execution of the Program/Project Review Board, Change Control Board and other Governance boards.

The name of the personnel, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Senior Portfolio/Program/Project Analyst, shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Senior Portfolio/Program/Project Analyst without prior approval from the CO. Senior Portfolio/Program/Project Analyst shall be available to the COR via telephone between the hours of 7am and 5pm Eastern Standard Time (EST), Monday through Friday, and shall respond to a request for discussion or resolution of problems within eight hours of notification.

6.1.3 Senior Administrative Specialist

The Contractor shall provide a Senior Administrative Specialist who shall oversee and manage the administrative tasks outlined in this SOW.

The name of the personnel, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Senior Administrative Specialist, shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Senior Administrative Specialist, without prior approval from the CO. The Senior Administrative Specialist shall be available to the COR via telephone between the hours of 7am and 5pm Eastern Standard Time (EST), Monday through Friday, and shall respond to a request for discussion or resolution of problems within eight hours of notification.

6.2 Qualified Staff

The Contractor shall provide qualified individuals with the education and experience required to support

the Government based on tasks described in the Tasks section (5.0) of this SOW.

The Contractor shall provide the COR with a resume for each individual proposed for review and approval based on the qualifications described in Staff Qualifications section (6.3) of this SOW.

The Contractor shall seek written approval from the COR for a waiver to assign any individual who does not meet the minimum qualifications.

The Contractor shall provide personnel that are able to fluently read, write, speak, and understand English as their primary or alternate language.

6.3 Staff Qualifications

The Contractor shall perform the work described in Place of Performance section (3.0) of this SOW with personnel fitting the following labor categories. Each labor category is described along with its education and experience requirements. Each personnel must have specialized experience and knowledge commensurate with the following descriptions and qualifications:

POSITION	DESCRIPTION	MINIMUM REQUIREMENTS
Senior Analyst*	Oversees the development of contractor staff, and alignment of the staff to the Government's requirement at the task order level. Provides and ensures quality and timely services and delivery of contractual items under the contract terms and conditions. Serves as point of contact with the Contracting Officer's Representative (COR) and Contracting Officer (CO). Performs day-to-day management of contract execution, possibly involving multiple groups of personnel at multiple locations. Establishes and maintains technical and financial reports demonstrating task order progress and delegates responsibilities to subordinates and oversees successful contract/task order completion. Maintains effective client interface with the COR. Motivates contractor staff and ensures contractor staff are adequately trained and fully understands the work environment. Contributes to the evaluation, analysis, and development of recommended solutions. Resolves complex problems, which require an in-depth knowledge of subject matter related to the designated field or discipline. Applies principles and methods of the subject matter to specialized	BA/BS + 10 years of relevant or Master's + 5 years of relevant experience.

	solutions. Areas of expertise may include business process reengineering, performance management, statistical process control, individual and organizational assessment and evaluation, process modeling and simulation, strategic and business planning, change management, organizational development, quality assurance, regulatory compliance, and situational awareness and decision support.	
Analyst	See Description for Senior Analyst. The analyst responsible for the learning and skill development task outlined in this SOW oversees the development of the PM skill development and training. Experienced with providing program management, training, skills assessments, developing curriculum, and similar support. Experienced with developing large enterprise-wide online training courses and programs. The ideal applicant would have knowledge of the 508 compliance requirements and other federal regulations regarding online content and accessibility. Ability to understand complex technical issues and communicate those issues to a non-technical audience. Ability to communicate effectively, both orally and in writing.	BA/BS + 5 Years of relevant experience or Master's + 3 years of relevant experience.
Senior Portfolio/ Program/ Project Analyst*	Assist program managers in their execution of programs. Will be required to assist with defining requirements; provides input to project scope, schedule and budget based on an understanding of the program lifecycle. Assist in maintaining changes to project baselines; monitors deliverables; assess documents, plans and applications; conducts quality reviews of projects and tasks. Prepares presentations and other materials to support project functions. Leads activities to identify project risks and assist in the development of mitigation plans. Drafts correspondence, reports, white papers, minutes, spreadsheets, communications products, briefs, and other documentation. Maintains and tracks action items and participates in meetings. Assist in drafting various documents supporting a procurement. Will be relied upon to provide technical and procurement guidance to junior contractor staff on the team.	BA/BS + 10 years of relevant or Master's + 5 years of relevant experience.
Senior Documentation Specialist	Supports the development and maintenance of effective information management plans, processes, repositories and systems. Organizes, maintains, tracks, and files documentation in electronic formats. Maintains document version control and configuration management. Evaluates documentation, specifications, reports, and presentations. Outlines and develops technical documentation detailing the design, development, testing, installation, and maintenance of systems and processes. Develops databases that extracts and interprets data from the repositories.	BA/BS + 10 years of relevant experience or Master's + 5 years of relevant experience.
Senior Technical	Gathers, analyzes, and composes complex technical information. Conducts research and ensures the use of proper technical terminology. Translates technical information into clear, readable documents to be used by technical and non-technical personnel. Organizes material and writes	BA/BS + 10 years of relevant experience or Master's + 5 years of relevant

Writer / Editor / Communication s Specialist	descriptive copy according to establish standards regarding order, clarity, conciseness, style, and terminology. Selects photographs, drawings, sketches, diagrams, and charts to illustrate material. Develops communications materials for publications, internet, strategic initiatives, user manuals, training materials, installation guides, white papers, reports, etc. Develops, writes, and edits functional descriptions, system specifications, special reports, or any other customer deliverables and documents. Provides technical writing support and deciphers directions provided on scripted storyboards, specifications, etc. Reviews documents for technical accuracy in accordance with applicable regulations. Supports content creating and management on networks and web platforms (i.e. Social Media).	experience.
Senior Administrative Specialist	Performs administrative duties as required such as writing memos, filing, typing, and copying documents. Develops spreadsheets, maintains program, project, and task files, technical support information for program, project managers. Organizes and maintains calendars for one or more managers, schedules meetings, takes meeting notes and distributes to attendees. Prepares correspondence, briefs, and reports and assists with planning, initiation, and tracking of task assignments and associated data. Assists with preparing and processing travel and maintaining travel requests and records. Distributes and monitor taskings, data calls and coordinating troubleshoot requests.	BA/BS + 7 years of relevant experience or Masters + 5 years of relevant experience.

**Staff fulfilling these positions are required to have a Project Management Professional Certification and/or Certified ScrumMaster Certification.*

6.4 Continuity of Support

The Contractor shall ensure that the required level of support 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., the Contractor shall provide e-mail notification to the COR prior to absence.

6.5 Employee Identification

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the contractor name, the employee's photo, name, 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.

6.6 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 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 COR shall ensure contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

6.7 Removing Employees for Misconduct Reasons

The Government may, at its sole discretion (via the CO), 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 CO

will provide the Contractor with a written explanation to support any request to remove an employee.

6.8 Training Requirements

The Contractor shall work with the Federal Training manager to ensure all personnel enroll and complete all DHS/S&T mandatory training.
The Contractor shall provide a list of all employees and their training status, completion dates, and upcoming training dates.

Additional training may be required at any time during this contract as notified by the COR or CO.

7. TRAVEL

The Contractor may be required to travel in support of this requirement. All travel required by the Government outside the Greater Washington DC Metropolitan Area (see OMB Bulletin No. 05-02 and code 47900) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations (FTR), with no profit or fee applied. The Contractor shall be responsible for obtaining written Contracting Officer's Representative (COR) approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

The Government will not reimburse the Contractor for local travel (within the Greater Washington, DC Metropolitan Area). All travel-related expenses (including, but not limited to, airfare, lodging, meals, rental cars, and incidental expenses) incurred by the Contractor as a result of performing the services in this SOW shall be reimbursed in compliance with the FTR and resultant awarded Task Order. All travel requests must receive prior written approval from the Task Order COR. Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoice(s).

8. SURGE RESPONSE

The Contractor may be required to provide additional support described in the base year and each option year, depending on the level of effort required each year. These tasks shall be reimbursed on a Labor Hour basis subject to the labor categories and hourly rates contained in the pricing schedule and the terms of the modification authorizing the work.

9. INSPECTION AND ACCEPTANCE CRITERIA

Inspection and acceptance of products and services shall be performed by a duly authorized Government representative identified in the Task Order in accordance with the Inspection and Acceptance clauses in the SETA III contract and as further defined in the Task Order.

All deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements by the COR or as detailed in individual Task Order. Inspection may include validation of information or software through the use of automated tools for the deliverables, as specified in the Task Order.

The Government requires a period not to exceed thirty (30) calendar days after receipt of final deliverable items for inspection and acceptance or rejection unless otherwise specified in the awarded Task Order. The Contractor shall provide work products and deliverables within the acceptance criteria identified below:

Quality measures, as set forth below, will be applied to each Work Product and Deliverable.

- **Adherence to Requirements** - Work products and deliverables shall adhere to the requirements in the statement of work and all DHS S&T policies and procedures.
- **Accuracy** – Work products and deliverables shall be free from errors and mistakes; and be

developed in accordance with applicable laws, regulations, policies, and procedures.
- **Completeness** – Work products and deliverables shall have all parts or elements.
- **Clarity** – Work products and deliverables shall be easy to understand.
- **Timeliness** – Work products and deliverables shall be available at the time required and generated on or before specified and mutually agreed to due dates. If a new due date has been agreed upon, then the work product and deliverable shall be available on or before that new due date.
- **Format** – Work products and deliverables shall be submitted in hard and/or soft copy, as appropriate. Both hard and soft copy formats shall follow specified guidance, directives, and/or policies.

10. DELIVERABLES

The Contractor shall provide all deliverables electronically, unless otherwise specified, directly to the COR and the PM (PSO Division Director). The Contractor shall deliver all technical reports and other data developed under this SOW, along with the appropriate documentation to the COR and PM (PSO Division Director) as they are completed, unless otherwise specified.

All deliverables become the property of the Government and may not be disseminated without prior written approval from DHS.

TASK	DELIVERABLE / EVENT	DUE BY	DELIVER/REPORT TO:
5.1	Post Award Conference	Ten (10) business days after award	N/A
5.1	Draft Contractor Project Plan (60/90/120-day plan)	Ten (10) business days after award	CO/COR/PM
5.1	Final Contractor Project Plan (60/90/120-day plan)	Fifteen (15) business days after post award conference.	CO/COR/PM
5.2	Monthly Status Report	Ten (10) calendar days after end of each month	COR/PM
5.3	PSO Sharepoint Site Content Refresh	Initial refresh no later than thirty (30) business days after award; At least monthly thereafter	PM

5.4	Draft Governance Support Strategy	Thirty (30) business days after post award conference	COR/PM
5.4	Final Governance Support Strategy	Twenty (20) business days after receipt of Government comments	COR/PM
5.5	Draft Communications Plan	Twenty (20) business days after post award conference	COR/PM
5.5	Final Communications Plan	Fifteen (15) business days after receipt of Government comments	COR/PM
5.6	Draft Training Plan	Twenty (20) business days after post award conference	COR/PM
5.6	Final Training Plan	Twenty (20) business days after receipt of Government comments	COR/PM
5.7	Draft Records Management File Plan	Sixty (60) business days after post award conference	COR/PM
5.7	Final Records Management File Plan	Twenty (20) business days after receipt of Government comments	COR/PM
5.8	Draft Staffing Plan	Ten (10) business days after award	COR/PM
5.8	Final Staffing Plan	Fifteen (15) business days after receipt of Government comments	COR/PM

11. WORK SCHEDULE

The Contractor shall provide on-site services Monday through Friday, from 7:00 AM to 5:00 PM (excluding federal holidays). All contractor personnel shall work for eight hours during this business day not including lunch or other breaks. These eight work hours must be spent performing work under this SOW. If offsite work is authorized it shall be completed in the same manner, for eight hours during the business day. The COR may approve deviations from the standard eight-hour day.

The holidays observed by the Federal Government are the following:

January 1	New Year's Day
Third Monday in January	Birthday of Martin Luther King, Jr.
Third Monday in February	Washington's Birthday
Last Monday in May	Memorial Day
July 4	Independence Day
First Monday in September	Labor Day

Second Monday in October	Columbus Day
November 11	Veterans Day
4th Thursday in November	Thanksgiving Day
December 25	Christmas

Contractor personnel may be permitted to telework, from home or from contractor facilities, in the event of Government office closures, commuting disruptions, continuity of operations exercises, or unusual work needs in special circumstances. Telework may be permitted on a permanent or regular basis. All telework must be approved by the COR and PSO Division Director.

12. Security Requirements

Safeguarding of Sensitive Information (MAR 2015)

(a) Applicability. This clause applies to **ManTech SRS Technologies, Inc.** 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:
(j)

(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.

(k)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 **ManTech SRS Technologies, Inc.** 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.

DHS may exercise full control over granting, denying, withholding, or terminating unescorted access to DHS facilities, DHS systems, and/or sensitive DHS information for government/contract employees. Access will be based upon the results of a DHS fitness/suitability investigation. DHS may, as appropriate, make favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the government/contract employee 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 DHS fitness/suitability authorization will follow. The granting of a favorable EOD decision or a full DHS 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 contract/task order. No employee of the government/contractor shall be allowed unescorted access to a

DHS facility, access to any sensitive DHS information, or access to DHS Systems without a favorable EOD decision or DHS fitness/suitability determination by the DHS HQ Office of Security. Government/contract employees assigned to the contract/task order not needing access to sensitive DHS information, DHS systems, or access to DHS facilities will not be subject to DHS fitness/suitability screening. Government/contract employees waiting on an EOD decision may not begin work on the task order. Limited access to DHS facilities is allowable prior to the EOD decision if the government/contract employee is escorted by an approved DHS employee. This limited access is to allow government/contract employees to attend briefings, nonrecurring meetings, and begin transition work. During one's limited access the government/contract employee will not have access to sensitive or classified DHS information.

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 government/contract employee 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 government/contract employee is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

HSAR 3052.204-71 Contractor Employee Access (SEP 2012)

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

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

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

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

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

(b) "Information Technology Resources" include, but are not limited to, computer equipment,

networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

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

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

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

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

(End of clause)

Base Period

Labor Category	Site (Gov/Cont)	ManTech Proposed Labor Category	Base Period			
			SETA III IDIQ Rate	Proposed Rate	Proposed Hours	Extended Price
CLIN 0001 Base Task(s)						
Senior Portfolio/Program/Project Analyst	Gov	Subject Matter Expert II	(b)(4)			
Senior Analyst	Gov	Task Order Manager				
Senior Administrative Specialist	Gov	Analyst				
Senior Documentation Specialist	Gov	Senior Documentation Specialist				
Senior Technical Writer/Editor/Communications Specialist	Gov	Senior Analyst				
Analyst	Gov	Subject Matter Expert II				
Analyst	Gov	Analyst				
CLIN 0001 Labor Total						
CLIN 0002 Travel						
Travel						
CLIN 0002 Total						
CLIN 0003 Surge Support Task						
Portfolio/Program/Project Analyst	Gov	Analyst				
Analyst	Gov	Analyst				
CLIN 0003 Surge Support Labor Total						
Base Period Labor Total						
Total Without Surge						
Total Base Period Price						

Option Period 1

Labor Category	Site (Gov/Cont)	ManTech Proposed Labor Category	Option Period 1			
			SETA III IDIQ Rate	Proposed Rate	Proposed Hours	Extended Price
CLIN 1001 Base Task(s)						
Senior Portfolio/Program/Project Analyst	Gov	(b)(4)	(b)(4)			
Senior Analyst	Gov					
Senior Administrative Specialist	Gov					
Senior Documentation Specialist	Gov					
Senior Technical Writer/Editor/Communications Specialist	Gov					
Analyst	Gov					
Analyst	Gov					
CLIN 1001 Labor Total						
CLIN 1002 Travel						
Travel						
CLIN 1002 Total						
CLIN 1003 Surge Support Task						
Portfolio/Program/Project Analyst	Gov					
Analyst	Gov					
CLIN 1003 Surge Support Labor Total						
Option Period 1 Labor Total						
Total Without Surge						
Total Option Period 1 Price						

Option Period 2

Labor Category	Site (Gov/Cont)	ManTech Proposed Labor Category	Option Period 2			
			SETA III IDIQ Rate	Proposed Rate	Proposed Hours	Extended Price
CLIN 2001 Base Task(s)						
Senior Portfolio/Program/Project Analyst	Gov	(b)(4)	(b)(4)			
Senior Analyst	Gov					
Senior Administrative Specialist	Gov					
Senior Documentation Specialist	Gov					
Senior Technical Writer/Editor/Communications Specialist	Gov					
Analyst	Gov					
Analyst	Gov					
CLIN 2001 Labor Total						
CLIN 2002 Travel						
Travel						
CLIN 2002 Total						
CLIN 2003 Surge Support Task						
Portfolio/Program/Project Analyst	Gov					
Analyst	Gov					
CLIN 2003 Surge Support Labor Total						
Option Period 2 Labor Total						
Total Without Surge						
Total Option Period 2 Price						

SETA III NON-DISCLOSURE AGREEMENT (NDA)
SUPPLEMENT to DHS NDA FORM 11000-6

[NAME OF GOVERNMENT PROGRAM OFFICE and CONTRACT NUMBER]

I am an employee of **<Company Name> <Company Segment> (<ACRONYM>)** assigned to work for the **<Government Agency>**, **<Agency Division>** (herein after referred to as the "PROGRAM") under **<Contract Title>**, **<Contract Number>**. In consideration of my being provided access under the PROGRAM to confidential, business-sensitive or proprietary information that may be in possession and under the confidence of the Government, I hereby agree that during the period of my employment on this PROGRAM or thereafter, I shall not disclose any such information except in compliance with this Agreement or at the direction of the Contracting Officer.

Information subject to the nondisclosure obligations of this Agreement ("Protected Information") includes information, such as plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 (Public Law 93-579), data that has not been released or otherwise made available to the public; and "Source Selection Information" and "Proprietary Information" of third party Contractors, as those terms are defined in Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. 423). Such Protected Information includes, but is not limited to information submitted to the Government on a confidential basis by other persons and covers such information whether or not in its original form (for example where the information has been included in subcontractor generated work or where it is discernible from materials incorporating or based upon such information).

I agree that I shall not release, disclose or use in any way that would permit or result in disclosure to any party outside the Government any Protected Information provided to me during or as a result of my performance on the PROGRAM without permission from the Contracting Officer. This prohibition applies to release of Protected Information to or between any affiliate of my employer or any other subcontractor, consultant, or employee of my employer or any joint venture involving my employer. In addition, Protected Information shall not be released, duplicated, used or disclosed, in whole or in part, for any purpose other than in the performance of the PROGRAM, unless so directed by the Contracting Officer. I acknowledge that the Contracting Officer is the only person who is authorized to direct me to release or disclose Protected Information.

I agree not to participate in any manner in the preparation of any proposal or bid to be submitted by any person or organization involving Source Selection Information to which I was exposed in my work on the PROGRAM.

I will not agree to access government staff email if the opportunity is presented, unless I am determined by the Contracting Officer to fill the position of an administrative assistant

with express permission to access government staff email.

I agree to use and examine Protected Information exclusively in the performance of work required to carry out my duties within the PROGRAM, and agree to take suitable steps to prevent the disclosure of such information to any parties other than those authorized to have access to such Protected Information under the PROGRAM. At the conclusion of my performance on the PROGRAM or as requested by the Contracting Officer or the Contracting Officer Representative, I agree to surrender all Protected Information in my possession or control. I will have no ownership or right to possess such Protected Information except to fulfill my specific PROGRAM work assignments.

I further agree that I will report to the **<Company Name> <company segment>**, Contracting Officer and Contracting Officer Representative any known or suspected violations of the spirit or the intent of the procedures established for the protection of sensitive information, otherwise be subject to criminal or civil penalties as outlined in 18 U.S.C § 1001 or 41 U.S.C § 2105.

I, the undersigned, having read and fully understood this Agreement, and agree to abide by the provisions of this Agreement.

TYPE and PRINT IN INK

_____

Employee Signature and Date

_____

Employee Name (Printed) and Title

_____

IDIQ Contractor Program Manager Signature and Date

_____

IDIQ Contractor Program Manager (Printed) and Title

STATEMENT OF WORK

1. BACKGROUND

The U.S. Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The DHS Directorate of Science and Technology (S&T) is tasked with researching and organizing the scientific, engineering, and technological resources of the United States and leveraging these existing resources into technological tools to help protect the homeland. The mission of DHS S&T is to enable, "effective, efficient, and secure operations across all homeland security missions by applying scientific, engineering, analytic, and innovative approaches to deliver timely solutions and support departmental acquisitions."

In support of this mission, DHS S&T provides science and technology products and research, from development through transition, to Department components and first responders. These may include knowledge products, such as reports or briefing packages that document conclusions from a study or assessment conducted by an S&T project and delivered to a customer, or technology solutions such as designs or pilots to help demonstrate a candidate solution.

The Program Support Office (PSO) was established in the Office of Enterprise Services as a central hub within DHS S&T for all matters related to management of programs and projects. The PSO provides direct support to Program and Project Managers (PMs) and facilitates the development of common repeatable standards, guidance, and program/project management processes for the Directorate. The PSO supports the S&T mission through basic PM support services, guidance documentation and templates, skill development, information sharing and best practices. The PSO is also responsible for promoting collaboration, communication, consistency, alignment, transparency, and continuous process improvement to maximize the value S&T delivers to its customers. The PSO promotes a culture of program/project management that will reduce costs, risks, better estimate program/project costs, and improve program/project quality. Support is provided to the Directorate in the following core service areas:

- **Operations Support:** The PSO serves as an information hub for PM documentation, standard PM processes and procedures, and templates. The PSO maintains a central repository for processes, tools, methodologies, and techniques to ensure PMs have what is needed to successfully manage S&T programs/projects. Additional support to the Directorate include the facilitation of programmatic reviews, reporting, performance measurement, change management, and process improvement.

- **Consulting Services:** The PSO partners with PMs to address program/project management related activities, such as facilitate project team meetings (i.e., kickoff meeting, risk reviews, schedule reviews, etc.), and build materials needed for their programs and projects. Additional support to the Directorate include coaching, mentoring, and matrixed support to program/project teams.

- **Learning and Skill Development:** The PSO provides supplemental skill development opportunities for PMs to help bridge the gap between traditional PM practices and performing program/project management in a research and development (R&D) environment. These services include facilitation of workshops and training series. The goal of the PSO is to establish a Program/Project Management Community of Practice.

2. SCOPE

The Program Support Office seeks expert consultation and support on program and project management services, governance and administrative services, documentation, methodology, and professional development services that will support and enhance the S&T mission. Systems Engineering and Technical Assistance (SETA) services for the PSO will include support to programmatic and business operations

that is flexible, innovative, transformative, and responsive to the dynamic and evolving needs of the S&T Directorate. Support services include program analysis, tracking, and reporting; program and communication coordination; consultation services in the areas of effective project execution, monitoring and control; studies and analysis related to portfolio/program/project optimization, business process engineering and performance data modeling; and program/project management knowledge sharing and skill development services.

3. PLACE OF PERFORMANCE

The primary place of performance will be the Department of Homeland Security, Science and Technology (DHS/S&T) Directorate headquarters located at:

1120 Vermont Avenue NW
Washington, DC 20005 (VTA)

Work shall be performed at the Government site. 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 Contracting Officer's Representative (COR) and S&T's Office of Security, should any sensitive or classified information be involved.

4. PERIOD OF PERFORMANCE

The Government contemplates an overall period of performance of 36 months consisting of one (1) base period and two (2) 12-month options. The anticipated option periods are structured as follows:

Base Period	06/02/2020 – 06/01/2021
Option Period I	06/02/2021 – 06/01/2022
Option Period II	06/02/2022 – 06/01/2023

5. TASKS

The Contractor shall provide support for each of the tasks described below for every year of the contract. All positions are expected to be full-time (at least 40 hours per week), unless otherwise specified by the COR.

All contractor support staff shall have a working knowledge and understanding of Software Applications such as: MS Office (Excel, Word, PowerPoint, Outlook), Adobe Acrobat and others as needed to perform the tasks outlined below.

All contractor support staff shall have a Secret Clearance. The Contractor shall begin processing individuals for DHS Fitness for these positions, as soon as possible.

5.1 Post Award Conference & Planning

Upon contract award, the Contractor shall hold a post award conference with key stakeholders to review the terms of the task order. The Contractor shall be prepared to present a draft 60/90/120- day project plan for all tasks outlined in this section.

5.2 Monthly Status Report

The Contractor shall provide a monthly status report no later than the 10th day of the month following the reporting period. This monthly status report shall describe technical progress by each sub-task listed in this

SOW. It shall include: accomplishments for the month; status of personnel and timesheets; problems encountered; solutions recommended; anticipated travel; and actions for the upcoming month.

The financial status section shall consist of a funds expenditure graphic, the total current labor hours and associated total current costs by category and individual for the month and the cumulative totals (hours and cost) to date for the project; travel costs broken down by destination, date, duration, purpose, and costs for both monthly and cumulative to date. The monthly and cumulative financial data shall be reconcilable to labor hours, travel, burdens, and fee invoiced monthly and cumulatively to date. The Contractor shall be prepared to present the report at a monthly meet upon the request of DHS.

5.3 Program Support Office (PSO) Management Support

The Contractor shall support and advise the PSO Division Director in developing and executing the strategic and tactical vision for the PSO, which includes the following:

- Providing expert advice in the development of the PSO brand and providing value across the S&T organizational matrix through the core tenets of governance, guidance, tools, and training;
- Recommending and employing agile, innovative and cutting-edge techniques and methodologies, such as modular approaches, wardley mapping, and design thinking;
- Assisting in the distribution and communication of results and, assist in developing corrective action or continuous improvement plans for ongoing change initiatives;
- Interfacing with key stakeholders; establishing and maintaining communications, scheduling meetings, and managing correspondence;
- Updating and maintaining the PSO intranet site (referred to as S&T Connect Site), which includes the document repository (referred to as the process asset library) containing PM tools and templates, and the PM resource center where PM can access useful information related to program/project management.
- Assisting and participating in the development and maintenance of strategic and process documentation (e.g. Project Manager Guide, Portfolio/Program Review Plan(s), associated directives, policies, procedures, and instructions) and their implementation. This includes participating in the creation of training materials and associated communication strategies and products to ensure that the S&T staff understands and has the templates/tools to execute business processes and procedures, in accordance with program and project management best practices, relevant internal and external directives, and the Program Management Improvement Accountability Act (PMIAA).

5.4 Operations & Governance Support

The Contractor shall provide support to address the full scope of management activities for programs/projects on behalf of the PSO. This support shall align with the DHS/S&T Operational Model Blueprint and associated business processes. The Contractor shall provide one-on-one support to the PMs in the development of program/project documentation; facilitation of key project team working sessions such as risk reviews, and kickoff meetings.
The Contractor shall support the establishment and execution of the Program/Project Review Board,

Change Control Board and other Governance boards. This includes the following: planning, preparation and distribution of advance meeting materials, minute taking, facilitating the meetings (including logistics), planning, coordinating, and communicating the agenda, tracking action items, posting of information on the PSO Portal, and monitoring and disseminating information.

Additional responsibilities shall include the following:

- Assisting and providing lead support in the development, coordination, and execution of the in-depth independent reviews of S&T program and projects (e.g., rubric development, methodology development, management of information required to evaluate review quality).

- Providing support for logistics planning and execution of independent portfolio analysis and reviews; data curation and quality control; metric definition and tracking; and reporting for the S&T portfolio. Reviews may include participation by senior members of the S&T staff, senior leaders from DHS components and other equivalent functional offices, and senior stakeholders across the Homeland Security Enterprise (HSE). Results will be used to recommend data-driven decisions to the Under Secretary of S&T and other senior leadership within S&T and across DHS.

- Providing support and assistance in the development and execution of data-driven strategies and techniques that inform the effectiveness, relevance, usage and quality of PSO products and services. The Contractor shall provide recommendations to the PSO Division Director and be able to model innovative, effective, and proven data-driven techniques for collecting and analyzing business data to help inform decision-making, process and product improvements and customer satisfaction. PSO customers include S&T portfolio managers, program managers, project managers, and senior leadership.

5.5 Administrative & Branding Support

The Contractor shall provide administrative and branding support to the PSO. The Contractor shall provide graphics design support for presentations, communications, and training materials. Administrative tasks shall include, but not limited to the following: development and distribution of internal memos/correspondence, briefing, and spreadsheets, electronic filing, and records management; arrange meetings and conference calls to include scheduling with other attendees using DHS approved applications and tools; scheduling conference rooms; maintaining metrics for PSO efforts; and coordination of daily operations of the PSO.

Additional responsibilities shall include the following:

- Maintaining the PSO Outlook calendar activities by scheduling appointments, meetings, conferences, and teleconferences in compliance with PSO Division Director preferences and guidance. The Contractor shall schedule meetings that align with availability of participants and conference rooms. The Contractor shall have the ability to use all forms of virtual communication available such as teleconferencing, virtual meetings, desktop sharing, video teleconferencing (VTC), etc.

- Drafting, coordinating, finalizing and distributing meeting agendas and assembling all related background material for participants. The Contractor shall attend designated meetings, capture relevant information and action items, provide meeting summaries to participants within 24 hours, upon review and approval of the PSO Division Director

- Developing and reviewing written memos, letters, and briefings for internal and external audiences for grammatical accuracy. The Contractor shall ensure that information is appropriate and in compliance with S&T and the PSO Division Director preferences and guidance. The Contractor shall coordinate the distribution and response of official S&T Executive Secretariat (ExecSec) taskers. Quality control duties include editing correspondence for grammar, formatting, and content, ensuring that responses are complete, concise and clearly stated.

- Creating travel authorizations and generate travel vouchers for PSO staff using Concur Government (ConcurGov). Contractor shall maintain awareness of applicable travel policies, procedures, and documentation requirements and serve as an information resource for the traveler.

- Assisting the PSO Division Director by handling incoming calls; answering routine inquiries, tracking, forwarding, and/or taking messages as appropriate and ensuring that adequate coverage is maintained during official business hours.

- Serving as the primary point of contact for the PSO Outlook inbox. The Contractor will monitor, distribute and coordinate responses to inquiries received. The Contractor shall respond within 1 business day to customers in a courteous and professional manner.

- Tracking and monitoring day-to-day official communications including task traffic, deadlines and questions.

- Responding to information requests, including taskers and other reporting requirements on or before the determined due date, unless otherwise noted by the PSO Division Director.

- Independently research, resolve, or recommend solutions to routine issues in performing a variety of duties related to special projects involving administrative issues.

- Establishing and maintaining effective working relationships with internal and external personnel and maintaining a customer-centered focus, at all times.

- Absorbing, organizing, and communicating large quantities of information in a fast-paced environment in a clear, concise and accurate manner.

- Staying informed of the mission, organizational structure, key personnel, current activities, status of current projects, and any issues affecting the PSO, S&T and DHS.

- Communicating with staff and customers in a manner that is clear, concise, and professional.

- Managing a variety of functions simultaneously and with flexibility to work under competing demands and deadlines.

- Be able to operate independently and work collaboratively in a team environment.

5.6 PM Learning and Skill Development Support

The Contractor shall support the PSO in the development of innovative, transformative, and creative professional development opportunities for S&T Portfolio, Program and Project Managers. The Contractor shall develop education materials and execute skill development activities, to include: instructor-led training (in-person and virtual), self-guided training for self-certification, and informational documents.

The Contractor shall create engaging learning and skill development workshops and educational forums that considers adult learning theory and accounts for various learning styles. Skill development activities shall maximize participants' attention and knowledge retention by making the appropriate use of all educational tools available to include: periodic knowledge checks, positive and negative examples, group exercises, embedded videos, animations, and facilitating dialogue among participants.

The Contractor shall provide technical and administrative support in applying standard training concepts, adult learning theory, and principles and techniques for the S&T PM learning and skill development program.

The Contractor shall perform administrative tasks to facilitate the training program such as: serving as the primary point of contact for PM training inquiries, filing and maintaining documents electronically in Government systems, as appropriate.
The Contractor shall provide support to training events by drafting and distributing training announcements; managing registration when applicable; setting up webinar and/or meeting spaces; scheduling and communicating expectations to training facilitators; and developing and processing post-training evaluations.

The Contractor shall analyze and review course materials to determine the effectiveness of learning sessions with regard to content and trainer; take correction action as necessary to improve training effectiveness.

The Contractor shall communicate and collaborate with all necessary stakeholders to develop and maintain a timely and accurate master training task listing, guest speaker contact list, and other materials in accordance with guidance from the PSO Division Director.

5.7 Records and Knowledge Management

Records management is the organizational function devoted to the management of information in an organization throughout its life cycle, from the time of creation or inscription to its eventual disposition. The ISO 15489-1: 2001 standard and the Federal National Archives and Records Administration (NARA) regulation. ("ISO 15489-1:2001") defines records management as "[the] field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records".

The Contractor shall develop a PSO records management plan in accordance with all Federal Regulations governing records management and that aligns with the overall S&T Records Management Plan.

The Contractor shall serve as the Records Custodian and work in coordination with the S&T Records Manager and Records Liaison to ensure that the records management plan is in compliance with all Federal Regulations regarding records management.

The Contractor shall support the PSO Division Director by using concepts, processes, tools, and methodologies of knowledge management.

The Contractor shall assist with the development, design, implementation, and maintenance of a website/portal for knowledge dissemination. This includes creating documents and implementing knowledge management governance policies and procedures.

5.8 Staffing Plan

The Contractor shall provide a written staffing plan in accordance with the criteria specified in the task order. The staffing plan shall contain the following:

- Descriptions of all proposed labor categories; mapping of all employees to their assigned labor categories;
- Explanation of the process undertaken to ensure proposed employees staffed in each labor category meet the specific qualifications and have the requisite skills for the position; and
- Explanation of the due diligence performed to verify that employees meet the specified qualifications and requisite skills for the assigned labor category. The Contractor shall correctly and consistently perform proper due diligence to verify all newly hired or replacement employees meet the specified qualifications for their assigned labor categories.

The Contractor shall seek written approval from the Contracting Officer (CO) and the Contracting Officer's Representative (COR) prior to making any staffing changes (e.g. new hires, replacements, etc.).

6. SKILL and RELEVANT EXPERIENCE REQUIREMENT

The Contractor shall provide personnel for performing the activities identified in the Tasks Section under this contract who are fully qualified, trained (to include appropriate certifications), experienced, competent to perform their assigned work, and physically able to perform the work required. No trainee and/or apprentice shall be assigned. The Contractor shall make its best efforts to retain personnel who have gained experience on this contract, and to minimize turnover. All personnel assigned to perform activities under this contract must be United States citizens.

The Contractor shall provide qualified individuals* with the necessary skill sets to support project and program managers. The individuals should have full understanding of project management theory and practices. Individuals should possess leadership and expertise in business process improvement, change management, risk management, quality management, building partnerships between support service areas and programmatic/operational areas, and creating project management competency in the workforce.

The Contractor shall provide qualified individuals with the necessary skill sets to support schedule development and maintenance. Individuals should possess skilled and efficient schedule building methods and has demonstrated experience with collecting project status information and working with the project team and other stakeholders to track schedule and cost, identifying variances and proposing solutions to minimize deviations from the project plan, and identifying areas of risk and proposing solutions to mitigate or avoid risk. Individuals should also possess skill and have demonstrated experience preparing operations or procedural manuals, writing technical documentation, conducting research, and/or preparing technical reports. Knowledge and proficiency in the use of Microsoft Office and SharePoint is required.

The Contractor shall propose labor categories it believes are necessary for successful performance of the Government's requirement consistent with the terms and conditions of its SETA III IDIQ Contract.

**Staff fulfilling this experience level are required to have a Project Management Professional Certification and/or Certified ScrumMaster Certification. See staffing table in Staff Qualifications section (6.3) for list of qualified personnel.*

6.1 Key Personnel

Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer (CO) and the Contracting Officer's Representative (COR) no less than 15 business days in advance. The Contractor shall 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 CO.

The Contractor shall not replace Key Contractor personnel without approval from the CO. The Government may designate additional Contractor personnel as Key at the time of award or through a contract modification.

The key positions for this requirement are:

6.1.1 Senior Analyst

The Contractor shall provide a Senior Analyst who shall be responsible for all contractor work performed under this SOW. The Senior Analyst shall oversee and verify the hours worked by all personnel, considering flexible schedules, breaks, leave, telework, and off-site meetings. This support personnel shall be a single point of contact for the CO and the COR. The Contractor shall ensure the designated personnel has a minimum of ten (10) years of experience. The Contractor shall ensure that mandatory and recurring training requirements for contractors supporting this SOW are completed.

The name of the contract management personnel, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Senior Analyst, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Senior Analyst, only one alternate shall have full authority to act for the contractor on all matters relating to work performed under this contract. Additionally, the Contractor shall not replace the Senior Analyst without prior approval from the CO. The Senior Analyst shall be available to the COR via telephone between the hours of 7am and 5pm Eastern Standard Time (EST), Monday through Friday, and shall respond to a request for discussion or resolution of problems within eight hours of notification.

6.1.2 Senior Portfolio/Program/Project Analyst

The Contractor shall provide a Senior Portfolio/Program/Project Analyst who shall oversee and manage contractor personnel tasked with operations and governance support work performed under this SOW; which includes the establishment and execution of the Program/Project Review Board, Change Control Board and other Governance boards.

The name of the personnel, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Senior Portfolio/Program/Project Analyst, shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Senior Portfolio/Program/Project Analyst without prior approval from the CO. Senior Portfolio/Program/Project Analyst shall be available to the COR via telephone between the hours of 7am and 5pm Eastern Standard Time (EST), Monday through Friday, and shall respond to a request for discussion or resolution of problems within eight hours of notification.

6.1.3 Senior Administrative Specialist

The Contractor shall provide a Senior Administrative Specialist who shall oversee and manage the administrative tasks outlined in this SOW.

The name of the personnel, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Senior Administrative Specialist, shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Senior Administrative Specialist, without prior approval from the CO. The Senior Administrative Specialist shall be available to the COR via telephone between the hours of 7am and 5pm Eastern Standard Time (EST), Monday through Friday, and shall respond to a request for discussion or resolution of problems within eight hours of notification.

6.2 Qualified Staff

The Contractor shall provide qualified individuals with the education and experience required to support

the Government based on tasks described in the Tasks section (5.0) of this SOW.

The Contractor shall provide the COR with a resume for each individual proposed for review and approval based on the qualifications described in Staff Qualifications section (6.3) of this SOW.

The Contractor shall seek written approval from the COR for a waiver to assign any individual who does not meet the minimum qualifications.

The Contractor shall provide personnel that are able to fluently read, write, speak, and understand English as their primary or alternate language.

6.3 Staff Qualifications

The Contractor shall perform the work described in Place of Performance section (3.0) of this SOW with personnel fitting the following labor categories. Each labor category is described along with its education and experience requirements. Each personnel must have specialized experience and knowledge commensurate with the following descriptions and qualifications:

POSITION	DESCRIPTION	MINIMUM REQUIREMENTS
Senior Analyst*	Oversees the development of contractor staff, and alignment of the staff to the Government's requirement at the task order level. Provides and ensures quality and timely services and delivery of contractual items under the contract terms and conditions. Serves as point of contact with the Contracting Officer's Representative (COR) and Contracting Officer (CO). Performs day-to-day management of contract execution, possibly involving multiple groups of personnel at multiple locations. Establishes and maintains technical and financial reports demonstrating task order progress and delegates responsibilities to subordinates and oversees successful contract/task order completion. Maintains effective client interface with the COR. Motivates contractor staff and ensures contractor staff are adequately trained and fully understands the work environment. Contributes to the evaluation, analysis, and development of recommended solutions. Resolves complex problems, which require an in-depth knowledge of subject matter related to the designated field or discipline. Applies principles and methods of the subject matter to specialized	BA/BS + 10 years of relevant or Master's + 5 years of relevant experience.

	solutions. Areas of expertise may include business process reengineering, performance management, statistical process control, individual and organizational assessment and evaluation, process modeling and simulation, strategic and business planning, change management, organizational development, quality assurance, regulatory compliance, and situational awareness and decision support.	
Analyst	See Description for Senior Analyst. The analyst responsible for the learning and skill development task outlined in this SOW oversees the development of the PM skill development and training. Experienced with providing program management, training, skills assessments, developing curriculum, and similar support. Experienced with developing large enterprise-wide online training courses and programs. The ideal applicant would have knowledge of the 508 compliance requirements and other federal regulations regarding online content and accessibility. Ability to understand complex technical issues and communicate those issues to a non-technical audience. Ability to communicate effectively, both orally and in writing.	BA/BS + 5 Years of relevant experience or Master's + 3 years of relevant experience.
Senior Portfolio/ Program/ Project Analyst*	Assist program managers in their execution of programs. Will be required to assist with defining requirements; provides input to project scope, schedule and budget based on an understanding of the program lifecycle. Assist in maintaining changes to project baselines; monitors deliverables; assess documents, plans and applications; conducts quality reviews of projects and tasks. Prepares presentations and other materials to support project functions. Leads activities to identify project risks and assist in the development of mitigation plans. Drafts correspondence, reports, white papers, minutes, spreadsheets, communications products, briefs, and other documentation. Maintains and tracks action items and participates in meetings. Assist in drafting various documents supporting a procurement. Will be relied upon to provide technical and procurement guidance to junior contractor staff on the team.	BA/BS + 10 years of relevant or Master's + 5 years of relevant experience.
Senior Documentation Specialist	Supports the development and maintenance of effective information management plans, processes, repositories and systems. Organizes, maintains, tracks, and files documentation in electronic formats. Maintains document version control and configuration management. Evaluates documentation, specifications, reports, and presentations. Outlines and develops technical documentation detailing the design, development, testing, installation, and maintenance of systems and processes. Develops databases that extracts and interprets data from the repositories.	BA/BS + 10 years of relevant experience or Master's + 5 years of relevant experience.
Senior Technical	Gathers, analyzes, and composes complex technical information. Conducts research and ensures the use of proper technical terminology. Translates technical information into clear, readable documents to be used by technical and non-technical personnel. Organizes material and writes	BA/BS + 10 years of relevant experience or Master's + 5 years of relevant

Writer / Editor / Communication s Specialist	descriptive copy according to establish standards regarding order, clarity, conciseness, style, and terminology. Selects photographs, drawings, sketches, diagrams, and charts to illustrate material. Develops communications materials for publications, internet, strategic initiatives, user manuals, training materials, installation guides, white papers, reports, etc. Develops, writes, and edits functional descriptions, system specifications, special reports, or any other customer deliverables and documents. Provides technical writing support and deciphers directions provided on scripted storyboards, specifications, etc. Reviews documents for technical accuracy in accordance with applicable regulations. Supports content creating and management on networks and web platforms (i.e. Social Media).	experience.
Senior Administrative Specialist	Performs administrative duties as required such as writing memos, filing, typing, and copying documents. Develops spreadsheets, maintains program, project, and task files, technical support information for program, project managers. Organizes and maintains calendars for one or more managers, schedules meetings, takes meeting notes and distributes to attendees. Prepares correspondence, briefs, and reports and assists with planning, initiation, and tracking of task assignments and associated data. Assists with preparing and processing travel and maintaining travel requests and records. Distributes and monitor taskings, data calls and coordinating troubleshoot requests.	BA/BS + 7 years of relevant experience or Masters + 5 years of relevant experience.

**Staff fulfilling these positions are required to have a Project Management Professional Certification and/or Certified ScrumMaster Certification.*

6.4 Continuity of Support

The Contractor shall ensure that the required level of support 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., the Contractor shall provide e-mail notification to the COR prior to absence.

6.5 Employee Identification

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the contractor name, the employee's photo, name, 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.

6.6 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 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 COR shall ensure contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

6.7 Removing Employees for Misconduct Reasons

The Government may, at its sole discretion (via the CO), 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 CO

will provide the Contractor with a written explanation to support any request to remove an employee.

6.8 Training Requirements

The Contractor shall work with the Federal Training manager to ensure all personnel enroll and complete all DHS/S&T mandatory training.
The Contractor shall provide a list of all employees and their training status, completion dates, and upcoming training dates.

Additional training may be required at any time during this contract as notified by the COR or CO.

7. TRAVEL

The Contractor may be required to travel in support of this requirement. All travel required by the Government outside the Greater Washington DC Metropolitan Area (see OMB Bulletin No. 05-02 and code 47900) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations (FTR), with no profit or fee applied. The Contractor shall be responsible for obtaining written Contracting Officer's Representative (COR) approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

The Government will not reimburse the Contractor for local travel (within the Greater Washington, DC Metropolitan Area). All travel-related expenses (including, but not limited to, airfare, lodging, meals, rental cars, and incidental expenses) incurred by the Contractor as a result of performing the services in this SOW shall be reimbursed in compliance with the FTR and resultant awarded Task Order. All travel requests must receive prior written approval from the Task Order COR. Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoice(s).

8. SURGE RESPONSE

The Contractor may be required to provide additional support described in the base year and each option year, depending on the level of effort required each year. These tasks shall be reimbursed on a Labor Hour basis subject to the labor categories and hourly rates contained in the pricing schedule and the terms of the modification authorizing the work.

9. INSPECTION AND ACCEPTANCE CRITERIA

Inspection and acceptance of products and services shall be performed by a duly authorized Government representative identified in the Task Order in accordance with the Inspection and Acceptance clauses in the SETA III contract and as further defined in the Task Order.

All deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements by the COR or as detailed in individual Task Order. Inspection may include validation of information or software through the use of automated tools for the deliverables, as specified in the Task Order.

The Government requires a period not to exceed thirty (30) calendar days after receipt of final deliverable items for inspection and acceptance or rejection unless otherwise specified in the awarded Task Order. The Contractor shall provide work products and deliverables within the acceptance criteria identified below:

Quality measures, as set forth below, will be applied to each Work Product and Deliverable.

- **Adherence to Requirements** - Work products and deliverables shall adhere to the requirements in the statement of work and all DHS S&T policies and procedures.
- **Accuracy** – Work products and deliverables shall be free from errors and mistakes; and be

developed in accordance with applicable laws, regulations, policies, and procedures.
- **Completeness** – Work products and deliverables shall have all parts or elements.
- **Clarity** – Work products and deliverables shall be easy to understand.
- **Timeliness** – Work products and deliverables shall be available at the time required and generated on or before specified and mutually agreed to due dates. If a new due date has been agreed upon, then the work product and deliverable shall be available on or before that new due date.
- **Format** – Work products and deliverables shall be submitted in hard and/or soft copy, as appropriate. Both hard and soft copy formats shall follow specified guidance, directives, and/or policies.

10. DELIVERABLES

The Contractor shall provide all deliverables electronically, unless otherwise specified, directly to the COR and the PM (PSO Division Director). The Contractor shall deliver all technical reports and other data developed under this SOW, along with the appropriate documentation to the COR and PM (PSO Division Director) as they are completed, unless otherwise specified.

All deliverables become the property of the Government and may not be disseminated without prior written approval from DHS.

TASK	DELIVERABLE / EVENT	DUE BY	DELIVER/REPORT TO:
5.1	Post Award Conference	Ten (10) business days after award	N/A
5.1	Draft Contractor Project Plan (60/90/120-day plan)	Ten (10) business days after award	CO/COR/PM
5.1	Final Contractor Project Plan (60/90/120-day plan)	Fifteen (15) business days after post award conference.	CO/COR/PM
5.2	Monthly Status Report	Ten (10) calendar days after end of each month	COR/PM
5.3	PSO Sharepoint Site Content Refresh	Initial refresh no later than thirty (30) business days after award; At least monthly thereafter	PM

5.4	Draft Governance Support Strategy	Thirty (30) business days after post award conference	COR/PM
5.4	Final Governance Support Strategy	Twenty (20) business days after receipt of Government comments	COR/PM
5.5	Draft Communications Plan	Twenty (20) business days after post award conference	COR/PM
5.5	Final Communications Plan	Fifteen (15) business days after receipt of Government comments	COR/PM
5.6	Draft Training Plan	Twenty (20) business days after post award conference	COR/PM
5.6	Final Training Plan	Twenty (20) business days after receipt of Government comments	COR/PM
5.7	Draft Records Management File Plan	Sixty (60) business days after post award conference	COR/PM
5.7	Final Records Management File Plan	Twenty (20) business days after receipt of Government comments	COR/PM
5.8	Draft Staffing Plan	Ten (10) business days after award	COR/PM
5.8	Final Staffing Plan	Fifteen (15) business days after receipt of Government comments	COR/PM

11. WORK SCHEDULE

The Contractor shall provide on-site services Monday through Friday, from 7:00 AM to 5:00 PM (excluding federal holidays). All contractor personnel shall work for eight hours during this business day not including lunch or other breaks. These eight work hours must be spent performing work under this SOW. If offsite work is authorized it shall be completed in the same manner, for eight hours during the business day. The COR may approve deviations from the standard eight-hour day.

The holidays observed by the Federal Government are the following:

January 1	New Year's Day
Third Monday in January	Birthday of Martin Luther King, Jr.
Third Monday in February	Washington's Birthday
Last Monday in May	Memorial Day
July 4	Independence Day
First Monday in September	Labor Day

Second Monday in October	Columbus Day
November 11	Veterans Day
4th Thursday in November	Thanksgiving Day
December 25	Christmas

Contractor personnel may be permitted to telework, from home or from contractor facilities, in the event of Government office closures, commuting disruptions, continuity of operations exercises, or unusual work needs in special circumstances. Telework may be permitted on a permanent or regular basis. All telework must be approved by the COR and PSO Division Director.

12. Security Requirements

Safeguarding of Sensitive Information (MAR 2015)

(a) Applicability. This clause applies to **ManTech SRS Technologies, Inc.** 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:
(j)

(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.

(k)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 **ManTech SRS Technologies, Inc.** 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.

DHS may exercise full control over granting, denying, withholding, or terminating unescorted access to DHS facilities, DHS systems, and/or sensitive DHS information for government/contract employees. Access will be based upon the results of a DHS fitness/suitability investigation. DHS may, as appropriate, make favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the government/contract employee 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 DHS fitness/suitability authorization will follow. The granting of a favorable EOD decision or a full DHS 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 contract/task order. No employee of the government/contractor shall be allowed unescorted access to a

DHS facility, access to any sensitive DHS information, or access to DHS Systems without a favorable EOD decision or DHS fitness/suitability determination by the DHS HQ Office of Security. Government/contract employees assigned to the contract/task order not needing access to sensitive DHS information, DHS systems, or access to DHS facilities will not be subject to DHS fitness/suitability screening. Government/contract employees waiting on an EOD decision may not begin work on the task order. Limited access to DHS facilities is allowable prior to the EOD decision if the government/contract employee is escorted by an approved DHS employee. This limited access is to allow government/contract employees to attend briefings, nonrecurring meetings, and begin transition work. During one's limited access the government/contract employee will not have access to sensitive or classified DHS information.

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 government/contract employee 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 government/contract employee is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

HSAR 3052.204-71 Contractor Employee Access (SEP 2012)

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

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

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

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

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

(b) "Information Technology Resources" include, but are not limited to, computer equipment,

networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

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

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

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

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

(End of clause)