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

1. REQUISITION NUMBER	PAGE	OF
RSTC-20-00038	1	36

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
70RSAT19D00000003	09/23/2020	70RSAT20FR0000091	70RSAT20R00000032	05/29/2020

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

8. OFFER DUE DATE/LOCAL TIME ET

9. ISSUED BY CODE DHS/OPO/S&T/S

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

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

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

NAICS: 541611
SIZE STANDARD: $15.0

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

15. DELIVER TO CODE S&T MURRAY LANE

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

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

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

17a. CONTRACTOR/ OFFEROR CODE 9329023640000 FACILITY CODE

NOBLIS INC
ATTN (b)(6)
2002 EDMUND HALLEY DRIVE
RESTON VA 20191

TELEPHONE NO. 7036102290

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

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

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

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 932902364+0000 Division: TCD Program: Technology Centers Project: Innovation Program Support DHS Contracting Officer's Representative: Alicia Henderson (b)(6) Appropriation Year: FY20 (J0 Funds) Budget Authority: 3-Year R&D (J0) Funds FY20 (J0) 3-year R&D Funds cannot be obligated *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$581,309.76

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

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

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

(b)(6)

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	past 09/30/2022 ALC: 70-08-1513 TAS: 70 20/22 0803 1. The U.S. Department of Homeland Security (DHS) issues this time-and-materials (T&M) Task Order Procurement Instrument Identifier (PIID) 70RSAT20FR0000091 ("Task Order" or "Contract") to obtain technical support services for the Science and Technology Directorate's (S&T), Technology Centers Division (TCD) pursuant to the terms and conditions of Noblis, Inc.'s ("Contractor") S&T Systems Engineering and Technical Assistance (SETA) III Indefinite-Delivery, Indefinite-Quantity (IDIQ) Contract identified in Item 2. 2. As a result of this action, the Base Period Contract Line Item Numbers (CLIN) 0001 and 0002 are funded in the amount of (b)(4) 3. Base Period CLIN 0003 and Option Periods 1 and 2 are unfunded and/or unexercised. 4. The Contractor shall perform all work under this Task Order in accordance with the attached Terms and Conditions, Statement of Work (SOW) and Pricing Schedule. Continued ...				

32a. QUANTITY IN COLUMN 21 HAS BEEN

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

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

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

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	5. Per FAR 16.601(d)(2), the amount of funds obligated under this Task Order is a ceiling that the Contractor exceeds at its own risk. All hours worked must be covered by a labor category listed in this Task Order and billed at the attendant fixed hourly labor rate for that labor category for the applicable performance period. Per Federal Acquisition Regulation 16.601(a), materials, as defined at FAR 2.101, used or acquired in the performance of this Task Order shall be billed consistent with the Contractor's SETA III IDIQ Contract. Materials CLINs may be incrementally funded at the Government's discretion up to their stated maximum price. Period of Performance: 09/23/2020 to 09/22/2023				
0001	Base Period - Labor Award Type: Time-and-materials Accounting Info: NONE000-000-J0-67-01-96-201-36-03-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-61-01-08-001-35-01-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-62-02-02-003-35-02-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Period of Performance: 09/23/2020 to 09/22/2021				(b)(4)
0002	Base Period - Materials Award Type: Time-and-materials Accounting Info: NONE000-000-J0-67-01-96-201-36-03-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-61-01-08-001-35-01-0000-00-00-00-00 -GE-OE-25-37-000000 Funded: (b)(4) Accounting Info: NONE000-000-J0-62-02-02-003-35-02-0000-00-00-00-00 Continued ...				(b)(4)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	-GE-OE-25-37-000000 Funded: (b)(4) Period of Performance: 09/23/2020 to 09/22/2021				
0003	Base Period: Optional Surge Labor Award Type: Time-and-materials Amount: (b)(4) (Option Line Item) Period of Performance: 09/23/2020 to 09/22/2021				(b)(4)
1001	Option Period (1) - Labor Award Type: Time-and-materials Amount: (b)(4) Option Line Item) Period of Performance: 09/23/2021 to 09/22/2022				
1002	Option Period (1) - Materials Award Type: Time-and-materials Amount: (b)(4) Option Line Item) Period of Performance: 09/23/2021 to 09/22/2022				
1003	Option Period (1): Optional Surge Labor Award Type: Time-and-materials Amount: (b)(4) (Option Line Item) Period of Performance: 09/23/2021 to 09/22/2022				
2001	Option Period (2) - Labor Award Type: Time-and-materials Amount: (b)(4) Option Line Item) Period of Performance: 09/23/2022 to 09/22/2023				
2002	Option Period (2) - Materials Award Type: Time-and-materials Amount: (b)(4) Option Line Item) Period of Performance: 09/23/2022 to 09/22/2023				
2003	Option Period (2): Optional Surge Labor Award Type: Time-and-materials Amount: (b)(4) (Option Line Item) Period of Performance: 09/23/2022 to 09/22/2023				
	The total amount of award: (b)(4) The Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	obligation for this award is shown in box 26.				

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

1. REQUIREMENT TITLE:

Chemical and Biological Sciences Subject Matter Expertise

2. PROCUREMENT INSTRUMENT IDENTIFIER:

70RSAT20FR0000091

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: Wednesday, September 23, 2020

6. PERIOD OF PERFORMANCE

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

6.2. The period of performance for this requirement is 12 months from date of award.

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

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

Option Period	Duration (in Months)
Option Period 1	12 months
Option Period 2	12 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 9/23/2020 through 9/22/2023.

7. INFORMATION

7.1. NAICS Code and Small Business Size Standard:

The principal nature of the requirements described in this Task Order 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 Task Order are best represented by PSC Code: R408 - Support-Professional: Program Management/Support

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

7.4. Telework for this requirement:

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

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

7.5. Security:

This requirement is:

☐ Unclassified ☐ Classified ☒ Mix of Both

The Facility Clearance Level for this requirement is:

☒ Unclassified ☐ Secret ☐ Top Secret

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

☒ Government ☐ Contractor ☐ Mix of Both

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

1120 Vermont Avenue NW, Washington DC

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 one (1) day; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least seven (7) days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 36 months.

(End of clause)

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

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

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

The Key Personnel or Facilities under this Contract:

All assigned personnel

HSAR Class Deviation 15-01 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

(b) *Definitions*. As used in this clause—

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

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

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the

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

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

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

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

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

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

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

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

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

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

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

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

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

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

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding*

Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

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

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

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in

these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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

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

Security Authorization Process Guide including templates.

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

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

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA

in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual

accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

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

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

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

(5) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

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

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

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

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

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

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

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

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

(1) The Contractor shall have in place procedures and the capability to notify

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

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

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

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

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

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

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

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

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

(End of clause)

HSAR Class Deviation 15-01 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

(b) *Security Training Requirements*.

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

subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

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

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

(End of clause) (End of clause)

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

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

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

(End of clause)

11.7. CONTRACTING OFFICER'S REPRESENTATIVE (COR)

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

(b) The COR for this Task Order is:

(b)(6)

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

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

(e) The ACOR for this Task Order is:

(b)(6)

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

11.8. CONTRACTING OFFICER AND CONTRACT SPECIALIST

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

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

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

(b)(6)

12. OPTIONAL TASKS AND SURGE CLINS

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

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

The Government will make all efforts to notify an awardee no later than 15 days before the exercise of an optional task or surge CLIN. This notice will be provided by e-mail. Optional tasks and surge CLINs will be exercised via formal modification to the task order. This modification will be sent by the task order Contract Specialist or Contracting Officer. Surge CLINs will not and cannot be ordered by the Contracting Officer's Representative.

ATTACHMENTS

Number	Title	# of Pages
(1)	Statement of Work	12
(2)	Pricing Table	2

Attachment 1 – Statement of Work

U.S. Department of Homeland Security (DHS)

Science and Technology Directorate (S&T)

Statement of Work (SOW)

for

Systems Engineering and Technical Assistance (SETA) Support Services

Chemical and Biological Sciences Subject Matter Expertise

1. General

1.1 Background

The United States Department of Homeland Security (DHS) is committed to using cutting-edge science and technology to make the U.S. more secure. The DHS Science and Technology Directorate (S&T) organizes and supports the scientific, engineering, and technological resources of the United States and applies these resources to produce and deploy technological tools and knowledge products to help protect the homeland. DHS S&T is organized into four main groups: Office of Mission and Capability Support, Office of Science and Engineering, Office of Innovation and Collaboration, and Office of Enterprise Services, that work together to support DHS operating Components and others in the Homeland Security Enterprise (HSE) [1]. S&T is organized by functions in which each Division plays a critical role in the execution of research and development programs benefitting homeland security missions. Within S&T, programs are matrixed teams that draw support across the Directorate in order to accomplish program goals.

The Technology Centers Division (TCD) within the Office of Science and Engineering is the source of scientific, engineering, and technological expertise and solutions for programs, projects, and activities across S&T and DHS. S&T Technology Centers supply subject matter expertise and conduct core scientific research to provide foundational knowledge and develop cross-cutting technological solutions that address current and future homeland security challenges. The Technology Centers are responsible for three primary activities:

Subject Matter Expert Advisement: Technology Center personnel are subject matter experts (SMEs) and advise S&T programs, DHS Components, and other key stakeholders in scientific, engineering, and technology areas critical to the homeland security enterprise.

S&T Program Technical Support: The Technology Centers directly contribute to S&T programs by serving as Technical Managers and providing expert support on programs to oversee the technical activities of those programs that deliver solutions against customer-identified requirements.

[1] DHS defines the homeland security enterprise as the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities, who share a common national interest in the safety and security of the United States and the American population (GAO, *Department of Homeland Security: Progress Made and Work Remaining after Nearly 10 Years in Operation*, GAO-13-370T (Washington, D.C.: Feb. 15, 2013)).

Core Research: The Technology Centers conduct cross-cutting, foundational research, analysis, and experiments, to build knowledge by:

- Maintaining S&T's technical baseline competency and awareness of the state-of-the-art/art-of-the-possible in key science, engineering, and technology areas.
- Understanding how scientific and technological advancements can be harnessed for homeland security missions – or how they may become are risk or threat.
- Determining how to secure the use of these advancements.
- Identifying methods for detecting, countering, and mitigating the misuse of these advancements.

S&T's individual Technology Centers focus on foundational science, advanced computating, and innovative systems and technology. While these Tech Centers conduct core research, the Division also houses a cadre of senior engineering and science experts who serve as expert advisors across the Department. They and the Technology Center SMEs work together to stay abreast of enduring and cutting-edge research and contribute to activities being conducted on behalf of S&T program managers and Component customers. Additionally, these senior expert advisors are made available to the Interagency and the Department to maintain open, collaborative relationships and address a wide range of critical problems facing the nation.

TCD works closely with S&T's Office of Mission and Capability Support (MCS), which primarily interacts with DHS operational Components, first responders at all levels of government, emergency management personnel and public safety and other homeland security organizations to define priorities, gaps and requirements to find or develop technology solutions. MCS focuses on the following DHS mission topic areas:

- ***Border, Immigration and Maritime*** supports U.S. Customs and Border Protection, U.S. Coast Guard, Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services with technology solutions for their operational needs. Through research, development, testing and evaluation, S&T supports these Components in operational settings such as ports of entry (POE) and areas between POE, covering all domains, including air, ground, underground, water, and underwater.

- ***First Responder and Detection*** supports DHS Countering Weapons of Mass Destruction Office, Federal Emergency Management Agency, Federal Law Enforcement Training Centers, and first responders. Through research, development, testing and evaluation, S&T strengthens emergency managers and responders' ability to protect the homeland by providing the tools and knowledge they need to save lives and protect property, while staying safe.

- ***Physical and Cyber Security*** supports the Cybersecurity and Infrastructure Security Agency (CISA), Transportation Security Administration (TSA), United States Secret Service (USSS) and Office of Intelligence and Analysis (I&A). S&T conducts research, development, testing and evaluation in three main focus areas: physical security, cybersecurity, and explosives detection and mitigation. Within these focus areas S&T assesses and analyzes threats and vulnerabilities to critical infrastructure, enhancing resilience through advanced planning and mitigation, preventing and disrupting criminal use of cyberspace, strengthening the security and reliability of the cyber eco system, streamlining passenger screening, and preventing homemade explosive attacks.

1.2 Scope of Work

DHS S&T is funded and operated by the US Government. Its government staff cannot work effectively without significant help from commercial companies contracted to perform important support services. Systems Engineering and Technical Assistance (SETA) contractors help S&T understand its technical mission and requirements as well as the state of the art in technical innovation. In addition, they answer the programmatic and organizational requirements needed to set up and operate a sophisticated, modern-day technological organization. SETA perform basic but critical support functions that often go unheralded. A

government organization dedicated to delivering on its mission must be a team of government decision-makers who set priorities, lead capabilities, and determine funding, married to an effective staff of knowledgeable, dedicated and broad-based support personnel.

SETA staff are required to assist the government in subject matter expert advisement. Recipients of such advisement may include customers both internal to S&T as well as operational Components within DHS, other federal agencies who are partners of DHS, and the Homeland Security Enterprise. Successful SETA staff help ensure that S&T conduct cross-cutting core research, develop its programs and their attendant projects; maintain awareness of technologies on or over the horizon; and understand the many parties, platforms, and processes inherent in a complex technology development system.

The scope of chemical and biological technical work performed by this SETA staff is pursuant to Section 1.2.1 of the SETA III indefinite-delivery, indefinite-quantity (IDIQ) SOW.

The efforts of this support contract will be matrixed across the organization. Matrixed offices, divisions and portfolios may include any of the four "pillars:" Office of Mission and Capability Support; Office of Science and Engineering; Office of Innovation and Collaboration; and Office of Enterprise Services. Sub-pillars and portfolios within each pillar each may have divisions, offices, personnel or other entities that require support.

This contract is limited to S&T staffing only. Any other activity, such as specific project funding, shall require a different funding vehicle.

2. Task Requirements

Because S&T has aligned itself into a matrix of personnel, skills, and customers, the Contractor must both possess and enable the flexibility of thinking and organization required to execute to multiple customers' needs across the Homeland Security Enterprise. The Contractor must be able to assist the government in responding to varied and changing circumstances and dynamic customer requirements in an agile and flexible manner.

The Contractor shall support DHS S&T in the execution of both Tech Center core research that enables S&T to understand how scientific and technological advancements can be harnessed for homeland security missions and S&T's large research and development (R&D) programs that provide solutions to current operational needs across the HSE. The program office is defined as its federal staff tasked with determining requirements, directing R&D and technology and knowledge discovery programs, and interacting with customers at the federal, state, local, tribal, territorial, and international levels to improve capabilities at all levels.

As needs arise based on the organizational matrix, support may be provided to any Technology Center, strategic program, R&D project, or Division within S&T in its role to provide technical expertise and support. The Contractor shall not be required to provide support without documented requirements, as determined by the requesting program and reviewed by COR and Task Order Manager (TOM), in consultation with the Government PM. Hours devoted to each Office or Division will be determined by the COR, in consultation with the Government PM.

The Contractor may be required to provide additional support under the task areas described in the base period and each option period, depending on the level of effort required for each period.

As identified by the government, tasks common to all support provided include but are not limited to technical expertise and advisement as needed:

2.1. The Contractor shall provide *scientific evaluation and technical support* to the government on factors relevant to enduring and technical research and developments on engineered and emerging chemical, biological, and explosives threats to the Homeland.

2.2. The Contractor shall participate in *technical exchanges*, workshops, conferences, and in-process reviews and demonstrations relating to chemical, biological, and explosives hazards and provide meeting minutes or reports outlining the events and any key items that require immediate attention. This may include both classified events, and/or events with S&T's domestic and international partners. These interactions are subject to Section H.12 of the SETA III IDIQ Contract.

2.3. The Contractor shall research and assess *state-of-the-art and emerging trends* in biological and chemical research. The Contractor shall present the results of their efforts, as required, through:

2.3.1. Gathering, analyzing, and composing complex technical information such as analyses of alternatives on technology solutions, technology capability summaries, and technical requirements documents.

2.3.2. Researching and assessing patent activity, published articles, market information, conference proceedings, research reports, etc.

2.3.3. Creating technical roadmaps relating to chemical, biological, and explosives hazards. Technical roadmaps outline plans for implementing technical solutions in both short and long-term timeframes.

2.4. The Contractor shall assist in preparation of *technical presentations* for delivery by Federal staff at meetings and conferences on the subject of biological and chemical research, methods, phenomena, or hazards. The Contractor will engage in technical writing and produce technical documentation regarding biological and chemical subjects.

2.5. The Contractor shall assist in preparing *technical responses to S&T Executive Secretary* taskers and other data calls related to biological and chemical research. Such services are limited by the IDIQ's H.11 clause "Disclosure and Avoidance of Inherently Governmental Functions."

2.6. The Contractor shall conduct *technical reviews* for assigned biological and chemical R&D programs and projects to monitor program, project, and research technical performance and review deliverables to ensure technical goals and objectives are met, identifying potential technical risks, and path forward options/recommendations.

3. Deliverables

3.1. Progress Meetings

The TOM shall review the status and results of Contractor performance with the COR and Government PM on a monthly basis, at a minimum, at scheduled meetings. These meetings can be either working or formal sessions to review overall program efforts. Monthly meetings may be held via teleconferences if in-person meetings are not workable.

3.2. Reports

The Contractor shall provide all written reports in electronic format with read/write capability using Microsoft Office and Adobe applications, in accordance with the Deliverables Chart (Section 3.3).

3.2.1. Project Plan: The Contractor shall deliver a draft Project Plan within three (3) business days of contract award to the Contracting Officer, COR, and Government PM. The Contractor shall deliver the final version of the Project Plan, incorporating Government comments provided at the Kick-Off Meeting, to the Contracting Officer, COR, and Government PM within five (5) working days following the Kick-Off

Meeting. Included in this plan shall be at a minimum the staffing, organization, assigned tasks, travel, and means of ensuring government satisfaction.

3.2.2. Monthly Progress Reports: The TOM shall provide a monthly progress report to the Contracting Officer, COR and PM via electronic mail. This report shall provide monthly cost and performance reporting of all tasks. At a minimum, these reports must include details of support provided, listing of completed assigned tasks, completed/planned travel events, past expenditures, projected expenditures for the next reporting period and to term, major issues affecting performance, any telework performed, detailed number of staff, hours worked by labor category, and any Contractor concerns or recommendations. The financial portion of the report must be structured to enable ready discernment of expenditure trends, projections, and variances.

3.2.3. Bi-Weekly Update: The Task Order Manager shall provide a bi-weekly, in person progress report using the attached "Quad Chart" to Government PM and COR. At a minimum, these reports shall include status of funds, staffing status, and issues requiring COR or Program Manager action. Bi-weekly status update meetings and Quad Chart submissions shall begin thirty (30) calendar days following Task Order award.

3.2.4. Customer Satisfaction Survey: The Task Order Manager shall conduct a survey of federal clients regarding their satisfaction with SETA performance in coordination with the COR and Government PM. Survey results may be anonymized for broad distribution but must be specific per federal client(s) for the COR's review.

3.2.5. Transition: Transition-In and Transition-Out activities shall be conducted in accordance with Attachment I of the Contractor's SETA III IDIQ Contract.

3.3 Deliverables Chart

DEL #	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	Draft Project Plan	With proposal	See solicitation.
2	Final Project Plan	Within five (5) working days of Kick-Off Meeting	One electronic copy shall be provided to the Contracting Officer's Representative (COR) and the Government PM.
3	Meeting Minutes	Within one (1) working day of meetings	One electronic copy to COR and Government PM.
4	Technical Reports	As needed as determined by COR and Government PM	One electronic copy to COR and Government PM.
5	Technical Roadmaps	As needed as determined by COR and Government PM	One electronic copy to COR and Government PM.
6	Draft Technical Presentations	As needed as determined by COR and Government PM	One electronic copy to COR and Government PM.

DEL #	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
7	Technical Review Results	As needed as determined by COR and Government PM	One electronic copy to COR and Government PM.
8	Monthly Progress Report of activities of each SETA in support of government clients, including status of funds and personnel hiring status	15th of each month.	One hard copy shall be provided to the COR and one electronically submitted copy shall be provided to the both the COR and CO.
9	Bi-weekly status update Quad Chart	At least two (2) working days before each bi-weekly status update	One electronic copy shall be provided to the COR and Government PM.
10	Bi-weekly status update in-person meeting with COR and PM	Bi-weekly, per federal staff availability	N/A
11	Draft Customer Satisfaction Survey	(With proposal)	(TBD)
12	Final Customer Satisfaction Survey	Five (5) working days following Kick-Off	One electronic copy shall be provided to the COR and Government PM.
13	Customer Satisfaction Survey results	Semi-annually (or more frequently, at Government direction)	One electronic copy shall be provided to the COR and Government PM.

4. Other Contract Details:

4.1 Period of Performance

The period of performance for this Task Order consists of a twelve (12) month base period and two (2) twelve (12) month option periods. The total period of performance, if all options are exercised, is thirty-six (36) months from date of award.

4.2 Representation at Meeting Events

In the performance of this Task Order, Contractor staff may be required to attend and/or participate in meetings, teleconferences, workshops, conferences, international and domestic partner technical exchanges, demonstrations, and other gatherings. In all interactions with parties outside of S&T, Contractor staff are bound by the terms of Section H.12 "Protocol and Contractor Badge."

Participating in any meetings, teleconferences, workshops, conferences, international and domestic partner technical exchanges, demonstrations, and other gatherings on behalf of DHS with parties outside of S&T without a technical Federal representative must be approved in advance by the COR.

4.3 Travel

Travel shall be necessary to meet and coordinate exchanges of information on this Task Order. Limited Contractor foreign travel is anticipated. The DHS S&T COR must approve all travel in advance. This travel will be managed by the TOM within the allocated travel budget. Travel will be reimbursed in accordance with the limits set forth in the Federal Travel Regulations and Federal Acquisition Regulation Subpart 31.205-46, provided the Contractor provides appropriate supporting documentation.

4.4 DHS-Furnished Information

S&T will provide DHS information, materials, and forms unique to DHS to ***the Contractor*** to support tasks under this SOW. Such DHS-provided information, materials, and forms shall remain the property of DHS, unless otherwise indicated in writing by DHS, and may not be distributed beyond the Contractor's staff without DHS's prior written permission.

4.4.1. The DHS S&T COR identified in this SOW will be the point of contact for identification of any required information to be supplied by DHS.

4.4.2. The Contractor will prepare all documentation (e.g., meeting and report deliverables or monthly status reports) according to the guidelines provided by DHS.

4.5 DHS-Furnished Facilities, Supplies, and Services

DHS-provided facilities is necessary for the services being performed under this SOW, such facilities will be provided at S&T's office in Washington, D.C. Parking facilities are not provided. Basic facilities such as work space and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general-purpose office supplies) will be provided to Contractor personnel working in S&T's office.

4.6 Place of Performance

The Contractor shall perform the work under this SOW at Federal facilities. Contractor staff may telework in the performance of this Task Order on a case-by-case basis approved in advance by the COR and Government PM.

4.7 DHS-Furnished Property

DHS property will be provided to the contractor or any of their performers unless otherwise agreed in a task order issued under this SOW. In such instances, DHS will maintain property records.

Before purchasing any items required to support technical tasks performed pursuant to this SOW, the Contractor shall obtain the DHS Contracting Officer and COR's prior written consent. If the DHS Contracting Officer and COR consent to such purchase, such item shall become the property of DHS. The Contractor must maintain any such items according to currently existing property accountability procedures. The DHS Contracting Officer and COR will determine the final disposition of any such items in writing at the conclusion of the Task Order's period of performance.

4.8 Security Requirements

Some of the work performed under this SOW will be classified with Secret and/or Top-Secret level classifications. All personnel assigned to perform work under this Task Order must obtain a Secret clearance and have the ability to obtain a Top-Secret clearance with access to Sensitive Compartmentalized Information (TS/SCI).

Labor Category	Clearance Required at EOD	Ability to Obtain Clearance Level
Senior Scientist	TS/SCI	N/A
Subject Matter Expert II	Secret	TS/SCI
Task Order Manager	Secret	TS/SCI

All unclassified "Official Use Only" work is expected to occur at the "medium" level per the NIST 800-60 (FIPS Security Categorization) and the Federal Information Security Management Act (FISMA). Any work at the "high" For Official Use Only level per the FISMA, or any work at the classified level, shall be performed on a stand-alone computer system accredited in accordance with the FISMA and applicable DHS policies. Some work may require working with Restricted Data, specifically including the following categories:

- 10.b Restricted Data
- 10.c Critical Nuclear Weapon Design Information
- 10.d Formerly Restricted Data
- 10.h Foreign Government Information

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.

4.9 Key Personnel

(a) All personnel assigned to support this effort are designated as *Key Personnel*, to include personnel assigned to support optional tasks and surge requirements. All experience will be evaluated based on relevance to this SOW.

(b) No later than the receipt of a written modification to exercise of any optional task(s) or surge line items in this Task Order, the Contractor must provide resumes for personnel to be assigned to support the exercised optional task(s) or surge requirements.

(c) Key personnel changes are subject to Section H.2 of the Contractor's SETA III IDIQ Contract. Key personnel changes require approval of the Contracting Officer and such requests shall be made in writing (including the resume of the proposed replacement) a minimum of fourteen (14) calendar days in advance.

4.10 Specific Technical Qualifications

The specific minimum technical qualifications for personnel performing work under this Task Order are outlined below:

Labor Category	Desired Education	Desired Experience and/or Expertise	Minimum Required Knowledge and Skills
Sr. Scientist	M.S. or higher: Organic, Inorganic Analytical, Physical Chemistry; or Biochemistry	Chemical synthesis preparation and execution Inorganic reaction, composition, and related elements Instrumentation for chemical characterization, contamination control, trace detection, and currency on state of the art for testing	Ability to manage all tasks and schedules to ensure activities are completed in a timely manner. Ability to communicate complex technical issues to a non-technical audience. Ability to research, analyze and compute mathematical and scientific data. Ability to apply advanced methods and techniques in a particular field of scientific specialization. Ability to develop, recommend and refine methods, theories and techniques to evaluate solutions to complex problems and to enhance performance standards, quality and productivity.
Subject Matter Expert II	M.S. or higher: Biological or chemical sciences	Multifunction chemical and biological agent detectors	Ability to manage all tasks and schedules to ensure activities are completed in a timely manner. Ability to communicate complex technical issues to a non-technical audience. Ability to plan and perform high-level engineering analysis, evaluation, design, integration, documentation, and implementation of complex solutions that require a thorough knowledge of applied mathematics, scientific, and/or technical skills. Ability to design and prepare engineering plans, reports and related documentation. Ability to absorb, integrate and interpret data through various methodologies.

Task Order Manager	Advanced Degree	Familiarity with chemical and biological fields of study	Ability to manage scope, schedule, and tasking of direct staff; ability to determine and solve resource needs. Ability to manage all tasks and schedules to ensure activities are completed in a timely manner. Ability to navigate matrixed technical environments. Ability to build collaborative, responsive relationships with federal clients.

4.10.1 Task Order Manager

The Contractor shall assign a Task Order Manager (TOM). The Task Order Manager shall be qualified to act as the Contractor's single point of contact for all technical and administrative matters related to this task order. The assigned TOM is not necessarily required to be dedicated solely to this Task Order, but the Government has discretion to determine whether TOM performance sufficiently facilitates or hinders execution of government's matrixed mission(s). The Contractor's management superior to the TOM must alert government COR and PM of all efforts proposed to be executed by TOM. The Contractor foregoing this responsibility is cause for TOM removal. The TOM shall be responsible for keeping the COR informed about Contractor progress throughout the performance period of this Task Order and ensure Contractor activities are aligned with DHS objectives.

4.11 Records Management

The Contractor must follow applicable National Archives and Records Administration standards and applicable DHS/S&T guidance as specified in the cognizant program office's approved Records Management File Plan.

4.12 Points of Contact

The Contractor POCs are as follows:

- Technical POC

(b)(6)

- Financial POC

(b)(6)

The Contractor may change an individual designated as a POC provided notice is given to the Government of such change.

ATTACHMENT: Bi-Weekly Quad Chart
(as referred to in Section 3.2.3)

Project Name: Date: XX/YY/ZZZZ

Gov Project Manager: email: xxxx.yyy@hq.dhs.gov **Task Lead: Xxxx Yyyy** email: Xxxx.Yyyy@Company.com

DESCRIPTION

Purpose: TBD
Problem Statement: TBD
Project Objective: TBD
Stakeholder Benefits: TBD
Scope of Work: TBD
Project Stakeholders: TBD

TASK DESCRIPTION / DELIVERABLES

Task 1: Project Management
Task 2: Requirements Validation
Task 3: Proof-of-Concept
Task 4: Prototype
Task 5: Design, Test & Evaluation
Task 6: Operational Test & Evaluation
Task 7: Transition
Task 8: Commercialization

Task Deliverables POP: 12/04/2016 to 12/03/2017	Due Date
Task 2	

ACCOMPLISHMENTS / SCHEDULE

Key Accomplishments/Events/Deliverables/Findings: (Previous 2 Weeks)
1. XXXXXXXXXXXX
2. XXXXXXXXXXXXXXXX
3. XXXXXXXXXXXXXXXXX
4. XXXXXXXXXXXXXXXXXXX

Planned Key Accomplishments / Events / Deliverables: (Next 2 Weeks)
1. YYYYYYYYYYYYYYYYY
2. YYYYYYYYYYYYYYYYYYYYYYYYYY
3. YYYYYYYYYYYYYYYYYYYYYYYYYY
4. YYYYYYYYYYYYYYYYYYYYYYYYYY

Planned Key Accomplishments / Events / Deliverables: (Next 30 – 60 Days)
1. ZZZZZZZZZZZZZZZZZZZ
2. ZZZZZZZZZZZZZZZZZZ
3. ZZZZZZZZZZZZZZZZZZZZZZ
4. ZZZZZZZZZZZZZZZZZZZZZZ

Monthly Expenditure	YTD Total	Balance	% Complete
$XX,XXX	$XXX,XXX	$X,XXX,XXX	XX %

STATUS: REPORT BY EXCEPTION

Requirements	Resources	Schedule	Dependency	Partner Engagement

= on track/no issue = minor issue/impact = problem/risk require mgmt input

Issue/Risk:
- if, then description
- if, then description

Resolution Approach:
Plan of action to resolve issue

Management Request:
Management support / involvement (if necessary)