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

1. REQUISITION NUMBER	PAGE	OF
OIT203012	1	107

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS06F0940Z		70SBUR20F00000222	70SBUR20R00000019	06/02/2020

7. FOR SOLICITATION INFORMATION CALL	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	DIANNE VALIANDO	802-872-4527	

9. ISSUED BY	CODE	10. THIS ACQUISITION IS
USCIS Office of Contracting Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403	CIS	☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % 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: 541512 SIZE STANDARD: $30.0

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	16. ADMINISTERED BY	CODE
DHS/USCIS/OIT/ISD 111 Massachusetts Avenue NW Washington DC 20529	HQOIT	USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403	CIS

17a. CONTRACTOR/ OFFEROR	CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
SOLUTIONS BY DESIGN II LLC [redacted] 1953 GALLOWS RD STE 650 VIENNA VA 221824096 TELEPHONE NO. [redacted]	1009429650000		See Invoicing Instructions	WEBVIEW

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

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 100942965+0000 Part I - Schedule GSA 8(a) STARS II Control Number: CN-S2-FY20-0047 Governance Communication Assessments & Classified Services (G-CACS) for the Office of Information Technology (OIT), Information Security Division (ISD) on a firm-fixed price (FFP) basis. In addition to the task order terms and *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* [redacted]

☐ 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: Factor 2 (R1) OFFER DATED 06/16/2020. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: ALL

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
	CHRISTOPHER C HATIN Digitally signed by CHRISTOPHER C HATIN Date: 2020.08.05 07:22:07 -04'00'

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
[redacted]	[redacted]	Christopher C. Hatin	

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	conditions, all 8(a) STARS II contract clauses are applicable to the resultant task order. The period of performance will be twelve (12) months, which includes a (1) month transition, a two (2) month base, and a nine (9) month option period as follows: Transition: 08/16/2020 - 09/15/2020 Base: 09/16/2020 - 11/15/2020 Option I: 11/16/2020 - 08/15/2021 Due to funding constraints, the Government reserves the right to establish new periods not to exceed the total twelve (12) month life of the task order. Dates for the period of performance will be adjusted upon issuance of the Authority to Work (ATW). No invoicing may occur until after the ATW. AAP Number: 2020049803 Accounting Info: ITNSESV ITP EX 000 20-05-00-000 23-20-0300-00-00-00-00 GE-25-76-00 000000				
0001	Information Services Consultant - Contract Lead and Senior Security Control Assessor (Key Personnel) in accordance with (IAW) Statement of Work (SOW) section 3.2 [redacted] estimated number of labor hours: [redacted] Continued ...	1	MO	[redacted]	[redacted]

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. MA LING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MA L 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 CERTIFY NG 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)
	POP: 1 month (FFP) PSC: D399 Delivery: 1 Days After Authority to Work				
0002	Information Services Consultant - Senior Security Control Assessor IAW SOW section 3.2 [redacted] estimated number of labor hours: [redacted] POP: 1 month (FFP) PSC: D399 Delivery: 1 Days After Authority to Work	1	MO	[redacted]	[redacted]
0003	Information Assurance Development Engineer - Security Control Assessors IAW SOW section 3.2 [redacted] estimated number of labor hours: [redacted] POP: 1 months (FFP) PSC: D399 Delivery: 1 Days After Authority to Work	1	MO	[redacted]	[redacted]
0004	Information Assurance Development Engineer - Classified ISSO (Key Personnel) IAW SOW section 3.3.1 [redacted] estimated number of labor hours: [redacted] POP: 1 month (FFP) PSC: D399 Delivery: 1 Days After Authority to Work	1	MO	[redacted]	[redacted]
0005	Communications Transmission Engineer - COMSEC Engineer IAW SOW section 3.6 [redacted] estimated number of labor hours: [redacted] POP: 1 month (FFP) PSC: D399 Delivery: 1 Days After Authority to Work	1	MO	[redacted]	[redacted]
0006	Information Services Consultant - Contract Lead and Senior Security Control Assessor (Key Personnel) IAW SOW section 3.2 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399	2	MO	[redacted]	[redacted]
0007	Information Services Consultant - Senior Security Continued ...	2	MO	[redacted]	[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Control Assessor IAW SOW section 3.2 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399				
0008	Information Assurance Development Engineer - Security Control Assessors IAW SOW section 3.2 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399	2	MO	[redacted]	[redacted]
0009	Information Assurance Development Engineer - Classified ISSO (Key Personnel) IAW SOW section 3.3.1 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399	2	MO	[redacted]	[redacted]
0010	Data Security Analyst Intermediate - Classified Support IAW SOW section 3.3.2 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399	2	MO	[redacted]	[redacted]
0011	Communications Transmission Engineer - COMSEC Engineer IAW SOW section 3.6 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399	2	MO	[redacted]	[redacted]
0012	Communications Transmission Engineer - TACCOM Engineer IAW SOW section 3.5 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399	2	MO	[redacted]	[redacted]
0013	Technical Writer - Policy Writer (Governance Support) IAW SOW section 3.4 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) Continued ...	2	MO	[redacted]	[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	PSC: D399				
0014	Travel IAW SOW Section 4.8 Not to Exceed (NTE) [redacted] POP: 2 months (FFP)	1	LO	[redacted]	[redacted]
0015	Data Security Analyst Intermediate - Classified Support IAW SOW section 3.3.3 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	2	MO	[redacted]	[redacted]
0016	Technical Writer - Policy Writer IAW SOW section 3.4.1 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	2	MO	[redacted]	[redacted]
0017	Information Services Consultant - Senior Security Control Assessor IAW SOW section 3.2.1 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item) Anticipated Exercise Date:	2	MO	[redacted]	[redacted]
0018	Information Assurance Development Engineer - Security Control Assessors IAW SOW section 3.2.1 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	2	MO	[redacted]	[redacted]
0019	Subject Matter Expert - Level III IAW SOW section 3.1.3.1 [redacted] estimated number of labor hours: [redacted] Continued ...	2	MO	[redacted]	[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	POP: 2 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)				
0020	Training Expert - Level II IAW SOW section 3.1.3.2 [redacted] estimated number of labor hours: [redacted] POP: 2 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	2	MO	[redacted]	[redacted]
1001	Information Services Consultant - Contract Lead and Senior Security Control Assessor (Key Personnel) IAW SOW section 3.2 (Option 1) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1002	Information Services Consultant - Senior Security Control Assessor IAW SOW section 3.2 (Option 1) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1003	Information Assurance Development Engineer - Security Control Assessors IAW SOW section 3.2 (Option 1) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1004	Information Assurance Development Engineer - Classified ISSO (Key Personnel) IAW SOW section 3.3.1 (Option 1) [redacted] estimated number of labor hours: [redacted] Continued ...	9	MO	[redacted]	[redacted]

NAME OF OFFEROR OR CONTRACTOR
SOLUTIONS BY DESIGN II LLC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)				
1005	Data Security Analyst Intermediate - Classified Support IAW SOW section 3.3.2 (Option 1) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1006	Communications Transmission Engineer - COMSEC Engineer IAW SOW section 3.6 (Option 1) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1007	Communications Transmission Engineer - TACCOM Engineer IAW SOW section 3.5 (Option 1) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1008	Technical Writer - Policy Writer (Governance Support) IAW SOW section 3.4 (Option 1) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1009	Travel IAW SOW Section 4.8 (Option 1) Not to Exceed (NTE) [redacted] POP: 9 months (FFP) Amount: [redacted] (Option Line Item)	1	LO	[redacted]	[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1010	Data Security Analyst Intermediate - Classified Support IAW SOW section 3.3.3 (Option 1, Optional CLIN) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1011	Technical Writer - Policy Writer IAW SOW section 3.4.1 (Option 1, Optional CLIN) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1012	Information Services Consultant - Senior Security Control Assessor IAW SOW section 3.2.1 (Option 1, Optional CLIN) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1013	Information Assurance Development Engineer - Security Control Assessors IAW SOW section 3.2.1 (Option 1, Optional CLIN) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]
1014	Subject Matter Expert - Level III IAW SOW section 3.1.3.1 (Option 1, Optional CLIN) [redacted] estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item)	9	MO	[redacted]	[redacted]

NAME OF OFFEROR OR CONTRACTOR
SOLUTIONS BY DESIGN II LLC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1015	Training Expert – Level II IAW SOW section 3.1.3.2 (Option 1, Optional CLIN) [redacted], estimated number of labor hours: [redacted] POP: 9 months (FFP) PSC: D399 Amount: [redacted] (Option Line Item) Part II – Task Order Terms and Conditions Part III – Attachments Attachment I: Statement of Work (SOW) Attachment II: Deliverables The total amount of award: [redacted] The obligation for this award is shown in box 26.	9	MO	[redacted]	[redacted]

PART II – TASK ORDER TERMS & CONDITIONS

THIS ORDER WILL BE SUBJECT TO THE CONTRACTOR'S 8(a) STARS II IDIQ CONTRACT TERMS AND CONDITIONS

FAR CLAUSES INCORPORATED BY REFERENCE

FAR 52.204-18 - Commercial and Government Entity Code Maintenance (Jul 2016)

FAR 52.204-19 - Incorporation by Reference of Representations and Certifications (Dec 2014)

FAR 52.212-4 - Contract Terms and Conditions -- Commercial Items (Oct 2018)

FAR 52.243-1 - Changes – Fixed Price (Aug 1987)

FAR CLAUSES INCORPORATED IN FULL TEXT

FAR 52.204-23 – Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (DEVIATION 2020-05)

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

"Covered article" means any hardware, software, or service that–

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

"Covered entity" means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and
(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement*.

(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA_Incidents@hq.dhs.gov, with required information contained in the body of the email.

In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.204-25 – Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)

(a) Definitions. As used in this clause--

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means--

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means--

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—

i. Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

ii. For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817). Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) Exceptions. This clause does not prohibit contractors from providing--

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

i. Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

ii. Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of Clause)

FAR 52.212-5 – Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items (Mar 2020) (DEVIATION Apr 2020)

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

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(l)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(5) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805note)).

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

_X_ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

_X_ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).

_X_ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

_X_ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Oct 2015) (31 U.S.C. 610lnote).
_X_ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).
_X_ (14) (i) 52.219-6, Notice of Total Small Business Set-Aside (Mar 2020) (15 U.S.C.644).
_X_ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).
_X_ (22) (i) 52.219-28, Post Award Small Business Program Representation (Mar 2020) (15 U.S.C. 632(a)(2)).
_X_ (27) 52.222-3, Convict Labor (June 2003) (E.O.11755).
_X_ (31) (i) 52.222-35, Equal Opportunity for Veterans (Oct 2015)(38 U.S.C. 4212).
_X_ (32) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C.793).
_X_ (33) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
_X_ (35) (i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
_X_ (36) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
_X_ (57) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct 2018) (31 U.S.C. 3332).
_X_ (60) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (DEC 20l3) (DEVIATION APR 2020)(31 U.S.C. 3903 and 10 U.S.C. 2307).
_X_ (61) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:
_X_ (1) 52.222-17, Non-displacement of Qualified Workers (May 2014)(E.O. 13495).
_X_ (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
_X_ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
_X_ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
_X_ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).
_X_ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).

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

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.
(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the dispute's

clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

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

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(l)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C.637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-17, Non-displacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(vii) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(viii) 52.222-26, Equal Opportunity (Sept 2015) (E.O.11246).

(ix) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C.4212).

(x) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C.793).

(xi) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C.4212)

(xii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 20 l 0) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xiii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

(xiv) (A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O 13627).

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

(End of clause)

FAR 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 **15 days***;* provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **30 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 **12 months.**

(End of Clause)

FAR 52.224-3 - Privacy Training *Alternate I (Jan 2017)*

(a) Definition. As used in this clause, "personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will--

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

FAR 52.252-2 - Clauses Incorporated by Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of the clause may be accessed electronically at these addresses: http://www.acquisition.gov/far.

(End of Clause)

HSAR CLAUSES INCORPORATED BY REFERENCE

HSAR 3052.203-70 – Instructions for Contractor Disclosure of Violations (Sep 2012)

HSAR 3052.205-70 – Advertisements, Publicizing Awards, and Releases (Sep 2012)

HSAR 3052.242-72 – Contracting Officer's Technical Representative (Dec 2003)

HSAR CLAUSES INCORPORATED IN FULL TEXT

HSAR 3052.204-70 - Security Requirements for Unclassified Information Technology Resources (Jun 2006)

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

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

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

HSAR 3052.204-71 - Contractor Employee Access Alternate I (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.

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

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

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

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

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

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

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

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

(End of Clause)

HSAR 3052.209-70 – Prohibition on Contracts with Corporate Expatriates (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that

section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) Certain stock disregarded. For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) Plan deemed in certain cases. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) Certain transfers disregarded. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) Special rule for related partnerships. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:
(i) warrants;
(ii) options;
(iii) contracts to acquire stock;
(iv) convertible debt instruments; and
(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) Disclosure. The offeror under this solicitation represents that [Check one]:

X it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of clause)

HSAR 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:

- Information Services Consultant - Contract Lead and Senior Security Control Assessor (1 FTEs)
- Information Assurance Development Engineer - Classified ISSO (1 FTEs)

(End of Clause)

HSAR CLASS DEVIATION 15-01 SPECIAL CLAUSES IN FULL TEXT

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.

   a. 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.

   b. 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 Attachment 6 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 email notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of Clause)

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

(b) Definitions. As used in this clause—

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

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

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law

107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

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

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

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

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

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

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

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

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.
(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.
(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit

sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

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

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

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

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

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

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:

Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

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

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

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the

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

(f) Sensitive Information Incident Reporting Requirements.

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

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

i. Data Universal Numbering System (DUNS);
ii. Contract numbers affected unless all contracts by the company are affected;
iii. Facility CAGE code if the location of the event is different than the prime contractor location;
iv. Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
v. Contracting Officer POC (address, telephone, email);
vi. Contract clearance level;
vii. Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
viii. Government programs, platforms or systems involved;
ix. Location(s) of incident;
x. Date and time the incident was discovered;
xi. Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
xii. Description of the Government PII and/or SPII contained within the system;
xiii. Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

xiv. Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

i. A dedicated telephone number to contact customer service within a fixed period;
ii. Information necessary for registrants/enrollees to access credit reports and credit scores;
iii. Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
iv. Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
v. Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
vi. Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

(End of Clause)

USCIS LOCAL CLAUSES INCORPORATED BY FULL TEXT

A. SECURITY REQUIREMENTS (Security Clause 2TS)

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Counterintelligence and Security Agency.

Any firm or business under contract with the Department of Homeland Security (DHS), which requires access to classified information, will require a Facility Security Clearance (FCL)

commensurate with the level of access required. Firms that do not possess a FCL, or the requisite level FCL, will be sponsored by DHS to obtain one.

FITNESS DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment Fitness authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment Fitness determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or Fitness determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information and/or classified information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the DHS Form 11000-25, Contractor Fitness/Security Screening Request Form and the USCIS Continuation Page to the DHS Form 11000-25. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, Security Questionnaire for Public Trust Positions via e-QIP:

1. DHS Form 11000-6, Conditional Access to Sensitive But Unclassified Information Non- Disclosure Agreement
2. FD Form 258, Fingerprint Card (2 cards)
3. DHS Form 11000-25, Contractor Fitness/Security Screening Request Form
4. USCIS Continuation Page to DHS Form 11000-25
5. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
6. Foreign National Relatives or Associates Statement

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information and/or classified information has resided in the U.S. for three of the past five years, OSI PSD

may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

VISIT AUTHORIZATION LETTER (VAL)

The Contractor is required to submit a VAL for those individuals who require access to classified information during performance on this contract and who have an active Personnel Security Clearance (PCL). The letter will be valid for a period not to exceed one year. If the requirement to access classified information no longer exists, or if access eligibility changes, OSI PSD will be notified immediately. The VAL must be submitted to OSI PSD in accordance with, and contain information as required by, Chapter 6 of the NISPOM.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract. In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (annually)
- **DHS Insider Threat Training** (annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure** Training (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS PKI Initiative Training** (if supervisor determines the need for a PKI certificate)

- **Computer Security Awareness Training** (if contractor requires access to USCIS IT systems, training must be completed within 60 days of entry on duty for new contractors, and annually thereafter)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire or on any security form listed above.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) http://www.dhs.gov/homeland-security-presidential-directive-12 contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity Verification (PIV) card throughout the period of performance on their contract.

Government-owned contractor- operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [10 business days unless a different number is inserted] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [10 business days unless a different number of days is inserted] from the date this clause is incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:

http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx

Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing out so that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft

http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Facility Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the Secret level, a Government employee or Contractor with the appropriate security clearance equal to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to their supervisor and then to the designated OSI Local Security Officer or OSI Field Security Manager for action as appropriate.

Subpart 4.4—Safeguarding Classified Information Within Industry

4.402 General.

(a) Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), entitled "National Industrial Security Program" (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829 amends Executive Order 10865, February 20, 1960

(25 FR 1583, February 25, 1960), entitled "Safeguarding Classified Information Within Industry," as amended by Executive Order 10909, January 17, 1961 (26 FR 508, January 20, 1961).

(b) The National Industrial Security Program Operating Manual (NISPOM) incorporates the requirements of these Executive orders. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence, is responsible for issuance and maintenance of this Manual. The following DoD publications implement the program:

(1) National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).

(2) Industrial Security Regulation (ISR) (DoD 5220.22-R).

(c) Procedures for the protection of information relating to foreign classified contracts awarded to U.S. industry, and instructions for the protection of U.S. information relating to classified contracts awarded to foreign firms, are prescribed in Chapter 10 of the NISPOM.

(d) Part 27—Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

4.403 Responsibilities of Contracting Officers.

(a) *Pre-solicitation phase*. Contracting officers shall review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor during contract performance.

(1) If access to classified information of another agency may be required, the contracting officer shall—

(i) Determine if the agency is covered by the NISP; and

(ii) Follow that agency's procedures for determining the security clearances of firms to be solicited.

(2) If the classified information required is from the contracting officer's agency, the contracting officer shall follow agency procedures.

(b) *Solicitation phase*. Contracting officers shall—

(1) Ensure that the classified acquisition is conducted as required by the NISP or agency procedures, as appropriate; and

(2) Include—

(i) An appropriate Security Requirements clause in the solicitation (see 4.404); and

(ii) As appropriate, in solicitations and contracts when the contract may require access to classified information, a requirement for security safeguards in addition to those provided in the clause (52.204-2, Security Requirements).

(c) *Award phase*. Contracting officers shall inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract as follows:

(1) Agencies covered by the NISP shall use the Contract Security Classification Specification, DD Form 254. The contracting officer, or authorized representative, is the approving official for the form and shall ensure that it is prepared and distributed in accordance with the ISR.

(2) Contracting officers in agencies not covered by the NISP shall follow agency procedures.

4.404 Contract clause.

(a) The contracting officer shall insert the clause at 52.204-2, Security Requirements, in solicitations and contracts when the contract may require access to classified information, unless the conditions specified in paragraph (d) of this section apply.

(b) If a cost contract (see 16.302) for research and development with an educational institution is contemplated, the contracting officer shall use the clause with its Alternate I.

(c) If a construction or architect-engineer contract where employee identification is required for security reasons is contemplated, the contracting officer shall use the clause with its Alternate II. (d) If the contracting agency is not covered by the NISP and has prescribed a

clause and alternates that are substantially the same as those at 52.204-2, the contracting officer shall use the agency- prescribed clause as required by agency procedures.

52.204-2 Security Clause Requirements.

As prescribed in 4.404(a), insert the following clause: Security Requirements (Aug 1996)

(a) This clause applies to the extent that this contract involves access to information classified "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)

Alternate I (Apr 1984). If a cost contract for research and development with an educational institution is contemplated, add the following paragraphs (e), (f), and (g) to the basic clause:

(e) If a change in security requirements, as provided in paragraphs (b) and (c), results (1) in a change in the security classification of this contract or any of its elements from an unclassified status or a lower classification to a higher classification, or (2) in more restrictive area controls than previously required, the Contractor shall exert every reasonable effort compatible with the Contractor's established policies to continue the performance of work under the contract in compliance with the change in security classification or requirements. If, despite reasonable efforts, the Contractor determines that the continuation of work under this contract is not practicable because of the change in security classification or requirements, the Contractor shall notify the Contracting Officer in writing. Until resolution of the problem is made by the Contracting Officer, the Contractor shall continue safeguarding all classified material as required by this contract.

(f) After receiving the written notification, the Contracting Officer shall explore the circumstances surrounding the proposed change in security classification or requirements, and shall endeavor to work out a mutually satisfactory method whereby the Contractor can continue performance of the work under this contract.

(g) If, 15 days after receipt by the Contracting Officer of the notification of the Contractor's stated inability to proceed, (1) the application to this contract of the change in security classification or requirements has not been withdrawn, or (2) a mutually satisfactory method for continuing performance of work under this contract has not been agreed upon, the Contractor may request the Contracting Officer to terminate the contract in whole or in

part. The Contracting Officer shall terminate the contract in whole or in part, as may be appropriate, and the termination shall be deemed a termination under the terms of the Termination for the Convenience of the Government clause.

Alternate II (Apr 1984). If employee identification is required for security or other reasons in a construction contract or architect-engineer contract, add the following paragraph (e) to the basic clause:

(e) The Contractor shall be responsible for furnishing to each employee and for requiring each employee engaged on the work to display such identification as may be approved and directed by the Contracting Officer. All prescribed identification shall immediately be delivered to the Contracting Officer, for cancellation upon the release of any employee. When required by the Contracting Officer, the Contractor shall obtain and submit fingerprints of all persons employed or to be employed on the project.

B. ADDITIONAL INFORMATION

INVOICE REQUIREMENTS

(a) In accordance with FAR Part 52.212-4(g), all invoices submitted to USCIS for payment shall include the following:

(1) Name and address of the contractor.

(2) Invoice date and invoice number.

(3) Contract number and other authorization for supplies delivered or services performed (including order number and contract line item number).

(4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.

(5) Shipping and payment terms.

(6) Name and address of contractor official to whom payment is to be sent.

(7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.

(8) Taxpayer Identification Number (TIN).

(b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.

(c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically using the "To" line in the e-mail address to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.

(d) If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

POSTING OF CONTRACT (OR ORDER) IN FOIA READING ROOM

(a) The Government intends to post the contract (or order) resulting from this solicitation to a public FOIA reading room.
(b) Within 30 days of award, the Contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The Contractor shall submit the documents to the USCIS FOIA Office by email at **foiaerr.nrc@uscis.dhs.gov** with a courtesy copy to the contracting officer.
(c) The USCIS FOIA Office will notify the contractor of any disagreements with the Contractor's redactions before public posting of the contract or order in a public FOIA reading room.

EXPECTATION OF CONTRACTOR PERSONNEL

The government expects competent, productive, qualified IT professionals to be assigned to the Task Order. The Contracting Officer may, by written notice to the contractor, require the contractor to remove any employee that is not found to be competent, productive, or qualified IT professional.

FINAL PAYMENT

As a condition precedent to final payment, a release discharging the Government, its officers, agents and employees of and from all liabilities, obligations, and claims arising out or under this contract shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion as soon thereafter as practicable.

KEY PERSONNEL

For the purposes of the contract clause at HSAR 3052.215-70, Key Personnel or Facilities, the Key Personnel are listed in Section 4.3.1 in the Statement of Work (SOW). All personnel submitted by a contractor to fill a key person billet shall meet required standards per Section 4.3.1 of the SOW**.**

GOVERNMENT FURNISHED PROPERTY (GFP)

Twenty (20) GFP laptops (Dell Latitude 5490 or compatible device) with power cords and twenty (20) PIV cards will be issued as-is in performing work on this contract; the quantity is reflective of the entire task order to include optional CLINS. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) will be used with the GFP. A webinar account will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations.

The Government has the right to implement Workplace as a Service (WPaaS) in lieu of providing GFP or as a replacement for existing GFP at its discretion during the life of the contract.

The Government will not be obligated to provide additional accessories for the laptop computers, such as monitors, computer bags, external mice, etc. The Contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation, or rehabilitation costs. The Contractor will be responsible for receipt, stewardship, and custody of the listed GFP until formally relieved of responsibility in

accordance with FAR 52.245-1 *Government Property* and FAR 52.245-9 *Use and Charges*. The property may not be used for any non-task order purpose. The Contractor bears full responsibility for any and all loss of this property, whether accidental or purposeful, at full replacement value.

AUTHORITY TO WORK (ATW)

(a) Performance of the work requires access to classified National Security Information (NSI) - Top Secret/SCI, Sensitive but Unclassified (SBU) information as well as USCIS computer systems. Section A. SECURITY REQUIREMENTS (Security Clause 2TS) applies.
(b) The contractor is responsible for submitting packages from employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such decision or termination, shall not excuse the contractor from performance of obligations under this task order.
(c) The contractor may submit background investigation packages immediately following task order award.
(d) This task order does not provide for direct payment to the contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the contractor.
(e) The government intends for full performance to begin 30 days after task order award (allowing 30 days for the EOD and transition period). All personnel must have received a favorable EOD prior to issuance of the ATW. The contracting officer will issue an ATW at least one day before full performance is to begin.

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

Statement of Work

Office of Information Technology

Security Governance Branch (SGB)

Governance Communications Assessments & Classified Services (G-CACS)

CONTENTS

1 MISSION

1.1 USCIS MISSION

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is responsible for lawful immigration to the United States. USCIS administers the nation's lawful immigration, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.

The USCIS Office of Information Technology (OIT) provides information technology (IT), expertise, and the strategic vision necessary to enable USCIS to deliver effective, efficient, and secure immigration services and products. OIT leads USCIS in the design, development, delivery, and deployment of IT services and solutions that are transforming the nation's immigration system.

1.2 INFORMATION SECURITY DIVISION MISSION

The Office of Management and Budget (OMB) Circular A-130 and the Federal Information Security Modernization Act of 2014 (FISMA) require federal agencies to develop, document and implement an Agency-wide information security programs. USCIS has an immediate need to strengthen the underlying foundation of our Cyber Security and Risk Management Programs. USCIS's cyber security program, managed by the OIT, Information Security Division (ISD) under the guidance of the Chief Information Security Officer (CISO) must be strengthened, enhanced and expanded, consistent with best practices outlined in the National Institute of Science and Technology (NIST) Risk Management and Cybersecurity Frameworks, to improve the agency's Risk Management capabilities.

USCIS ISD, under the direction of the USCIS CISO, is responsible for the management and strategic leadership of the USCIS Cyber Security Programs, providing agency-level cyber and information security oversight, governance, and compliance to ensure that USCIS IT infrastructure and information systems are properly secured to protect the confidentiality, integrity and availability of the information that is stored, transmitted and processed in support of the agency's mission.

The Security Governance Branch (SGB) is responsible for providing security management oversight, governance, training, and compliance to ensure that the USCIS IT infrastructure and information systems, both at the classified and unclassified levels, are properly secured while protecting the confidentiality, integrity, and availability of information that is stored,

processed, and transmitted, in USCIS information systems, which include tactical and security communications devices. SGB will provide management and strategic leadership of the USCIS Security Governance Program, consistent with FISMA and the NIST Cyber Security Frameworks, and in alignment with each of the five ISD Strategic goals:

- Goal 1 - Elevate the Cybersecurity Posture: Safeguard the USCIS infrastructure, systems, and data by evaluating, elevating and strengthening our cybersecurity posture
- Goal 2 – Intelligence, Hunting, Monitoring and Response: Enhance USCIS's monitoring programs and capabilities to proactively prevent, detect, and respond and recover from advanced cyber threats
- Goal 3 - Standardization and Automation: Implement innovative and automated solutions to enhance cybersecurity architecture, controls, tools and measures of effectiveness
- Goal 4 – Training and Awareness: Empower ownership of cybersecurity responsibilities through improved awareness and understanding of cybersecurity compliance, threats, and impacts
- Goal 5 - Oversight and Governance: Enhance organizational efficiency, effectiveness and unity of effort to achieve mission requirements

The SGB Governance, Communication, Assessments, and Classified Services (GCACS) will be responsible for Communications Security (COMSEC), Tactical Communications (TACCOM) Engineering and Implementation Services, Classified Systems and Sensitive Compartmented Information Facility (SCIF) Support, Security Authorization Services, Governance document creation, review, and Program Management with Training support for the Office of Information Technology and the USCIS Enterprise.

The SGB's primary responsibilities are ensuring the confidentiality, integrity, and availability of the information stored, processed, and transmitted in support of the Agency's mission by:

- Establishing, implementing, and maintaining IT Security policies and procedures;
- Providing overall management of Communications Security (COMSEC) assets within USCIS;
- Providing COMSEC training to USCIS users;
- Providing technical support and Subject Matter Expertise for the USCIS Tactical Communications (TACCOM) needs throughout the enterprise:
- Reviewing, revising, and drafting IT Security governance documents:
- Providing Information System Security Officers (ISSO) and desktop support for USCIS Sensitive Compartmented Information Facilities (SCIF):

- Providing oversite and coordination for USCIS classified networks and Homeland Security Data Network (HSDN) installations.
- Assessing, documenting and evaluating IT security controls in a wide range of environments.
- Ensuring all USCIS personnel are appropriately trained on their IT security roles and responsibilities.
- Providing Executive Program Management support services

1.3 OBJECTIVES

The objective of this Statement of Work (SOW) is to obtain professional services for the USCIS-OIT-ISD Security Governance Branch (SGB). A successful contract constitutes the delivery of the following objectives:

- Assess and optimize existing SGB services/functions consistent with the NIST Risk Management and Cyber Security Frameworks;
- Establish qualitative and quantitative performance metrics to monitor the performance of each functional area;
- Automate reporting mechanisms by creating new (or leveraging existing) USCIS tools and processes, as well as industry best practice techniques;
- Develop and implement innovative technology, streamlined capabilities and processes that strengthen, enhance and improve the functional areas identified in this SOW;
- Provide Program Management Oversight (PMO) support services for the Security Governance Branch. The PMO will effectively manage the staffing, technical capacity, capability, and appropriate plans to deliver GCACS tasks and services on schedule and within budget.

1.4 SCOPE

This task order will be the primary vehicle to obtain professional services to achieve the objectives stated above for the requirements for the USCIS/OIT/ISD GCACS. It provides a description of the services sought to assess the current state of each functional area of the Security Governance Branch, and establish new, robust, innovative and proactive solutions and dynamic agile capabilities to refresh and optimize each functional area.

The Security Governance Branch is comprised of the following functional areas for this contract:

- Program Management
- Enterprise Security Control Assessment (SCA) Support

- Classified Systems and SCIF Support
- Governance Support
- Tactical Communications (TACCOM) Support
- Communications Security (COMSEC) Support

The GCACS will also provide Strategic Operations services, including program planning, management, communications, operations and training support services to ISD and all of its branches.

USCIS is seeking a contractor to provide results-oriented, agile security services that provide the functions and activities necessary for the ISD/SGB to effectively and efficiently implement and manage its functional areas to successfully achieve its mission.

This enhanced program management approach will provide the organization with the structure and discipline required to help manage SGB operations and ensure its success, with a focus on improved capabilities, improved outcomes, process improvement, and technology development and integration, information management, results management, and performance management.

2 CURRENT STATE

2.1 METHODOLOGY

The Contractor shall be subject to all current and future versions of DHS Sensitive Systems Policy Directive 4300A, DHS National Security Systems Policy 4300B, DHS Sensitive Compartmented Information (SCI) Instruction Manual 4300C, the annual DHS Information Security Performance Plan, National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series, Federal Information Processing Standards (FIPS) and all associated USCIS policies including all associated attachments, concepts of operation (CONOPS), processes and standard operating procedures. Documents which are not publicly available will be provided to the selectee upon contract award.

All efforts described above shall be conducted in accordance with established Federal statutory requirements (e.g. 1996 Federal Clinger-Cohen Act (CCA), Section 508 of the 1998 Federal Rehabilitation Act, FISMA), departmental regulatory guidelines (e.g. DHS Acquisition Management Directive 102-1, USCIS Systems Engineering Life Cycle (SELC) guide), and through use of the industry's best practices for Information Technology Security Authorization activities.

2.2 CURRENT OPERATIONS

Current SGB operations are spread across six different task areas. Each task area presents its own set of challenges and opportunities. Currently there are two separate contracts providing support to SGB operations which limits synergy and effectiveness of a cohesive mission. Moreover, the previous contracts did not provide support for COMSEC and Governance services. Additionally, this contract will have the capability to obtain professional, experienced contract personnel to coordinate strategic operations, performance optimization and management support services for ISD and its branches that will result in an integrated strategy.

Many of the current tasks supporting the SGB functional areas require manual data entry and analysis. USCIS has many security tools for performing security assessments from which data are compiled and analyzed to determine the security posture of systems and programs, and the related risks for the Agency. Manual review of test results can impact other branch and program methodologies and timelines with their USCIS Continuous Monitoring (CM) efforts. The SGB SCA and Governance team works in cooperation with the Risk Management Branch (RMB) and Security Engineering Branch to ensure the continuous monitoring process of USCIS systems and policies are not negatively impacted.

The COMSEC program supports the USCIS enterprise and is managed in compliance with the DHS Central Office of Record (COR) requirements. At a minimum, COMSEC requires a two-person validation operation to manage the program which currently we are understaffed to support.

The TACCOM program provides technical expertise to the USCIS enterprise in developing and maintain a telecommunications capability. This includes providing operator training, developing governance documents, programing frequencies, Crypto key management, site surveys and equipment maintenance at USCIS facilities.

While USCIS SGB is seeking results oriented agile security services as described in Section 1.4: Scope, the contractor must maintain current operations for all functional areas. Refer to Sections 3.1 – 3.3 for related tasks.

3 TASKS

The Contractor shall execute the requirements of this SOW through the following tasks:

3.1 PROGRAM MANAGEMENT AND CONTINUOUS PROCESS IMPROVEMENT (CPI)

3.1.1 PROGRAM MANAGEMENT

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff, provide Program Management support for planning, execution, and completion of all project activities in accordance with best project management practices. While USCIS will provide management oversight, it is the responsibility of the Contractor to manage all corporate resources and supervise all Contractor staff in the performance of all work on this Task Order. The Contractor shall assign a Project Manager to this task who will manage the day-to-day activities of the Contractor staff.

The Contractor shall ensure the project is staffed with an adequate number of assigned personnel possessing the required certifications, qualifications, skills, and experience. The Project Manager shall organize, direct, and coordinate the planning and execution of all activities, review the work of subordinates, including subcontractors, and ensure that the schedule, performance parameters, and reporting responsibilities are met. The Project Manager shall integrate the Contractor's management and technical activities across this Task Order to ensure they are consistent. The Government has the right to reprioritize workloads to support mission needs, as necessary.

The Government will provide a tool such as (JIRA/Confluence/LeanKit) for managing tasks, activities and deliverables in support of this Task Order. The Program Manager or designee is responsible for managing tasks, activities and deliverables, and providing status reports, as requested by the Government.

The Contractor's Project Manager shall be the primary interface with the Government Program Manager or designee. Attendance at weekly status meetings and ad hoc meetings is required.

Independently of the number and size of subcontractors the prime Contractor partners with, the Contractor shall present a united team to the Government.

The contractor shall provide Program Planning documentation as described in Attachment II – Deliverables. Additionally, at the request of the COR, the Government Program

Manager, or a Government Project Manager, the Contractor shall be required to prepare briefing materials, deliver briefings, participate in meetings with USCIS organizations and/or external organizations, and present program content. The Contractor may be required to schedule/ plan meetings as requested by the Government. The Contractor shall develop, as necessary, written recommendations, oral presentations and/or executive briefing materials.

The following meetings are mandatory for the Contractor to attend:

- Task Order Kick-Off meeting;
- Daily Stand Ups;
- Weekly status meeting with Government staff. The Contractor PM and project leads shall participate in person at the location designated by the Government and may be required to schedule the meeting upon request;
- Monthly Program Management Reviews (PMR); and
- Other ad-hoc meetings scheduled by USCIS senior leadership or the Government team.

The Contractor will be required to interact with multiple other contractor teams. The Government expects full Contractor cooperation, proper meeting attendance, and coordination to accomplish joint work.

3.1.2 PROGRAM MANAGEMENT OVERSIGHT (PMO)

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

- Provide Program Management Oversight (PMO) support services for the Security Controls Assessment, TACCOM, COMSEC, Governance, and Classified Systems & SCIF Support Programs under the Security Governance Branch. PMO will effectively manage the staffing, technical capacity, capability, and appropriate plans to deliver GCACS tasks and services on schedule and within budget.
    - Perform oversight and management of all GCACS contract activities, including: on-boarding, terminations, deliverables, and management of resources, contract performance and cost;
    - Serve as the Government's single point of contact for all GCACS contract actions, questions, and recommendations;
    - Identify and resolve issues and risks that could adversely impact performance, costs and/or delivery schedule;
    - Conduct quarterly gap analyses for each functional area; recommend areas for improvement to the government;

  - Prepare a Quality Management Plan detailing hoe it intends to manage and assess the quality of task performance, to include; what methods are used to validate that the quality control efforts are timely, effective, and delivering the results specified in the SOW;
  - Establish and maintain a process, using agile methodologies, for managing work processes/products and reporting; and
  - Prepare weekly status reports and briefings including metrics for management review showing functionality of services, GCACS staffing plans and value added to the organization.
- Provide ongoing support focused on continuously improving, automating, streamlining, optimizing and enhancing processes and operations resulting in improved organizational efficiency, effectiveness and productivity of the Security Governance Branch and its functional areas.
- Assist the SGB in assessing, obtaining, integrating, and fully leveraging the right technology and implementing solutions to solve business challenges, improve business processes through automation, and support the collection and recording of technical information, as well as a focus on strategic outcomes, results, and key performance indicators
- Develop and implement a communication strategy to inform and collaborate with internal and external stakeholders on cyber risks by:
  - Developing and establishing a stakeholder/customer engagement model for each SGB functional area to inform internal (USCIS) and external customers on how to engage with SGB teams and comply with federally mandated DHS' Information Security Program policies, procedures, standards, and guidelines;
  - Developing processes, procedures including documenting SOPs for each functional area;
  - Drafting communications and notifications as directed to keep stakeholders/customers informed when there are changes to any of the Risk Management functional areas; and
  - Establishing and maintaining a Document/ Knowledge Management Repository for:
    - SCA Related Documents,
    - Governance Related Documents,
    - Frequently Asked Questions (FAQs), and
    - Other documents and procedures, as directed.
- Perform other duties as assigned by the government.

3.1.3 ISD STRATEGIC OPERATIONS SUPPORT (OPTIONAL CLIN)

The objective of this CLIN is to obtain professional, experienced contract personnel to coordinate strategic operations, performance optimization and management support services for ISD and its branches that will result in an integrated strategy, governance, management, communications and security training processes to better identify and execute key priorities and help communicate a clear vision and path forward for the ISD workforce and its many stakeholders and customers. The contractor shall provide support in the following areas: strategy and governance, mission integration, continuous process improvement and automation, performance measurement, monitoring and reporting, stakeholder engagement, communications and marketing, knowledge management, policy development, Standard Operating Procedures (SOP) development and management, and learning and training.

3.1.3.1 PROGRAM MANAGEMENT SUPPORT – SUBJECT MATTER EXPERT

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

- Provide a standard, scalable, and repeatable approach to strategic program management and mission alignment and integration, including a sound governance and engagement process to manage ISD programs and to coordinate with internal and external employees and stakeholders.
- Assist ISD in establishing and implementing its strategic vision and identifying meaningful outcomes and objectives that are clearly defined and measured, and aligned with OIT, USCIS and DHS goals and objectives.
- Provide SOPs to better inform ISD employees and customers on how to engage with ISD and comply with federally mandated DHS' Information Security Program policies, procedures, standards, and guidelines;
- Learning, training and knowledge management services to develop, deliver, track and memorialize information security education and training efforts to ensure the dissemination and enforcement of policies, practices, and procedures as required and mandated by USCIS, DHS, NIST and FISMA.
- Communications and marketing services to better inform and collaborate with ISD stakeholders;

- Support focused on continuously improving, automating, streamlining, optimizing and enhancing processes and operations resulting in improved organizational efficiency, effectiveness, productivity and measures to enhance the ISD and USCIS mission.
- Program and project management support to enhance ISD execution effectiveness
- The contractor shall possess knowledge and experience working with Agile programs.
- The contractor shall have the requisite project management experience to successfully administer, organize, direct, coordinate, plan, and perform work activities, supervise and review the work of subordinates, including subcontractors, to ensure that all contract requirements are met.
- Project Managers shall successfully provide program and project management support for: risk management, integrated schedule management, performance metrics, document management, and change management.
- Shall support the facilitation of effective governance, cross-project integration, performance monitoring and the implementation of Agile security processes

3.1.3.2 PROGRAM MANAGEMENT – TRAINING SUPPORT

The Information Security Training Program is charged with developing, delivering, and tracking information security education and training efforts across organization for the general user population (Federal Employees, Contractors, and Interns) as well as for Information Security Professionals. The program ensures the enforcement of policies, practices, and procedures as required and mandated by USCIS, DHS, OPM, NIST, and FISMA. The program is intended to integrate with enterprise solutions and programs in order to improve business processes. The program supports effective communication throughout the organization with information security related initiatives and guidance.

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

- Provide learning, training and knowledge management services to develop, deliver, track and memorialize information security education and training efforts to ensure the dissemination and enforcement of policies, practices, and procedures as required and mandated by USCIS, DHS, NIST and FISMA.

- Develop, facilitate, assist and provide continuous support for the Information Security Training Program to include but not limited to ad-hoc training activities as it applies to various training topics, skill-levels, and audiences as defined and directed by the Government.
- Provide knowledgeable Information Security focused trainers to develop and deliver training content and material as requested by the Government.
- Develop and deliver Section 508 compliant static and active/animated course curriculum using a variety of common off-the-shelf training development tools.
- Develop and deliver specialized training products for high level officials as requested.
- Assist with the development of tips, training, and guidance as it relates to Cyber Security Awareness initiatives across the organization.
- Assist with the development of broadcast messages and agency-wide communications in support of the Cyber Security Awareness initiatives and Information Security Training program.
- Read, follow, and reference applicable USCIS and DHS policies, procedures, and guidelines such as but not limited to DHS 4300A Sensitive Systems Policy/Handbook and Attachment G.
- Develop, manage, and maintain all training documents, briefings, trackers, policies, and SOPs related to Information Security Training or as requested by the Government.
- Participate in working groups such as the DHS Information Security Training Working Group and USCIS Training Facilitator's Working Group.
- Coordinate and engage with other entities across the organization as required to facilitate solutions and resolve training related issues.
- Manage, maintain, and track all assigned tasks and duties related to Information Security Training.
- Escalate all outstanding or unresolved issues, questions or concerns to the Program Manager (PM) and the Government
- Provide continuous support for the Computer Security Awareness Training (CSAT) program as directed and required by the government.
- Review, revise, develop, and maintain CSAT content and exam materials IAW current policies, procedures, and standards (currently provided in ECN and PALMS).
- Manage, maintain, and create CSAT tracking processes, procedures, reports, and surveys.

- Manage and maintain the CSAT Mailbox and respond to customer inquiries with 24-48 hours during the work week.
- Work closely with the Help Desk and HCT/PALMS support teams to resolve customer issues.
- Work closely with HCT/PALMS support teams to develop, manage, and maintain CSAT course material, training records, and reports.
- Manage and maintain the CSAT program for new employee onboarding to include grading exams, tracking progress, and updating training records in PALMS.
- Monitor, track, and report non-compliant users to the Government for account disablement (24-hour initial requirement for new users and 365-day refresher training requirement for current users).
- Develop and maintain an alternative process to track CSAT compliance for users that have completed CSAT outside of USCIS (i.e. DoD or DoS CSAT courses).
- Develop and maintain an alternative/backup CSAT program in the event the primary CSAT program is not available.
- Participate and assist with the development of new and up-to-date CSAT programs and initiatives.
- Support the daily CSAT program by managing and responding to various inquires activities and correspondence
- Provide continuous support for the Role-Based Training Program (i.e. Privileged User Training) as directed and required by the government.
- Review, revise, develop, and maintain all Role-Based Training IAW current policies, procedures, and standards (currently provided in ECN and PALMS).
- Ensure all Role-Based training is available and appropriately assigned in PALMS.
- Manage and maintain a current and accurate list of Privileged Users based on approved G1186 forms and notification reports from AMB/ICAM.
- Manage and maintain the INFOSEC Mailbox and respond to customer inquiries with 24-48 hours during the work week.
- Track and ensure Privileged Users are complaint with annual training requirements.

3.2 SECURITY CONTROL ASSESSMENT SUPPORT

This task supports all Risk Management Framework (RMF) activities as outlined in the NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. This includes the process for managing security and privacy risk, including assessing the information security categorization; control selection, implementation, system and common control authorizations, and continuous monitoring.

Further, this task supports the security activities associated with evaluating, implementing, managing security practices and continued operations of new and existing technologies across the USCIS OIT Enterprise. The Contractor shall provide oversight into all system related security responsibilities as required. The Contractor shall support both USCIS Sensitive but Unclassified (SBU) and For Official Use Only (FOUO) systems. The Contractor shall perform all duties and responsibilities in accordance with DHS Sensitive Systems Policy Directive 4300A, DHS National Security Systems Policy 4300B, NIST 800-53/800-53A, and other applicable guidance.

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

- Risk Management Framework (RMF) Activities: Support all activities as outlined in the NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. This includes the process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.
- Provide the subject matter expertise to support the capability to assess individual systems simultaneously per federal government schedule. Each assessment will be complete within a period of 10 - 15 business days based on the complexity of the system, unless it is not realistic and the government has agreed to an extended period of time. The contractor shall submit written request for an extension within 3 business days upon assignment.
- Provide the subject matter expertise and proficiency using tools for security assessments, including but not limited to Nessus, WebInspect, DB Protect, Fortify, Appscan, Information Assurance Compliance System (IACS), RSA Archer, Nipper, Burp Suite Pro, WebSphere, ActiveState Perl, Aquafold, SoapUI Pro, Ultraedit, SNSScan, SolarWinds Engineer's Toolset, Fortify and/or other as required.
- Develop and provide all documentation necessary for performing a Security Control Assessment, to include but not limited to the following:
    - Security Control Assessment Plan (SCAP) or Security Assessment Plan (SAP)

  - The SCAP/SAP shall provide the objectives and scope for the security control assessment and a detailed roadmap of how the testing assessment shall be conducted.
  - The SCAP/SAP shall also identify security risks and threat vulnerabilities across all facets of the enterprise systems and connection points that are within the defined system authorization boundary.
    - System Access Requests
    - Plan of Actions & Milestones (POA&Ms)
    - Security Assessment Report (SAR)
    - Authorization Letters (Approval to Operate (ATO), Approval to Connect (ATC), Approval to Use (ATU), Interim Authority to Test (IATT), Authority to Proceed (ATP), and any other authorization documentation)
    - Requirement Technical Results – these results will include exact findings per IP Address. The government will provide guidance and a template to utilize.
    - Security Control Traceability Matrix (SCTM)/ Requirements Traceability Matrix (RTM)
- Other ad hoc system specific documentation as specified by the government
- Ensure that system access required for testing is acquired at least 30 days prior to Security Assessment start date and remains for at least 6 months post-assessment to accommodate any additional follow-on testing.
- Be proficient at testing, analyzing and interpreting Security Assessment Results for all systems, including but not limited to the following platforms:
  - Microsoft Server 2012/2016/Other
  - Windows Workstation Platforms
  - Microsoft SQL Server Platforms
  - Oracle DBs
  - Solaris / AIX / UNIX / Linux/ CentOS
  - Pervasive DB
  - Mobile Devices
  - Mainframes
  - Routers/Switches/Firewalls
  - Printers/Faxes/Multi-Function Devices
  - Cold fusion / PHP / ASP
  - Websphere / JAVA
  - Cloud Service Providers (CSPs)
    - IaaS (Infrastructure as a Service)
    - SaaS (Software as a Service)
    - PaaS (Platform as a Service)
- Conduct Security Control Assessments for each USCIS system as part of the Security Authorization Process; for each new system and for systems with expiring ATOs or when required by the Federal Government. In addition, SCAs will be

conducted as required for systems entering into the Ongoing Authorization (OA) program or for systems currently in the OA Program based on the system's Control Allocation Table (CAT). This includes all USCIS Major Applications, General Support Systems and/or any sub-systems, minor applications or other information systems.

- A full Security Assessment is defined as testing that involves management, operational and technical controls for any given system. The scope of the testing will be proposed by the contractor and agreed upon or modified by the federal government lead.
- Limited / Ad Hoc Security Assessments are defined as testing that involves a scope as defined by the government (usually only technical controls) but can sometimes be other controls. The deliverable from this testing will be the technical results documents, with modifications to the original Security Assessment Report (SAR) and RTM as required/requested by the Federal Government.
- Review the controls that support the Requirements Traceability Matrix (RTM) and the details of the Security Plan (SP) to determine completeness and accuracy, including:
  - Ensuring accuracy of the assets identified within the system
  - Ensuring the assets are being properly tested within Security Center 5 or other related tool as required by the government and that the monthly testing results are accurate and proper credentials have been provided in order to yield accurate results
  - Identify any rogue assets that should be within the system boundary
- Provide a comprehensive Document Review (DR) of all SAP artifacts to support the SCA.
- All SAP documents must be fully reviewed to meet both DHS and USCIS FISMA requirements prior to SCA Kickoff, with the exception of the SP which should have Section 1 approved at SCA Gate 1 and Section 2 approved at SCA Gate 2 as per the USCIS SCA SOP, unless otherwise directed by the government.
- The SCA DR Team will implement a 2 day turn around for the following artifacts: FIPS 199, e-Authentication, PTA/PIA, ISA, BIA, MOU/MOA/IAA, CP, CPT, and other documents as deemed by the government and a 5 day turn around for the review of the full Security Plan (SP) / 2 day turn around for a Section 1 review of the SP.
- Establish a mailbox and report tracking mechanism to ensure that the federal staff knows where all SAP documents are in the review process at all times by running a simple report.
- Maintain, follow and abide by the SCA SOP that is provided by the government.
- Provide Security Assessment Results to meet Federal Government requirements and standards, which will include at a minimum the following documents: SAP, SAR, RTM, and a detailed technical results

document as stipulated by the Federal Government upon Security Assessment completion (ten days from task start).
    - Assist with the interpretation and analysis of Security Assessment Results upon completion of each Security Assessment and/or as requested to assist with post-assessment questions, to assess the vulnerability and risk to the system and to USCIS or other connected systems. Formal documentation of the analysis may be required.
- Create a POA&M table for each system in preparation for the Authorization within 2 days after acceptance of the SAR by the federal government. The POA&M Table shall be written to meet a quality standard ensuring they are approved by the federal government after only one round of comments.
- Security Assessments for any system will include 100% of all assets for any automated tests and 30% of all assets for any manual testing unless otherwise agreed upon or directed by the Government Task Lead.
- Collect un-remediated vulnerabilities from all sources and create POA&Ms as required and directed by the government.
- Provide technical review of ISSO provided artifacts or ad-hoc scans to accommodate POA&M closures and closure of all USCIS POA&Ms.
- Artifacts will be reviewed and a response provided to the ISSO within 2 business days of submittal from the ISSO. Response must include whether the artifact was acceptable to close the POA&M or not. If not, the response must be sufficiently detailed to provide the ISSO with a path forward for what is required to close the POA&M.
- Establish a mailbox and report tracking mechanism to ensure that the federal staff knows where all POA&Ms are in the POA&M management process at all times by running a simple report.
- Ensure that the federal staff knows where all POA&M closure requests are in the review process at all times by running a simple report.
- Contractor will travel to USCIS locations to perform on-site assessments as needed per government instruction.

3.2.1 SECURITY CONTROL ASSESSOR (SCA) SURGE (OPTIONAL CLIN)

This task supports a surge for the SCA Team as additional resources are identified and/or the mission grows beyond the support of the base contract.

This task supports the all Risk Management Framework (RMF) activities as outlined in the NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. This includes the process for managing security and privacy risk, including assessing the information security categorization; control selection, implementation, system and common control authorizations, and continuous monitoring.

Further, this task supports the security activities associated with evaluating, implementing, managing security practices and continued operations of new and existing technologies across the USCIS OIT Enterprise. The Contractor shall provide oversight into all system related security responsibilities as required. The Contractor shall support both USCIS Sensitive but Unclassified (SBU) and For Official Use Only (FOUO) systems. The Contractor shall perform all duties and responsibilities in accordance with DHS Sensitive Systems Policy Directive 4300A, DHS National Security Systems Policy 4300B, NIST 800-53/800-53A, and other applicable guidance.

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

- Risk Management Framework (RMF) Activities: Support all activities as outlined in the NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. This includes the process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.
- Provide the subject matter expertise to support the capability to assess individual systems simultaneously per federal government schedule. Each assessment will be complete within a period of 10 - 15 business days based on the complexity of the system, unless it is not realistic and the government has agreed to an extended period of time. The contractor shall submit written request for an extension within 3 business days upon assignment.
- Provide the subject matter expertise and proficiency using tools for security assessments, including but not limited to Nessus, WebInspect, DB Protect, Fortify, Appscan, Information Assurance Compliance System (IACS), RSA Archer, Nipper, Burp Suite Pro, WebSphere, ActiveState Perl, Aquafold, SoapUI Pro, Ultraedit, SNSScan, SolarWinds Engineer's Toolset, Fortify and/or other as required.
- Develop and provide all documentation necessary for performing a Security Control Assessment, to include but not limited to the following:
    - Security Control Assessment Plan (SCAP) or Security Assessment Plan (SAP)
        - The SCAP/SAP shall provide the objectives and scope for the security control assessment and a detailed roadmap of how the testing assessment shall be conducted.
        - The SCAP/SAP shall also identify security risks and threat vulnerabilities across all facets of the enterprise systems and connection points that are within the defined system authorization boundary.
    - System Access Requests
    - Plan of Actions & Milestones (POA&Ms)
    - Security Assessment Report (SAR)
    - Authorization Letters (Approval to Operate (ATO), Approval to Connect (ATC), Approval to Use (ATU), Interim Authority to Test (IATT), Authority to Proceed (ATP), and any other authorization documentation)
    - Requirement Technical Results – these results will include exact findings per IP Address. The government will provide guidance and a template to utilize.

  - Security Control Traceability Matrix (SCTM)/ Requirements Traceability Matrix (RTM)
- Other ad hoc system specific documentation as specified by the government
- Ensure that system access required for testing is acquired at least 30 days prior to Security Assessment start date and remains for at least 6 months post-assessment to accommodate any additional follow-on testing.
- Be proficient at testing, analyzing and interpreting Security Assessment Results for all systems, including but not limited to the following platforms:
  - Microsoft Server 2012/2016/Other
  - Windows Workstation Platforms
  - Microsoft SQL Server Platforms
  - Oracle DBs
  - Solaris / AIX / UNIX / Linux/ CentOS
  - Pervasive DB
  - Mobile Devices
  - Mainframes
  - Routers/Switches/Firewalls
  - Printers/Faxes/Multi-Function Devices
  - Cold fusion / PHP / ASP
  - Websphere / JAVA
  - Cloud Service Providers (CSPs)
    - IaaS (Infrastructure as a Service)
    - SaaS (Software as a Service)
    - PaaS (Platform as a Service)
- Conduct Security Control Assessments for each USCIS system as part of the Security Authorization Process; for each new system and for systems with expiring ATOs or when required by the Federal Government. In addition, SCAs will be conducted as required for systems entering into the Ongoing Authorization (OA) program or for systems currently in the OA Program based on the system's Control Allocation Table (CAT). This includes all USCIS Major Applications, General Support Systems and/or any sub-systems, minor applications or other information systems.
  - A full Security Assessment is defined as testing that involves management, operational and technical controls for any given system. The scope of the testing will be proposed by the contractor and agreed upon or modified by the federal government lead.
  - Limited / Ad Hoc Security Assessments are defined as testing that involves a scope as defined by the government (usually only technical controls) but can sometimes be other controls. The deliverable from this testing will be the technical results documents, with modifications to the original Security Assessment Report (SAR) and RTM as required/requested by the Federal Government.
  - Review the controls that support the Requirements Traceability Matrix (RTM) and the details of the Security Plan (SP) to determine completeness and accuracy, including:
    - Ensuring accuracy of the assets identified within the system

        - Ensuring the assets are being properly tested within Security Center 5 or other related tool as required by the government and that the monthly testing results are accurate and proper credentials have been provided in order to yield accurate results
        - Identify any rogue assets that should be within the system boundary
    - Provide a comprehensive Document Review (DR) of all SAP artifacts to support the SCA.
    - All SAP documents must be fully reviewed to meet both DHS and USCIS FISMA requirements prior to SCA Kickoff, with the exception of the SP which should have Section 1 approved at SCA Gate 1 and Section 2 approved at SCA Gate 2 as per the USCIS SCA SOP, unless otherwise directed by the government.
    - The SCA DR Team will implement a 2 day turn around for the following artifacts: FIPS 199, e-Authentication, PTA/PIA, ISA, BIA, MOU/MOA/IAA, CP, CPT, and other documents as deemed by the government and a 5 day turn around for the review of the full Security Plan (SP) / 2 day turn around for a Section 1 review of the SP.
    - Establish a mailbox and report tracking mechanism to ensure that the federal staff knows where all SAP documents are in the review process at all times by running a simple report.
    - Maintain, follow and abide by the SCA SOP that is provided by the government.
    - Provide Security Assessment Results to meet Federal Government requirements and standards, which will include at a minimum the following documents: SAP, SAR, RTM, and a detailed technical results document as stipulated by the Federal Government upon Security Assessment completion (ten days from task start).
    - Assist with the interpretation and analysis of Security Assessment Results upon completion of each Security Assessment and/or as requested to assist with post-assessment questions, to assess the vulnerability and risk to the system and to USCIS or other connected systems. Formal documentation of the analysis may be required.
- Create a POA&M table for each system in preparation for the Authorization within 2 days after acceptance of the SAR by the federal government. The POA&M Table shall be written to meet a quality standard ensuring they are approved by the federal government after only one round of comments.
- Security Assessments for any system will include 100% of all assets for any automated tests and 30% of all assets for any manual testing unless otherwise agreed upon or directed by the Government Task Lead.
- Collect un-remediated vulnerabilities from all sources and create POA&Ms as required and directed by the government.
- Provide technical review of ISSO provided artifacts or ad-hoc scans to accommodate POA&M closures and closure of all USCIS POA&Ms.
- Artifacts will be reviewed and a response provided to the ISSO within 2 business days of submittal from the ISSO. Response must include whether the artifact was acceptable to close the POA&M or not. If not, the response must be sufficiently detailed to provide the ISSO with a path forward for what is required to close the POA&M.

- Establish a mailbox and report tracking mechanism to ensure that the federal staff knows where all POA&Ms are in the POA&M management process at all times by running a simple report.
- Ensure that the federal staff knows where all POA&M closure requests are in the review process at all times by running a simple report.
- Contractor will travel to USCIS locations to perform on-site assessments as needed per government instruction.

3.3 CLASSIFIED SYSTEMS AND SCIF SUPPORT

3.3.1 CLASSIFIED SYSTEMS INFORMATION SYSTEM SECURITY OFFICER (C-ISSO) SUPPORT

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

Possess and maintain a Top-Secret Sensitive Compartment Information TS-SCI security clearance pursue the responsibilities of a classified support personnel. Provide Classified Information System Security Officer (C-ISSO) support for USCIS classified applications and Tier-I/II support for **USCIS SCIF**s. The C-ISSO task will be given to the two USCIS Headquarters resources. The Contractor shall perform all duties and responsibilities in accordance with DHS 4300A, DHS 4300B, DHS 4300C, DHS ISSO Guide, and other applicable guidance. The Contractor will support USCIS Enterprise Classified and Unclassified Systems within USCIS SCIFs as required.

The USCIS Headquarter contractor resources shall be assigned C-ISSO duties for the existing USCIS applications/systems in addition to the Tier-I/II support duties. The Headquarters C-ISSOs may be assigned additional systems or applications. The remaining SCIF contractor resources will only be responsible for providing Tier-I/II level support to SCIF personnel.

Classified-ISSO Duties:

- Risk Management Framework (RMF) Activities: Support all activities as outlined in the NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. This includes the process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.
- Security Authorization Documentation: Initial development and, at least, annual reviews/updates of the FIPS 199, e-Authentication, Privacy Threshold Analysis (PTA)/Privacy Impact Analysis (PIA), Security Plan (SP), Contingency Plan (CP), and Contingency Plan Test (CPT), Interconnection Security Agreement (ISAs) and

Memorandum of Agreement/Understanding (MOA/Us) and any other FISMA related security documentation.

- Security Control Assessment Response: Support all assessment activities by responding to interview questions as well as working with the system teams to gather appropriate evidence as directed by the SCA team.
- Change Management: Review all change requests for potential impact to the system security posture.
- Continuous Monitoring: Conduct audit log and account management reviews as required, and update the any additional logs, as necessary.
- Configuration/Patch/Vulnerability Management: Review scan results for the system assets, identify the respective remediation's for misconfigurations and weaknesses, and work with the system team to ensure timely implementation of fix.
- Incident Response: Work with the Security Operations Center (SOC) and system teams to investigate and analyze any incidents affecting assigned system(s).
- Have the ability to apply a comprehensive knowledge across key tasks and high impact assignments
- Evaluate performance results and recommend major changes affecting short-term project growth and success
- Function as a technical expert across multiple project assignments
- Work on high priority ad-hoc request such as data calls, Senior Management Initiatives (CIO, CISO, etc.), DHS/USCIS mandates, etc.
- Per the DHS 4300C, ensure all new hardware/systems (to include standalone, guest systems, and systems of different classification levels) introduced and/or operated within the SCIF are recorded and updated in a hardware inventory list. All new/updated inventory lists must be forwarded to the I&A CISO Security Control Assessor (SCA).
- Participate USCIS or DHS ISSO training courses to satisfy training requirements associated with the role of ISSO. The ISSO may provide proof of other training courses (if available) to the I&A CISO for acceptance of meeting the training requirement.
- Assist the I&A CISO with matters regarding oversight and compliance, and when specifically directed by I&A CISO, distribute additional security awareness information or training requirements to the user community as appropriate (Additional insight will be provided through ICOP training).
- Must report to the I&A CISO/ICOP PM (on a monthly basis) as part of the continuous monitoring activities, as well as the monthly checklist.
- Ensure system related information is entered into the DHS Classified Information Assurance Compliance System (CIACS) as necessary.

3.3.2 CLASSIFIED SUPPORT

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

Possess and maintain a Top-Secret Sensitive Compartment Information TS-SCI security clearance pursue the responsibilities of a classified support personnel. Provide Classified Information System Security Officer (C-ISSO) support for USCIS classified applications and Tier-I/II support for USCIS SCIFs. The C-ISSO task will be given to the two USCIS Headquarters resources. The Contractor shall perform all duties and responsibilities in accordance with DHS 4300A, DHS 4300B, DHS 4300C, DHS ISSO Guide, and other applicable guidance. The Contractor will support USCIS Enterprise Classified and Unclassified Systems within USCIS SCIFs as required.

The USCIS Headquarter contractor resources shall be assigned C-ISSO duties for the existing USCIS applications/systems in addition to the Tier-I/II support duties. The Headquarters C-ISSOs may be assigned additional systems or applications. The remaining SCIF contractor resources will only be responsible for providing Tier-I/II level support to SCIF personnel.

Classified Support Duties:

- Ensure protective measures are in place for the security of the IT equipment in the SCIFs (Washington D.C, Harrisonburg, VA, and Lee Summit, MO, Burlington, VT, Atlanta, GA) and any future SCIFs, the documented equipment and media going in and out of the SCIFs, as well as providing technical support for the users and HSDN rooms.
- Assist with any Service Desk incident or request for service regarding software or hardware within the SCIF
- Ensure compliance with all Intelligence Community (IC) policies and guidance concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses.
- Assist the I&A CISO with matters regarding oversight and compliance, and when specifically directed by I&A CISO, distribute additional security awareness information or training requirements to the user community as appropriate (Additional insight will be provided through ICOP training).
- Report IT security incidents (including computer viruses) in accordance with established procedures.
- Report security incidents not involving IT resources to the appropriate security office and/or the USCIS SSO.
- Complete and maintain an up to date inventory of all system components for assigned classified system.

- Ensure Rules of Behavior are signed for all system users.
- Ensure a visitor log is being utilized and maintained for access to physical spaces where system components reside and review the visitor logs on at least a monthly basis.
- Attend security awareness and related training programs and distribute security awareness information to the user community as appropriate.
- Provide input to appropriate IT security personnel for preparation of reports to higher authorities concerning information systems.
- Provide Security Incident Management and Security Architecture assistance, including but not limited to development and maintenance of technical and administrative processes, methods, procedures and solutions, as required.
- Complete security questionnaires attached to any USCIS, DHS and OneNet change requests.
- Review and provide recommendations to Government managers for USCIS, DHS and OneNet change requests that are reviewed at the various boards.
- Provide gateway support to the USCIS Information Technology Lifecycle Management (ITLM) resources for USCIS information systems.
- Perform tasks to support DHS ICCB CR requirements for all USCIS information systems, including review of DHS CR packages, ICCB CR forms, and CR test and backout plans as well as submit DHS ICCB security questionnaires and required security package for applicable CRs.
- Support the development and documentation of contingency plans, disaster recovery (DR) plans, and Continuity of Operations (CONOPS) plans. In addition, the Contractor shall support the execution of emergency backups in coordination with other infrastructure operational components and/or DHS Data Center specific requirements.
- Provide support to SCIF users in troubleshooting software, hardware and network problems for all unclassified (CISNET) and classified (HSDN & C-L:AN) equipment and systems within the SCIF.
- Work with the USCIS unclassified Desktop Support Contractor in supporting the unclassified equipment within the SCIF.
- Ensure protective measures are in place for the security of the IT equipment in the SCIFs (Washington D.C, Harrisonburg, VA, and Lee Summit, MO, Burlington, VT, Atlanta, GA) and any future SCIFs, the documented equipment and media going in and out of the SCIFs, as well as providing technical support for the users and HSDN rooms.
- Assist with any Service Desk incident or request for service regarding software or hardware within the SCIF
- Ensure compliance with all Intelligence Community (IC) policies and guidance concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses.

- Per the DHS 4300C, ensure all new hardware/systems (to include standalone, guest systems, and systems of different classification levels) introduced and/or operated within the SCIF are recorded and updated in a hardware inventory list. All new/updated inventory lists must be forwarded to the I&A CISO Security Control Assessor (SCA).
- Perform HSDN and C LAN Token Authority duties such as issue tokens, replace defective/lost tokens, receive good tokens no longer needed by the user, and reset PINs.
- Escort un-cleared personnel/vendors/technicians who have a valid need to be in the secured facilities (SCIFs/HSDN rooms) to complete a task.
- Assist DHS ESOC and CIS SOC with data spillage of classified data on equipment that is of a lower classification.
- Provide monthly reports to DHS for the classified equipment that is in the SCIFs.
- Assist the USCIS SOC with the monthly DHS IOC Exercises on the classified networks to pass down unclassified information to the USCIS SOC on the unclassified system.
- Perform other related tasks as requested by the Government.

The table below provides the services required at each SCIF location.

Location	C-ISSO	Tier I/II Support	Notes
USCIS Headquarters	X	X	
USCIS Headquarters-131 M Street	X	X	131 M Street NW is considered to be a part of the Headquarters SCIF
Harrisonburg, VA		X	The Harrisonburg facility is considered to be a part of the Headquarters SCIF for support purposes.
Burlington, VT		X	
Atlanta, GA		X	
Lee's Summit, MO		X	

3.3.3 CLASSIFIED SUPPORT (OPTIONAL CLIN)

This Optional CLIN will support a surge for one Classified Support Personnel that will provide services to USIS HQ, located in the Washington DC area as an additional resource to support the mission if additional funding is acquired.

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

Possess and maintain a Top-Secret Sensitive Compartment Information TS-SCI security clearance pursue the responsibilities of a classified support personnel. Provide Classified Information System Security Officer (C-ISSO) support for USCIS classified applications and Tier-I/II support for USCIS SCIFs. The C-ISSO task will be given to the two USCIS Headquarters resources. The Contractor shall perform all duties and responsibilities in accordance with DHS 4300A, DHS 4300B, DHS 4300C, DHS ISSO Guide, and other applicable guidance. The Contractor will support USCIS Enterprise Classified and Unclassified Systems within USCIS SCIFs as required.

The USCIS Headquarter contractor resources shall be assigned C-ISSO duties for the existing USCIS applications/systems in addition to the Tier-I/II support duties. The Headquarters C-ISSOs may be assigned additional systems or applications. The remaining SCIF contractor resources will only be responsible for providing Tier-I/II level support to SCIF personnel.

Classified Support Duties:

- Ensure protective measures are in place for the security of the IT equipment in the SCIFs (Washington D.C, Harrisonburg, VA, and Lee Summit, MO, Burlington, VT, Atlanta, GA) and any future SCIFs, the documented equipment and media going in and out of the SCIFs, as well as providing technical support for the users and HSDN rooms.
- Assist with any Service Desk incident or request for service regarding software or hardware within the SCIF
- Ensure compliance with all Intelligence Community (IC) policies and guidance concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses.
- Assist the I&A CISO with matters regarding oversight and compliance, and when specifically directed by I&A CISO, distribute additional security awareness information or training requirements to the user community as appropriate (Additional insight will be provided through ICOP training).
- Report IT security incidents (including computer viruses) in accordance with established procedures.
- Report security incidents not involving IT resources to the appropriate security office and/or the USCIS SSO.
- Complete and maintain an up to date inventory of all system components for assigned classified system.
- Ensure Rules of Behavior are signed for all system users.

- Ensure a visitor log is being utilized and maintained for access to physical spaces where system components reside and review the visitor logs on at least a monthly basis.
- Attend security awareness and related training programs and distribute security awareness information to the user community as appropriate.
- Provide input to appropriate IT security personnel for preparation of reports to higher authorities concerning information systems.
- Provide Security Incident Management and Security Architecture assistance, including but not limited to development and maintenance of technical and administrative processes, methods, procedures and solutions, as required.
- Complete security questionnaires attached to any USCIS, DHS and OneNet change requests.
- Review and provide recommendations to Government managers for USCIS, DHS and OneNet change requests that are reviewed at the various boards.
- Provide gateway support to the USCIS Information Technology Lifecycle Management (ITLM) resources for USCIS information systems.
- Perform tasks to support DHS ICCB CR requirements for all USCIS information systems, including review of DHS CR packages, ICCB CR forms, and CR test and backout plans as well as submit DHS ICCB security questionnaires and required security package for applicable CRs.
- Support the development and documentation of contingency plans, disaster recovery (DR) plans, and Continuity of Operations (CONOPS) plans. In addition, the Contractor shall support the execution of emergency backups in coordination with other infrastructure operational components and/or DHS Data Center specific requirements.
- Provide support to SCIF users in troubleshooting software, hardware and network problems for all unclassified (CISNET) and classified (HSDN & C-L:AN) equipment and systems within the SCIF.
- Work with the USCIS unclassified Desktop Support Contractor in supporting the unclassified equipment within the SCIF.
- Ensure protective measures are in place for the security of the IT equipment in the SCIFs (Washington D.C, Harrisonburg, VA, and Lee Summit, MO, Burlington, VT, Atlanta, GA) and any future SCIFs, the documented equipment and media going in and out of the SCIFs, as well as providing technical support for the users and HSDN rooms.
- Assist with any Service Desk incident or request for service regarding software or hardware within the SCIF
- Ensure compliance with all Intelligence Community (IC) policies and guidance concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses.
- Per the DHS 4300C, ensure all new hardware/systems (to include standalone, guest systems, and systems of different classification levels) introduced and/or operated

within the SCIF are recorded and updated in a hardware inventory list. All new/updated inventory lists must be forwarded to the I&A CISO Security Control Assessor (SCA).

- Perform HSDN and C LAN Token Authority duties such as issue tokens, replace defective/lost tokens, receive good tokens no longer needed by the user, and reset PINs.
- Escort un-cleared personnel/vendors/technicians who have a valid need to be in the secured facilities (SCIFs/HSDN rooms) to complete a task.
- Assist DHS ESOC and CIS SOC with data spillage of classified data on equipment that is of a lower classification.
- Provide monthly reports to DHS for the classified equipment that is in the SCIFs.
- Assist the USCIS SOC with the monthly DHS IOC Exercises on the classified networks to pass down unclassified information to the USCIS SOC on the unclassified system.
- Perform other related tasks as requested by the Government.

The table below provides the services required at each SCIF location.

Location	C-ISSO	Tier I/II Support	Notes
USCIS Headquarters	X	X	
USCIS Headquarters-131 M Street	X	X	131 M Street NW is considered to be a part of the Headquarters SCIF
Harrisonburg, VA		X	The Harrisonburg facility is considered to be a part of the Headquarters SCIF for support purposes.
Burlington, VT		X	
Atlanta, GA		X	
Lee's Summit, MO		X	

3.4 GOVERNANCE SUPPORT

The Governance function establishes a framework for consistently collecting, analyzing, and distributing guidance, materials and knowledge throughout USCIS. These security documents are developed and compiled in accordance with DHS Directive 4300A, "Sensitive Systems Policy and Handbook" and NIST to protect the confidentiality, integrity, and availability of

USCIS information and information assets to accomplish the Agency's mission(s). Program Support provides technical writing and communication expertise to facilitate a broad range of ISD requirements ranging from the development of acquisition packages to briefing materials and stakeholder correspondence.

The USCIS Governance Program is established in accordance with FISMA Office of Management and Budget (OMB) Circular A-130, Management of Federal Information resources, Appendix III, Security of Federal Automated Information resources; and DHS policy. This Information Assurance (IA)/Security Governance Program established the framework for the overall Information Security Program through the development, documentation, and maintenance of IA (Security) policies, standards, procedures, and guidance. The compilation of these documents is essential to the overall effectiveness of the Agency working towards enterprise security solutions and implementing them in accordance with well-defined security architecture.

The Contractor shall:

- Maintain, review and develop ISD policies and procedures utilizing simple and plain language.
- Maintain and update ISD policies and procedures to reflect any changes in the U.S. Laws, Executive Branch, DHS and Component internal standard operating procedures.
- Review all security control content in accordance with NIST SP 800-53 (latest edition/revision), "Recommended Security Controls for Federal Information Systems and Organizations", DHS 4300A and any other applicable guidance in drafting security policies.
- Publish and maintain the current policies and procedure library within the USCIS documentation repository system, and assist the Government POC in the transferring of ISD documentation to the appropriate SharePoint libraries.
- Manage the USCIS routing and approval process for documents created and maintained, and coordinate with offices external to ISD, for the purpose of reviewing and updating policies and procedures.
- Compare and analyze USCIS policies and procedures to ensure compliance with OMB, Government Accountability Office (GAO), NIST, DHS, National Archives and Records Administration (NARA), and other authoritative guidance sources as established by U.S. law or the Executive Branch.
- Develop policies and procedures as directed by the client in relationship to Information Assurance.
- Participate annually in the reviewing of the DHS 4300-series and other DHS policies, memorandums, and documentation forwarded to USCIS for component-level review.
- Assist in the coordination efforts of the Agency's reviews and responses to draft information security policies, procedures, processes, guides and audit documentation.
- Collect and provide a coordinated response of all reviews prior to submission.

- At the direction of the client, participate in working groups such as the DHS Information Security Working Group, IA Policy Working Group, DHS Cybersecurity Working Group, DHS Security Policy Working Groups and others as directed. Provide meeting minutes for each attended working group, per meeting.
- Assist with writing, editing and publishing IT system security and privacy planning policy, procedures, and technical system documentation as requested by the Government
- Assist the program manager, acquisition team and technical personnel with the development of documentation to support the acquisition of IT security services and equipment. Specifically support the collection of relevant information, writing, and editing of the necessary acquisition documents for submission to the program manager for review.
- Support the creation and technical writing for white papers, position papers, decision memorandums, guides, communications, PowerPoint presentations to a variety of audiences including stakeholders, management and end users.
- Assist the Federal liaison providing support to internal and external agencies/auditors, such as DHS and GAO and document system security reviews, inspections, audits and other evaluations and control audit requirements (i.e. NIST 800-53-A).

3.4.1 GOVERNANCE SUPPORT SURGE (OPTIONAL CLIN)

This Optional CLIN will support a surge for one Governance Support Personnel that will provide services to SGB as an additional resource to support the Governance mission if additional funding is acquired.

The Governance function establishes a framework for consistently collecting, analyzing, and distributing guidance, materials and knowledge throughout USCIS. These security documents are developed and compiled in accordance with DHS Directive 4300A, “Sensitive Systems Policy and Handbook” and NIST to protect the confidentiality, integrity, and availability of USCIS information and information assets to accomplish the Agency’s mission(s). Program Support provides technical writing and communication expertise to facilitate a broad range of ISD requirements ranging from the development of acquisition packages to briefing materials and stakeholder correspondence.

The USCIS Governance Program is established in accordance with FISMA Office of Management and Budget (OMB) Circular A-130, Management of Federal Information resources, Appendix III, Security of Federal Automated Information resources; and DHS policy. This Information Assurance (IA)/Security Governance Program established the framework for the overall Information Security Program through the development, documentation, and maintenance of IA (Security) policies, standards, procedures, and guidance. The compilation of these documents is essential to the

overall effectiveness of the Agency working towards enterprise security solutions and implementing them in accordance with well-defined security architecture.

The Contractor shall:

- Maintain, review and develop ISD policies and procedures utilizing simple and plain language.
- Maintain and update ISD policies and procedures to reflect any changes in the U.S. Laws, Executive Branch, DHS and Component internal standard operating procedures.
- Review all security control content in accordance with NIST SP 800-53 (latest edition/revision), "Recommended Security Controls for Federal Information Systems and Organizations", DHS 4300A and any other applicable guidance in drafting security policies.
- Publish and maintain the current policies and procedure library within the USCIS documentation repository system, and assist the Government POC in the transferring of ISD documentation to the appropriate SharePoint libraries.
- Manage the USCIS routing and approval process for documents created and maintained, and coordinate with offices external to ISD, for the purpose of reviewing and updating policies and procedures.
- Compare and analyze USCIS policies and procedures to ensure compliance with OMB, Government Accountability Office (GAO), NIST, DHS, National Archives and Records Administration (NARA), and other authoritative guidance sources as established by U.S. law or the Executive Branch.
- Develop policies and procedures as directed by the client in relationship to Information Assurance.
- Participate annually in the reviewing of the DHS 4300-series and other DHS policies, memorandums, and documentation forwarded to USCIS for component-level review.
- Assist in the coordination efforts of the Agency's reviews and responses to draft information security policies, procedures, processes, guides and audit documentation.
- Collect and provide a coordinated response of all reviews prior to submission.
- At the direction of the client, participate in working groups such as the DHS Information Security Working Group, IA Policy Working Group, DHS Cybersecurity Working Group, DHS Security Policy Working Groups and others as directed. Provide meeting minutes for each attended working group, per meeting.
- Assist with writing, editing and publishing IT system security and privacy planning policy, procedures, and technical system documentation as requested by the Government
- Assist the program manager, acquisition team and technical personnel with the development of documentation to support the acquisition of IT security services and equipment. Specifically support the collection of relevant

information, writing, and editing of the necessary acquisition documents for submission to the program manager for review.

- Support the creation and technical writing for white papers, position papers, decision memorandums, guides, communications, PowerPoint presentations to a variety of audiences including stakeholders, management and end users.
- Assist the Federal liaison providing support to internal and external agencies/auditors, such as DHS and GAO and document system security reviews, inspections, audits and other evaluations and control audit requirements (i.e. NIST 800-53-A).

3.5 TACTICAL COMMUNICATIONS (TACCOM)

USCIS TACCOM Program is responsible for the management and operation of the USCIS tactical communications capabilities. The primary customers of the USCIS TACCOM program are the Office of Security and Integrity (OSI), Mission Integrity Division (MID), Emergency Management Safety (EMS) Branch, and OSI Investigations Division (ID). Support is also provided to other USCIS Offices and Directorates such as the Refugee Affairs and International Operations (RAIO) Directorate as needed. The TACCOM program must be capable of supporting normal operations, major incidents, and major disaster communications and must be scalable to support additional users in times of crisis. The sharing of knowledge and information is central to the effective discharge of USCIS mission and operational responsibilities. As such, reliable, available, and secure tactical communications are a mission-critical requirement for employee safety and mission and operational effectiveness. Reliable and protected wireless technology provides USCIS with continuous access to timely information, including intelligence, logistics, investigative reporting, investigative assignment, and administrative support functions.

USCIS tactical communications systems support essential emergency management operations within the National Capital Region (NCR), major Service Centers, District Offices, Regional Offices and critical USCIS Continuity of Government (COG) and Continuity of Operations (COOP) communication activities. The maturing and strengthening of USCIS's mission require that USCIS operate and maintain its tactical communications equipment to support Emergency communications, COOP/COG requirements, and foster innovative approaches and solutions to Engineering and Maintenance challenges and program improvements. Through effective and efficient support, this initiative will support essential operations to protect the people of the United States and bolster operational effectiveness by streamlining processes, creating innovative solutions to agency requirements and improving service delivery.

The Contractor shall provide engineering support for the TACCOM program and may provide support the COMSEC program. The contractor shall obtain and maintain a Top-Secret Sensitive Compartment Information TS-SCI security clearance to pursue the responsibilities of a communications security engineer. The contractor shall adhere to the DHS Systems Engineering

Life Cycle (SELC) process as established by DHS Management Directive 102-01-103. Any deviation or tailoring from the DHS SELC guide will have prior approval from government. The engineering support for TACCOM includes the documentation of the feasibility study, system engineering requirement analysis, Systems Engineering Master Plan (SEMP), Test and Evaluation Management Plan (TEMP) at various TACCOM locations.

The USCIS TACCOM infrastructure currently consists of, Motorola conventional P25 compliant, Motorola non-P25 compliant hardware and Barrett HF Transceivers (Base and Portable) and antennas.

- Approximately 9 infrastructure sites nationwide, with growth anticipated to approximately 380 sites during the duration after task order award.
- The contractor is expected to provide support for Portable/Handheld TACCOM devices which will be located within the National Capital Region (NCR). Any deployed handheld radios will be shipped to USCIS Headquarters (HQ) for support.
- Approximately 5-20 collateral duty Emergency Management Coordinators (EMC) and Emergency Response Group (ERG) volunteers within each USCIS facility (depending on building size) equipped with portable and mobile radios of various manufacture.
- Major facilities are located in the Washington DC metro area, Virginia, Vermont, Nebraska, Texas, Missouri and California. In addition, smaller offices are located in every state as well as Out of the Continental U.S (OCONUS) and international locations. The international office locations are not part of this SOW. Travel to the locations under this task area is expected to be minimal.
- The USCIS radio inventory consists of Motorola Quad Band Portable Radios: XTS 8000 UHF/VHF 700/800MHz, Motorola DTR 500, DTR 650, DTR 700 and DTR 720 handheld radios, and Barrett 4020 and 4050 High Frequency Transceiver radios; All radios should be capable of Over the Air Rekey/Over The Air Programing (OTAR/OTAP).
- The contractor shall be proficient in using manufactures (Motorola and Barrett, or similar) radio programing software to manage, configure, program, develop and load code plugs, channels, frequencies, etc.
- The contractor is expected to have knowledge and experience with radio transmission principles and theory, antenna theory, and basic antenna design.
- The contractor shall have experience with antenna modeling or design software such as EZNEC or attain the capability within 6 months.
- The contractor shall have or attain within one year, a Federal Communications Commission (FCC) Amateur Radio License at the Technician level or greater.
- Addend Training and maintain technical skills on tactical communication systems utilized by USCIS and attend government sponsored training on new and/or existing communication systems.
- Participate and maintain accurate inventories of all TACCOM assets. The contractor shall work with appropriate government POCs as required.

- Communicate with TACCOM vendors at the government's request on behalf of the government.
- Participate in meetings and provide meaningful participation as needed.
- Generate reports and other deliverables as requested to meet the government's needs (i.e. Data calls);
- Facilitate meetings as necessary with leaders, managers, project managers, stakeholders, vendors, and users.
- Work in collaboration with support elements to test and evaluate TACCOM solutions to assist in meeting the objectives of the program.
- Create and maintain user, administrator, engineering, and compliance/accreditation documentation as requested
- Effectively partners and communicates with business and technical stakeholders
- Mentor and train USCIS employees in TACCOM equipment, tools, techniques and procedures.
- Design of sites, systems, and technical solutions to meet operational requirements, with adherence to technical standards and USCIS direction
- Integration of equipment, parts, and accessories, testing of equipment, installation of equipment, and optimization of new equipment, systems, and technical solutions
- Evaluation, analysis, and recommendations of existing, new, and emerging technologies in support of USCIS TACCOM operations
- Administrative support to document and manage sites and circuits in support of USCIS TACCOM Program.
- The Contractor shall manage and coordinate resources to ensure the on-time delivery of services, equipment, and projects for the Government.
- The Contractor shall manage and coordinate the Contractor's costs for services, equipment, and projects to ensure that projects and O&M efforts are completed in a cost-effective manner.
- The Contractor shall report to the Government the status of all projects and O&M efforts, including costs, schedule, technical performance, issues, and planned work.
- The Contractor shall assist with any technology transfers required by USCIS from industry, government and/or academia.
- The Contractor shall develop or provide assistance with the development of training documentation and books, slide deck presentations, and other related training materials.
- Perform other duties as assigned by the government.

3.6 COMMUNICATIONS SECURITY PROGRAM SUPPORT

This task supports the COMSEC program which is responsible to prevent unauthorized access to telecommunications traffic, or to any written information that is transmitted or transferred. The contractor will provide a resource to provide operations and maintenance to ensure cryptographic security, emission security, transmission security, and ensure the safety

of the network's cryptographic information equipment. The contractor shall obtain and maintain a Top-Secret Sensitive Compartment Information TS-SCI security clearance pursue the responsibilities of a communications security engineer.

The Contractor shall, under the leadership and guidance of the Government PM and supporting government staff:

- Providing expertise as a COMSEC Responsible Officer when required by the Government in individual task orders;
- Rapidly resolving COMSEC issues to the complete satisfaction of the appropriate COMSEC inspection authorities;
- Receipt, custody, issuance, safeguarding, accounting for and when necessary, destruction of COMSEC material for offices and/or operating units under their areas for responsibility;
- Maintaining COMSEC and performing system administrator functions with full access privileges to the Local Management Devices / Key Processors (LMDs/KPs);
- Creating, deleting, and modifying COMSEC operator accounts and create/delete hand receipt holder accounts;
- Performing downloads of crypto key from the Electronic Key Management System (EKMS);
- Conduct inventories of COMSEC material IAW with regulations;
- Maintaining up-to-date records of COMSEC inventory and submitting required accounting reports;
- Maintaining crypto equipment and operational keys;
- Rekeying and reinitializing crypto equipment as required and troubleshoot/resolve crypto problems;
- Processing COMSEC material for shipping through the Defense Courier Service, US Registered Mail, and FedEx;
- Maintain copies of all briefings and debriefings;
- Undergo required COMSEC training within six months of appointment and update training yearly;
- Perform required audits of each COMSEC account in accordance with government schedules and timelines;
- Provide help desk for technical and administrative questions;
- Evaluate new COMSEC equipment for use by USCIS employees and contractors;
- Represent USCIS in working groups and committees;
- Provide technical support to USCIS to facilitate interoperability of purchases of COMSEC equipment;
- Complete documents and updates as necessary to include but not limited to: COMSEC SOPs, COMSEC training documentation, COMSEC material accounting, and COMSEC Incident Reports.
- Mentor and train USCIS employees in COMSEC equipment, tools, techniques and procedures
- Perform other duties as assigned by the government.

4 TASK ORDER ADMINISTRATION

4.1 DELIVERABLES

The Contractor shall submit the deliverables that are indicated in Attachment II to the Government COR, Program Manager (PM), and Contracting Officer (CO), or as directed by the Government.

The Contractor shall provide all necessary personnel and deliverables based on the required delivery date(s) established by mutual agreement between the Government and the Contractor in the Task Order.

The table in Attachment II aggregates all the deliverables that are part of this Task Order.

4.1.1 INSPECTION AND ACCEPTANCE OF DELIVERABLES

Inspection and acceptance of deliverables will use the following procedures:

- In keeping with Agile methods and principles and vary based on team agreements and structure, acceptance criteria may be identified with each user story and/or sprint.
- For other deliverables, the government will provide written acceptance, comments, and/or change requests, if any, within ten (10) calendar days of receipt of task order deliverables.
- If government acceptance, comments, and/or change requests are not provided to the contractor within 15 calendar days after delivery of a deliverable, the contractor shall assume government acceptance.

Upon receipt of the Government comments, the Contractor shall, within 5 business days, rectify the situation and re-submit the Task Order deliverable(s) if it is not a "draft" deliverable. If it is a "draft" deliverable, the Contractor shall rectify the situation before the next scheduled submission of this deliverable.

4.2 PLACE OF PERFORMANCE

The principal place of performance with the exception of the Classified Systems and SCIF Support shall be at the Government provided work site at USCIS Headquarters, currently located at 111 Massachusetts Avenue NW, Washington, DC and will soon move to Camp Springs, MD. The TACCOMs and COMSEC Engineers also will perform duties in the SCIF and Secret Open/Closed

The principal place of performance with the exception of the Classified Systems and SCIF Support shall be at the Government provided work site at USCIS Headquarters, currently located at 111 Massachusetts Avenue NW, Washington, DC and will soon move to Camp Springs, MD. The TACCOMs and COMSEC Engineers also will perform duties in the SCIF and Secret Open/Closed Facilities. Additionally, two Classified Support personnel will support the SCI Facilities and Secret Open/Closed Facilities; one will support the SCIF located in Atlanta, GA SCIF and one will support the SCIF located in Lee Summit, MO. Meetings will ordinarily take place at OIT offices in the Washington, DC metropolitan area, including 20 Massachusetts Avenue, NW, 111 Massachusetts Avenue, NW, Washington, DC, and Camp Springs, MD. The contractor is expected to be available for meetings and normal work performance at any USCIS locations within the DC metropolitan area. The government requires that contractor personnel be onsite at minimum two days a week. The SCIFs will be at USCIS Government Locations. Additionally, contractors will not be granted access until all requirements of the DCI Directive 6/4 and Intelligence Community Directive (ICD) 704 have been met.

The TACCOM and Security Control Assessment tasks may require travel outside of the National Capital Region to support mission requirements.

4.3 CONTRACTOR WORKFORCE

This SOW is comprised of two personnel labor categories: Key Personnel and the Contract Staff. The Contractor shall also ensure the Key Personnel and the other Contract Staff have the experience and qualifications necessary to perform the duties and/or task areas outlined in this SOW. The Government PM may waive the requirement for certifications and experience, on a case by case basis.

The Government shall have the authority to remove or suspend Contractor personnel from the contract for any one of a number of reasons, included but not limited to poor performance, inability to pass or maintain certification requirements, or unacceptable behavior. Additionally, the Government shall receive and approve the resume of each hire.

4.3.1 KEY PERSONNEL

The personnel listed in the table below are considered key personnel and shall possess the following skills, level of experience, and certifications.

Key Personnel are considered essential to the work being performed under this task order and, in accordance with HSAR 3052.215-70, may be changed from time to time during the course of the task order by adding or deleting personnel, as appropriate.

All lead personnel on the Task Order shall possess not only management skills, but technical skills as well and be hands-on executors, rather than just managers. The Contractor shall identify key personnel, provide a statement of qualifications and resume for each individual upon task award and at any time there is a change. The statement of qualification will include a YES or NO declaration for meeting each of the requirements and the resume will show how the individual meet the requirements for the position. The Government Program Manager (PM) shall accept, reject, or request an in-person meeting with all proposed Key Personnel within five (5) business days.

Before removing or replacing any Key Personnel (abruptly, or for other than cause), the Contractor shall notify the Contracting Officer, in writing, before the change become effective. When a person identified as Key Personnel requires removal or replacement for cause, the Contractor shall notify the Contracting Officer within one (1) hour of removal and provide sufficient information supporting the action. Key Personnel are critical to the success of this work and shall meet the experience and other requirements set forth in the below.

Labor Category	Role on the Program	Required Certification(s)/ Experience
Program Manager Level III	Provide overall authority and responsibility for the Contractor Task Order management and execution (1 Contractor Full Time Equivalent (CFTE 1).	• BA/BS and seven (7) continuous years of Program Management experience in Security Operations or equivalent area* • Active PMI Project Management Professional (PMP) or an equivalent/ higher certification* • Active ISC2 Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) or comparable certification* • Fluent knowledge of Agile development and management methodologies • Contractor certification and experience must be approved in advance by the Government PM and may be waived/ exempted on a case-by-case basis • **Personnel serving in this task order must be able to attain and keep a TOP SECRET level clearance.**

Labor Category	Role on the Program	Required Certification(s)/ Experience
COMSEC	Alternate COMSEC Custodian (1 CFTE)	• Each contractor in this task area shall have and maintain at least one (1) active certification such as but not limited to Network+, Security+, CASP, GSEC, GSLC, CISSP, or other comparable certification or experience which must be approved in advance by the Government on a case-by-case basis. . • The contractor shall have a minimum of four (4) years of experience as a COMSEC Custodian. • Contractor shall be staffed in USCIS Headquarters and the ability to travel on an as needed basis (example: Mt. Weather, Bluemont VA, Harrisonburg, VA; • **Must possess and maintain a TOP SECRET SCI level clearance without waiver or conditions**

Classified Systems and SCIF Support	Provide Classified ISSO Support for USCIS classified applications or systems; Provide Desktop support services to users within the SCIF on unclassified and classified networks. (3 CFTE)	• Each contractor in this task area shall have and maintain at least one (1) active certification such as but not limited to Network+, Security+, CASP, GSEC, GSLC, CISSP, CEH, CISM, CISA or other comparable certification or experience which must be approved in advance by the Government on a case-by-case basis. • Each Contractor in this task area shall have at least three (3) years of specialized experience in one of the below positions: Information Systems Security Officer, Information Systems Security Engineer, Information Systems Security Auditor or Information Systems Security Manager. • Each contractor in this task area shall have a minimum of three (3) years of experience with analyzing, assessing and implementing corrective actions based on vulnerability management tools. • Shall be proficient in providing workstation level desktop support • In depth knowledge of Microsoft Windows operating environment with Administrator level access • Each contractor in this task area shall have a minimum of three (3) years of experience with leading projects, technical writing, administrative tasks, and conducting briefings. • Contractor shall be staff in Washington, D.C., Atlanta, GA, Lee Summit, MO and the ability to travel to Harrisonburg, VA on an as needed basis; • **Must possess and maintain a TOP SECRET/SCI level clearance; without waiver or conditions**

Labor Category	Role on the Program	Required Certification(s)/ Experience
Security Control Assessment	Perform assessments USCIS application and system controls. Provides reports to support USCIS Risk Management Program. (4 CFTE)	• Each contractor in this task area shall have and maintain at least one (1) active certification such as but not limited to Security+, CASP, GSEC, GSLC, CISSP, CEH, CISM, CISA or other comparable certification or experience which must be approved in advance by the Government on a case-by-case basis. • Each Contractor in this task area shall have at least three (3) years of specialized experience in one of the below positions: Information Systems Security Officer, Information Systems Security Engineer, Information Systems Security Auditor or Information Systems Security Manager. • Each contractor in this task area shall have a minimum of three (3) years of experience with analyzing, assessing and implementing corrective actions based on vulnerability management tools. • Each contractor in this task area shall have a minimum of three (3) years of experience with leading projects, technical writing, administrative tasks, and conducting briefings. • Contractor shall be staffed in Washington, D.C. and must be able to attain up to a SECRET level clearance.

Labor Category	Role on the Program	Required Certification(s)/ Experience
Governance Program Support	Supports the SGB Governance Program (1 CFTE)	• Each contractor in this task area shall have Bachelor's degree. • Each contractor in this task area shall have experience with leading projects, technical writing, administrative tasks, and conducting briefings with a strong focus on writing IT Security policies and procedures. • Each contractor in this task area shall have advanced Microsoft Excel and Access skills to perform extensive data mining, correlation and reporting. • Contractor shall be staffed in Washington, D.C.

Labor Category	Role on the Program	Required Certification(s)/ Experience
TACCOM Program Support	Supports the USCIS TACCOM Program. Manages radio training Program. Installs radio and antenna systems. Programs and manages handheld radios Researches telecommunication technology. Creates TACCOM related policy documents and training material. Alternate COMSEC Custodian.	• TACCOM Engineer shall each have and maintain at least one (1) active certifications: Network+, Security+, ISC2 CISSP or other comparable certification which must be approved in advance by the PM on a case-by-case basis; • BS or minimum of six (6) years of experience with HF, UHF/VHF radio operations and maintenance, base station and mobile radio installation, engineering, frequency management, antenna selection/installation/repair, • Must be proficient using Software Defined Radios (SDR) and IP based radio systems, • Must be proficient using Motorola CPS (or similar) radio programing software, • Must be proficient in developing and maintaining custom radio Code-Plugs for Motorola handheld portable radios, • Must be proficient using antenna modeling software, for example EZNEC or similar, • Must be familiar with Communications Security (COMSEC) policy, procedures and safeguards. Must be familiar with KY-99A and Ky-100 key loading devices, • **Shall possess and maintain a Top Secret National Security Clearance.** • Located in Washington, D.C. • Occasional travel outside the NCR.

Labor Category	Role on the Program	Required Certification(s)/ Experience
Training Expert	Learning, training and knowledge management services to develop, deliver, track and memorialize information security education and training efforts to ensure the dissemination and enforcement of policies, practices, and procedures as required and mandated by USCIS, DHS, NIST and FISMA.	• Each contractor in this task area shall be a Level II • A minimum of five (5) years of experience coordinating, developing, and maintaining training course materials, briefs, and reports. • The above contractor shall have senior level experience with leading projects, technical writing, administrative tasks, and conducting briefings. • The above contractor shall have advanced Microsoft Excel and Access skills to perform extensive reporting. • The above contractor shall have extensive experience with graphic design and development of Section 508 complaint training applications containing static graphics, active animations, video, and voice course content using a variety of common off-the-shelf training development tools such as but not limited to Adobe Captivate. • A minimum of five (5) years of experience with data mining, extracting, correlating, analyzing, and compiling complex data sets from various sources utilizing advanced functions in Excel and Database tools. • The above contractor shall also have extensive experience developing, administering, and maintaining SharePoint sites to include webpages, user permissions, lists and reports, file libraries, surveys, and dashboards.

4.3.2 CONTRACTOR STAFF

The contractor shall determine the labor mix for the team to provide the best overall solution to the government.

The contractor's work shall conform to the Task Order provided by USCIS and the agile processes set up by USCIS but managed by the team. The team must have all of the skills necessary to perform the tasks stated in this SOW. It is important that the team as a whole has the skills necessary to complete the work. Most team members should have more than one skill.

4.4 GOVERNMENT FURNISHED PROPERTY

USCIS will provide contractor staff with Government furnished property to include Windows laptop for the PM and contract staff. Reporting, tracking and proper handling is the responsibility of the contractor. The Government has the right to implement Workplace as a Service (WPaaS) in lieu of providing GFP or as a replacement for existing GFP at its discretion during the life of the contract.

Equipment/ Government Property	Date/Event Indicate when the GFP will be furnished	Date/Event Indicate when the GFP will be returned	Unit	Unit Cost	Quantity*	Manufacture & Model Number	"As -is"
Laptop computer with power cord	After EOD	Upon departure	EA	$1,800	20	Dell Latitude 5490	Yes
PIV card	After EOD	Upon departure	EA	$500	20	-	Yes

*Quantity reflects the entire task order to include optional CLINS

The Government will not be obligated to provide additional accessories for the laptop computers, such as monitors, computer bags, external mice, etc. The Contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation, or rehabilitation costs. The Contractor will be responsible for receipt, stewardship, and custody of the listed GFP until formally relieved of responsibility in accordance with FAR 52.245-1 *Government Property* and FAR 52.245-9 *Use and Charges*. The property may not be

used for any purpose unrelated to the GCACS task order. The Contractor bears full responsibility for any and all loss of this property, whether accidental or purposeful, at full replacement value.

4.5 GOVERNMENT FURNISHED INFORMATION

USCIS will grant access to the tools and software that is required to perform all tasks. The USCIS federal managers will work closely with the contractor team to provide oversight and guidance to achieve the goals of the program.

Informational Resource/ Systems	Date/Event Indicate when the SW will be furnished	Date/Event Indicate when the SW will be returned
System access – contractor staff will be provided access to USCIS systems and tools. Access will be provided to staff based on job duties	Upon authorized EOD and full BI adjudication (required for access to Prod environment)	Access will be terminated upon contractor departure
DHS, USCIS intranet and email system	Upon EOD	Access will be terminated upon contractor departure

The Contractor will be exposed to additional informational resources while working with USCIS, such as DHS and USCIS policies and management directives, informational meetings, demonstrations by other programs and vendors, business SOPs, etc.

4.6 HOURS OF OPERATION

The Contractor shall be available during normal business hours for the Government, between 8am to 5pm, Monday through Friday, excluding Federal Government holidays. This time period includes a 1-hour unpaid lunch period.

The Government requires the Contractor to manage the hours in which staff operates so that service is provided when required within normal business hours. At times, based on the needs of the mission, the Government will require service outside of the normal duty hours and upon COR/PM direction, and given an advanced notice if possible, the contractor shall work weekends and Government holidays.

4.7 TELEWORK

Telework is authorized in support of this effort based on the contractor's telework guidance after review and acceptance of the Contractor's Corporate Telework Plan by the Contracting Officer. The Contractor's Corporate Telework Plan is due at the kick-off meeting. Before beginning to telework, all employees shall complete the annual Computer Security Awareness Training (CSAT) requirement, access to which shall be provided by USCIS.

4.8 TRAVEL

Travel within the local commuting area will not be reimbursed. For the purpose of this Task Order the local commuting area is defined as a fifty (50) mile radius from the primary place of performance. For contractor personnel who work on-site in USCIS offices, the local commuting area is defined as a fifty (50) mile radius from the USCIS site. Home to work travel is not reimbursable. All travel shall be at the Government's direction and shall be preapproved by the COR in writing 14 days before execution. Travel is only authorized for mission-specific requirements (NOT professional development).

Travel will not be reimbursed at more than applicable rates cited in the Federal Travel Regulation, 41 Code of Federal Regulations (CFR), Chapters 300 through 304 prescribed by the General Services Administration, for travel in the conterminous 48 United States, unless one of the exceptions identified in the code are applicable. Travel will be reimbursed in accordance with FAR subsection 31.205-46, Travel Costs and the General Services Administration's Federal Travel Regulations. The contractor shall include receipt(s) with the approved corresponding travel request(s) for all reimbursables at the time of invoicing. The invoice for travel must be submitted within 30 days from date of travel.

4.9 ACCESSIBILITY REQUIREMENTS – SECTION 508

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-

vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

Item that contains Information and Communications Technology (ICT): Deliverable documents and reports

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including Electronic documents; Electronic forms): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

Applicable 508 requirements for software features and components (including Electronic content and software authoring tools and platforms; Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, and 504 Authoring Tools

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Collaboration environments

Applicable Exception: N/A Authorization #: N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including Electronic documents; Electronic forms): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

Applicable 508 requirements for software features and components (including Electronic content and software authoring tools and platforms; Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, and 504 Authoring Tools

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

2. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.

3. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/compliance-test-processes.

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

5. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall

be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

6. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

Instructions to Offerors

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.0 508 (or later). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed in accordance with all the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Supports", "Supports with Exceptions", "Does Not Support", and "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each ICT Item that will be developed, modified, installed, configured, integrated, maintained, or hosted by the contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.

3. For each commercially available authoring tool offered that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Offeror shall describe the level of Section 508 compliance supported for the content that can be generated.

Acceptance Criteria

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:
    - Accessibility test results based on the required test methods.
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).
2. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

4.10 SECURITY REQUIREMENTS

4.10.1 APPLICABLE POLICIES AND REFERENCES

The Contractor shall be subject to all current and future versions of DHS Sensitive Systems Policy Directive 4300A, DHS National Security Systems Policy 4300B, DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, the annual DHS Information Security Performance Plan, National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series, Federal Information Processing Standards (FIPS) and all associated USCIS policies including all associated attachments, concepts of operation (CONOPS), processes and standard operating procedures. Documents which are not publicly available will be provided to the selectee upon contract award.

All efforts described above shall be conducted in accordance with established Federal statutory requirements (e.g. 1996 Federal Clinger-Cohen Act (CCA), Section 508 of the 1998 Federal Rehabilitation Act, FISMA), departmental regulatory guidelines (e.g. DHS Acquisition Management Directive 102-1, USCIS Systems Engineering Life Cycle (SELC) guide), and through use of the industry's best practices for Information Technology Security Authorization activities.

4.10.2 DHS ENTERPRISE ARCHITECTURE COMPLIANCE

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

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

All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile; all products are subject to DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the HLS EA TRM Standards and Products Profile.

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

Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

G-CACS DELIVERABLES

The table below aggregates all the deliverables that are required for this task order.

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1	Daily Stand Up	Discuss daily progress of the sprint, blockers, etc.	Daily
3.1	Sprint Review	Demonstrate work that was completed in the sprint; explain work that was not able to be completed	Every two (2) weeks
3.1	Burn Up Charts	Explain status of team progress against the scope of work	Every two (2) weeks at Sprint Review
3.1	Sprint Retrospective	Discuss the sprint, blockers, what went well, etc, and use this info to continue to improve performance	Every two (2) weeks after Sprint Review
3.1	Sprint Planning	Establish sprint goals, plan, and prioritize the work to be accomplished in the upcoming sprint including stretch goals	Every two (2) weeks after Sprint Review
3.1	Backlog Grooming	Groom and prioritize upcoming work and include dependencies	As needed, usually weekly
3.1	Team Lead Check In	Discuss the progress of the overall program, Government's level of satisfaction with the contractor and any issues that need to be addressed; Plan for upcoming meetings or activities, discuss personnel changes	Every two (2) weeks, or as needed
3.1	Jira Confluence Wiki	Update project documents on the Jira Confluence Wiki on daily basis	Confluence Wiki

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1	Release Planning Review and Post Implementation Review Documentation	Update documentation; Attend the RPR/PIR meeting	As needed
3.1	Project Management Plan	A Project Management Plan that facilitates its implementation of continuous delivery precepts describing the technical approach, organizational resources, and management controls they will employ to meet the cost, performance and schedule requirements throughout SOW execution	Initial: Within 30 days after Authority to Work Ad Hoc: As major changes occur

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1	Transition-Out Plan	An outgoing Transition Plan, transitioning work from the Contractor to the Government. The Transition Plan shall include, but not be limited to: • Coordination with Government representatives; • Review, evaluation, and transition of current Contractor support services; • Transition of historical data • Transition of Government-approved Contractor training materials and certification process documentation; • Transfer of all necessary business and/or technical documentation • Transfer of compiled and un-compiled source code, to include all versions, maintenance updates, and patches; • Transfer of the GFE inventory management system, all user and maintenance documentation, and current GFE information in the system; • Facilitation of applicable Government debriefings and personnel out-processing procedures; and • Turn-in of all Government keys, identification and access cards, and security codes; • Any other information as requested by the Government.	No later than eight (8) weeks prior to end of final period of performance

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1	Communications Plan	A Communications Plan illustrating how the Contractor communicates with the Government (including the Government PM, COR and CO). This Communication Plan shall include regular communications, work products, and communications during an emergency (such as a natural disaster or national emergency).	Within 30 days after Authority to Work
3.1	Quality Control Plan	The Quality Control Plan provides a systematic method to ensure performance standards for the stated contract.	Within 30 days of Authority to Work Template will be provided after the Kick-Off meeting

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1 – 4.6	Risk Management Plan	The Risk Management Plan shall address what risks the Contractor has identified, risk validation, the estimated impact of these risks, a response to these issues, and estimated timeframe for resolution of risk(s). As it relates to risk validation and events detection, the Contractor's Risk Management Plan shall include a plan of action for issue validation including the following: • Verifying that an actual event (risk) exists including a written plan detailing their validating process. (The Contractor shall notify the Government PM when updating or changing the validation process.) • Reporting time: contractor shall report all known events within twenty-four (24) hours of known issue, risk and/or event • At a minimum who the incident report needs to go to including key government personnel The Contractor shall also describe its Risk Management plan for addressing unforeseen risks.	Initially, within 30 days of contract award, and upon contractor recognizing a new risk thereafter
3.1 – 4.7	Risk Register	As risks are identified, the contractor shall log them on the register as well as the actions taken to respond to the risk. Risks may be applicable to all sections of the SOW. An acceptable format may be determined by the Government PM after the Kick-Off Meeting.	Initial: Within 30 days of contract award Weekly and upon contractor recognizing a new risk thereafter

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1	Continuous Training Plan	A Training Plan for new employees and to refresh the technical skills of its staff. The contractor shall ensure all system users receive the initial computer security awareness training within 24 hours of their first log in, and annually thereafter. The contractor shall ensure personnel with significant security responsibilities (privileged users/administrators) receive the initial specialized role-based training specific to their security responsibilities, and annually thereafter. The contractor shall report quarterly on security training compliance. The Government will not allow costs, nor reimburse costs associated with the contractor training employees to attain and/or maintain personnel qualification requirements listed in the SOW. Training and associated travel costs shall not be charged to the Government.	Quarterly

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1	Weekly Status Report	The Weekly Status Report (WSR) shall include: • Summary of weekly project and program activities • List of tasks assigned by functional area and team • List of accomplishments and completed tasks and work products by functional area and team • Performance Metrics with status of projects by functional area and team via JIRA/ Confluence reports • Outstanding project concerns • Activities planned for the upcoming week by functional area and team • Staffing Performance Measure: List of all required positions mapped to contractor names with work status (active or vacant) and labor category by functional area and team • Progress on staffing plan to include status on entry on duty (EOD) and training requirements An acceptable format may be determined by the Government PM after the Kick-Off Meeting.	At the end of each week

3.1	Monthly Status Report	The Monthly Status Report (MSR) shall include: • Performance Summary: A summary of work activities by functional area and team completed for the month along with the degree of government technical direction required to solve issues or events. If government technical direction was needed to meet a SOW requirement, an explanation was to why the contractor was unable to provide that requirement and the anticipated date the contractor will meet that requirement. The Performance Summary includes documenting any major risks and/or issues and any significant progress and events. • Progress and Events: includes the delivery of documents, artifacts, and reports. The summary should provide enough detail for the reader with limited familiarity with the SOW to comprehend the value that the Contractors are providing to the USCIS Risk Management Program. • Resource Expenditures: Resource expenditures track funds expended during the reporting period and their purpose in order to understand the burn rate and provide fiscal accountability to external stakeholders. For firm fixed price contracts the resource expenditures are used for Internal Use reporting purposes and in order to measure hours expended. • Quality and Standards Adherence Performance Measure: A summary of documents and work products submitted to the Government by functional area and team during the month. A summary of documents and work products submitted to the Government which required more	Monthly, By the 10th of every month with the invoice

Work Products			
Reference	**Requirement**	**Description**	**Interval**
		than two Government reviews to achieve Government acceptance. An acceptable format may be determined by the Government PM after the Kick-Off Meeting.	
3.1	Program Management Review (PMR) Brief	The PMR brief shall provide a detailed overview of the contract's performance, accomplishments, risks and issues and planned projects. The PMR shall include, but is not limited to: • Prior month's performance, schedule, cost data and resource allocation; • Current month's performance, schedule, cost data and resource allocation; • Schedule, cost data and resource allocation for planned projects/ initiatives; • Accomplishments; • Issues, including recommendations for resolution; and • Identified risks and mitigation actions taken. An acceptable format may be determined by the Government PM after the Kick-Off Meeting.	Beginning of each month, reporting in arrears
3.1.2	Stakeholder Engagement Strategy	The Strategy shall include, but is not limited to, a stakeholder engagement model for each RMB functional area to inform internal (USCIS) and external customers on how to engage with RMB teams and comply with federally mandated DHS' Information Security Program policies, procedures, standards, and guidelines.	To be determined by the Government PM after the Kick-Off Meeting

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1.2	Standard Operating Procedures (SOPs)	The SOPs shall include, but are not limited to, detailed processes and procedures for each functional area.	Initially: To be determined by the Government PM after the Kick-Off Meeting Updated as changes occur thereafter
3.1.2	Notices to Stakeholders	The notifications shall include, but are not limited to, communications to keep stakeholders informed when there are changes to any of the Risk Management functional areas. Notifications will be drafted in coordination with the Government PM and/or staff.	As Needed
3.1.3	Gap Analysis Discoveries Report	The report shall document the discoveries from the Risk Management Program Gap Analysis which may include, but are not limited to: • An overview of the discovered findings • An explanation for why the gaps exists • Recommended mitigation/ action • Projected costs/ resources required for remediation An acceptable format may be determined by the Government PM after the Kick-Off Meeting.	To be determined by the Government PM after the Kick-Off Meeting

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1.2	Quarterly Gap Analysis Report	The Gap Analysis Report shall document discoveries which may include, but are not limited to: • Duplication of effort • Improvements to streamline processes/ procedures • Manual processes to be automated • Areas in which significant effort outweighs the return on investment • Recommended mitigation/ action An acceptable format may be determined by the Government PM after the Kick-Off Meeting.	Beginning of each quarter, reporting in arrears

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.1, 3.2, 3.3	Status Briefings/ Executive Reports/ Work Products	As required by the COR, USCIS Government PM or Federal Function Lead, the Contractors shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work objectives that require USCIS attention. The meetings may be scheduled regularly or may be adhoc. In the event the Government requires additional information related to contract technical, cost, or schedule performance, risks, resources, or any contract-related data, the Contractors shall provide this report /information in the format requested by the Government. Requests for adhoc reporting may vary in scope and complexity and may require the Contractors to attend OIT meetings to obtain required information, review and research applicable documentation, and extract applicable data required to assemble the adhoc report. Acceptable formats will be determined by the Government PM or staff.	As Requested by the Government

Work Products			
Reference	**Requirement**	**Description**	**Interval**
3.2	SCA Deliverables	Deliverables to align with tasking requirements in Section 3.2. This may include, but not limited to: • SCA Data Trending Slide • System / Program Briefing Reports • System Risk Analysis Reports • Security Authorization Documentation Tracking Reports • FISMA Inventory documentation • Weakness Remediation Reports • Waiver Tracking Reports	Various
4.3.1	Key Personnel Qualifications	A statement of qualifications and resume for all proposed Key personnel. This document should reference the section of the resume for applicable experience.	Within 10 days of contract award and within 10 days of each change
4.4	Government Furnished Property Report	The report shall be submitted to the COR and Contracting Officer on DHS Form 700-5 *Contractor Report of Government Property*.	Within 90 days after contract award and as changes occur thereafter
4.7	Telework Plan	The Contractor's Corporate Telework Plan is due at the kick-off meeting. Prior to commencement of teleworking activities, the Contractor shall provide the USCIS Government PM and COR a listing of personnel proposed to telework, along with identified objectives to be performed, for approval. Telework shall be considered a privilege, not a right, and shall not impact contractor's productivity or ability to satisfy any requirement in the SOW.	During the Kick-Off Meeting