

**SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS**

1. REQUISITION NUMBER

PAGE OF PAGES

**OFFEROR TO COMPLETE BLOCKS 12,17,23,24, & 30**

1 2

2. CONTRACT NO. 70B02C20D00000019	3. AWARD/EFF. DATE 07/02/2020	4. ORDER NUMBER	5. SOLICITATION NUMBER 70B02C20Q00000188	6. SOLICITATION ISSUE DATE
--------------------------------------	----------------------------------	-----------------	---	----------------------------

7. FOR SOLICITATION INFORMATION CALL: <b>(b) (6), (b) (7)(C)</b>	8. OFFER DUE DATE/ LOCAL TIME
---	-------------------------------

9. ISSUED BY DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave., NW NP 1310 Washington DC 20229	10. THIS ACQUISITION IS <input checked="" type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> UNRESTRICTED OR <input checked="" type="checkbox"/> SET ASIDE: _____ % FOR: <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> EDWOSB <input type="checkbox"/> 8(A) NAICS: 541512 SIZE STANDARD:
--	---

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE	12. DISCOUNT TERMS Within 30 days Due net	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/> 13b. RATING	14. METHOD OF SOLICITATION <input checked="" type="checkbox"/> RFQ <input type="checkbox"/> IFB <input type="checkbox"/> RFP
--	--	--	---

15. DELIVER TO See Attached Delivery Schedule	16. ADMINISTERED BY DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave., NW NP 1310 Washington DC 20229
--	---

17a. CONTRACTOR/ OFFEROR ANDURIL INDUSTRIES INC 2722 MICHELSON DR IRVINE CA 92612-1603 TELEPHONE NO.	18a. PAYMENT WILL BE MADE BY DHS - Customs & Border Protection Commercial Accounts Sect. 6650 Telecom Drive, Suite 100 Indianapolis IN 46278
--	--

<input checked="" type="checkbox"/> 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. <input checked="" type="checkbox"/> SEE ADDENDUM
--	--

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
10	O&S (Land Tower/Maritime/Ghost/Dust)	1.000	AU		
20	New capabilities, Training & Trvl	1.000	AU		
30	Land Tower Procurement	1.000	AU		
40	Maritime/Ghost/Dust UGS Pilots	1.000	AU		

25. ACCOUNTING AND APPROPRIATION DATA N/A	26. TOTAL AWARD AMOUNT (For Govt Use Only) \$0.00
--	--

<input checked="" type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.	<input type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.
--	--

<input checked="" type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN <u>1</u> 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 HEREIN.	<input checked="" type="checkbox"/> 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____ YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: _____
--	---

30a. SIGNATURE OF OFFEROR/CONTRACTOR <b>(b) (6), (b) (7)(C)</b>	31c. DATE SIGNED
--	------------------

**(b) (6), (b) (7)(C)**

(TYPE OR PRINT)

CONTRACT NO.: 70B02C20D00000019	REQUISITION NUMBER	AWARD/EFF. DATE 07/02/2020
------------------------------------	--------------------	-------------------------------

## ADDITIONAL INFORMATION:

The Department of Homeland Security, Customs and Border Protection (CBP) hereby issues an Indefinite Delivery Indefinite Quantity (IDIQ) Contract with Firm Fixed Price Contract Line Items to Anduril Industries for the procurement of up to 170 Autonomous Surveillance Tower Systems (AST's). The Contractor shall provide the AST's in accordance with the Statement of Work and Performance Specifications attached hereto.

This sole source award is a Small Business Innovative Research (SBIR) directed procurement pursuant to the Small Business Innovative Research and Small Business Technology Transfer (STTR) Program Directive.

There are four Ordering Periods, which are detailed as follows:

Base Period: July 2, 2020 - July 1, 2021  
Option Period 1: July 2, 2021 - July 1, 2022  
Option Period 2: July 2, 2022 - July 1, 2023  
Option Period 3: July 2, 2023 - July 1, 2024  
Option Period 4: July 2, 2024 - July 1, 2025

The Ceiling Price for this IDIQ contract is \$249,550,000.00. The minimum guarantee is 5 AST's and is effective for the Base Ordering Period only.

The Government's rights in computer software delivered, generated, or accessed in performance of this Agreement will be governed solely by the rights and restrictions identified in FAR 52.227-19. The Government will also only have limited rights in any limited rights data that the Contractor delivers under this Agreement and marks accordingly. Otherwise, the Government's rights in technical data will be governed by FAR 52.227-20.

The Contract Officer Representative's name and contact information is as follows:

(b) (6), (b) (7)(C)

32a. QUANTITY IN COLUMN 21 HAS BEEN <input type="checkbox"/> RECEIVED <input type="checkbox"/> INSPECTED <input type="checkbox"/> ACCEPTED AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED					
32b. SIGNATURE OF AUTHORIZED GOVT. REPRESENTATIVE		32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE			32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
			32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
33. SHIP NUMBER <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL		34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	
37. CHECK NUMBER					
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY			
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT			42a. RECEIVED BY (Print)		
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER		41c. DATE	42b. RECEIVED AT (Location)		
			42c. DATE REC'D (YY/MM/DD)		42d. TOTAL CONTAINERS

## TABLE OF CONTENTS

SECTION I	SCHEDULES .....	3
I.1	SCHEDULE OF SUPPLIES/SERVICES.....	3
I.2	ACCOUNTING and APPROPRIATION DATA.....	6
I.3	DELIVERY SCHEDULE.....	6
SECTION II	CONTRACT CLAUSES.....	7
II.1	52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) .....	7
II.2	52.203-17 CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (APR 2014).....	7
II.3	52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011) 7	7
II.4	52.204-13 SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (OCT 2018).....	7
II.5	52.204-18 COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (JUL 2016) .....	7
II.6	52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (OCT 2018).....	7
II.7	52.216-18 ORDERING (OCT 1995).....	7
II.8	52.216-19 ORDER LIMITATIONS (OCT 1995) .....	7
II.9	52.216-22 INDEFINITE QUANTITY (OCT 1995).....	8
II.10	52.227-20 Rights in Data-SBIR Program (May 2014).....	8
II.11	52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984) .....	10
II.12	3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012) .....	10
II.13	52.204-23 - PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018) (DEVIATION 20-05) 11	11
II.14	52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TLELCOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 2020-05).....	12
II.15	52.215-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS -- COMMERCIAL ITEM (JUN 2020) .....	14
II.16	52.217-6 Option for Increased Quantity (MAR 1989) .....	20
II.17	52.217-7 Option for Increased Quantity-Separately Priced Line Item (MAR 1989).....	20
II.18	52.217-9 Option to Extend the Term of the Contract (Mar 2000) .....	20
II.19	52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013) 20	20
II.20	52.244-6 SUBCONTRACTS FOR COMMERCIAL ITEMS (AUG 2019).....	21
II.21	CONTRACT TYPE (OCT 2008).....	22
II.22	SPECIFICATIONS, STATEMENT OF WORK, STATEMENT OF OBJECTIVES OR PERFORMANCE WORK STATEMENT ATTACHED (JUN 2013).....	22
II.23	PERIOD OF PERFORMANCE (MAR 2003).....	22
II.24	CONTRACTING OFFICER'S AUTHORITY (MAR 2003) .....	22
II.25	ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016).....	22
II.26	GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003).....	23
II.27	SECURITY PROCEDURES (APR 2019).....	23
II.28	GOVERNMENT PROPERTY (MAR 2003) .....	25
II.29	SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011) .....	25
II.30	SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015).....	26

II.31 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015) ..... 32

## SECTION I SCHEDULES

## I.1 SCHEDULE OF SUPPLIES/SERVICES

IDIQ MINIMUM GUARANTEE: 5 ASTs (During Base Ordering Period)

IDIQ MAXIMUM QUANTITY: UP TO 170 ASTs

TOTAL IDIQ CONTRACT CEILING PRICE (ALL ORDERING PERIODS): \$ 249,550,000.00

Total Funded Value of Award: \$0.00

Total Funded Value of IDIQ Contract Award: \$0.00

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	O&S (Land Tower/Maritime/Ghost/Dust)	1.000	AU	\$0.00	\$0.00
20	New capabilities, Training & Trvl	1.000	AU	\$0.00	\$0.00
30	Land Tower Procurement	1.000	AU	\$0.00	\$0.00
40	Maritime/Ghost/Dust UGS Pilots	1.000	AU	\$0.00	\$0.00

ORDERING PERIOD (BASE PERIOD): 07/02/2020 THROUGH 07/01/2021

ITEM DESCRIPTION	QTY	TYPE	UNIT	UNIT PRICE	TOTAL PRICE
CLIN 0001: AUTONOMOUS SENTRY TOWER KIT OR LOOKOUT KIT, LAND BASED	142	FFP	EACH	(b) (4)	(4)
CLIN 0002: AUTONOMOUS SENTRY TOWER, MARINE BASED	3	FFP	EACH	(b) (4)	(4)
CLIN 0003: SUAS GHOST CAPABILITY	0	FFP	EACH	(b) (4)	(4)
CLIN 0004: AUTONOMOUS GROUND SENSOR DUST	0	FFP	EACH	(b) (4)	(4)
CLIN 0005: AUTONOMOUS SENTRY TOWER KIT, LAND BASED - O&S	60	FFP	EACH	(b) (4)	(4)
CLIN 0006: AUTONOMOUS SENTRY TOWER, MARINE BASED - O&S	1	FFP	EACH	(b) (4)	(4)
CLIN 0007: SUAS GHOST CAPABILITY - O&S	7	FFP	EACH	(b) (4)	(4)
CLIN 0008: AUTONOMOUS GROUND SENSOR DUST - O&S	0	FFP	EACH	(b) (4)	(4)
CLIN 0009: NEW CAPABILITIES DEVELOPMENT	0	FFP	EACH	(b) (4)	(4)
CLIN 0010: TRAINING/SUPPORT/PROFESSIONAL SERVICES	0	FFP	EACH	(b) (4)	(4)
CLIN 0011: TRAVEL (Not To Exceed)	0	NTE		(b) (4)	(4)
CLIN 0012: TOWER RELOCATION FEE	0	FFP	EACH	(b) (4)	(4)
CLIN 0013: COMPLEX COMMUNICATIONS PACKAGE	0	FFP	EACH	(b) (4)	(4)

ORDERING PERIOD (OPTION PERIOD 1) 07/02/2021 THROUGH 07/01/2022

ITEM DESCRIPTION	QTY	TYPE	UNIT	UNIT PRICE	TOTAL PRICE
CLIN 0101: AUTONOMOUS SENTRY TOWER KIT OR LOOKOUT KIT, LAND BASED	0	FFP	EACH	(b) (4)	(4)
	0			(b) (4)	(4)
CLIN 0102: AUTONOMOUS SENTRY TOWER, MARINE BASED		FFP	EACH	(b) (4)	(4)
	0			(b) (4)	(4)

CLIN 0103: SUAS GHOST CAPABILITY		FFP	EACH
CLIN 0104: AUTONOMOUS GROUND SENSOR DUST	0	FFP	EACH
CLIN 0105: AUTONOMOUS SENTRY TOWER KIT, LAND BASED - O&S	201	FFP	EACH
CLIN 0106: AUTONOMOUS SENTRY TOWER, MARINE BASED – O&S	4	FFP	EACH
CLIN 0107: SUAS GHOST CAPABILITY – O&S	7	FFP	EACH
CLIN 0108: AUTONOMOUS GROUND SENSOR DUST - O&S	0	FFP	EACH
CLIN 0109: NEW CAPABILITIES DEVELOPMENT	0	FFP	EACH
CLIN 0110: TRAINING/SUPPORT/PROFESSIONAL SERVICES	0	FFP	EACH
CLIN 0111: TRAVEL (Not To Exceed)	0	NTE	
CLIN 0112: TOWER RELOCATON FEE	0	FFP	EACH
CLIN 0113: COMPLEX COMMUNICATIONS PACKAGE	0	FFP	EACH

## ORDERING PERIOD (OPTION PERIOD 2) 07/02/2022 THROUGH 07/01/2023

ITEM DESCRIPTION	QTY	TYPE	UNIT
CLIN 0201: AUTONOMOUS SENTRY TOWER KIT OR LOOKOUT KIT, LAND BASED	0	FFP	EACH
CLIN 0202: AUTONOMOUS SENTRY TOWER, MARINE BASED	0	FFP	EACH
CLIN 0203: SUAS GHOST CAPABILITY	0	FFP	EACH
CLIN 0204: AUTONOMOUS GROUND SENSOR DUST	0	FFP	EACH
CLIN 0205: AUTONOMOUS SENTRY TOWER KIT, LAND BASED - O&S	201	FFP	EACH
CLIN 0206: AUTONOMOUS SENTRY TOWER, MARINE BASED – O&S	4	FFP	EACH
CLIN 0207: SUAS GHOST CAPABILITY – O&S	7	FFP	EACH
CLIN 0208: AUTONOMOUS GROUND SENSOR DUST - O&S	0	FFP	EACH
CLIN 0209: NEW CAPABILITIES DEVELOPMENT	0	FFP	EACH
CLIN 0210: TRAINING/SUPPORT/PROFESSIONAL SERVICES	0	FFP	EACH
CLIN 0211: TRAVEL (Not To Exceed)		NTE	
CLIN 0212: TOWER RELOCATON FEE	0	FFP	EACH

(b) (4)

CLIN 0213: COMPLEX COMMUNICATIONS PACKAGE	0	FFP	EACH
---	---	-----	------

(b) (4)

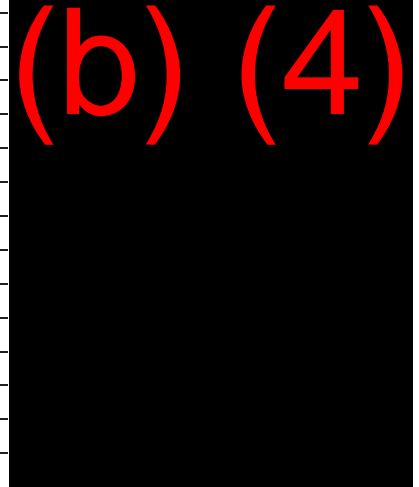
**ORDERING PERIOD (OPTION PERIOD 3) 07/02/2023 THROUGH 07/01/2024**

ITEM DESCRIPTION	QTY	TYPE	UNIT
CLIN 0301: AUTONOMOUS SENTRY TOWER KIT OR LOOKOUT KIT, LAND BASED	0	FFP	EACH
CLIN 0302: AUTONOMOUS SENTRY TOWER, MARINE BASED	0	FFP	EACH
CLIN 0303: SUAS GHOST CAPABILITY	0	FFP	EACH
CLIN 0304: AUTONOMOUS GROUND SENSOR DUST	0	FFP	EACH
CLIN 0305: AUTONOMOUS SENTRY TOWER KIT, LAND BASED - O&S	201	FFP	EACH
CLIN 0306: AUTONOMOUS SENTRY TOWER, MARINE BASED – O&S	4	FFP	EACH
CLIN 0307: SUAS GHOST CAPABILITY – O&S	7	FFP	EACH
CLIN 0308: AUTONOMOUS GROUND SENSOR DUST - O&S	0	FFP	EACH
CLIN 0309: NEW CAPABILITIES DEVELOPMENT	0	FFP	EACH
CLIN 0310: TRAINING/SUPPORT/PROFESSIONAL SERVICES	0	FFP	EACH
CLIN 0311: TRAVEL (Not To Exceed)		NTE	EACH
CLIN 0312: TOWER RELOCATION FEE	0	FFP	EACH
CLIN 0313: COMPLEX COMMUNICATIONS PACKAGE	0	FFP	EACH

**ORDERING PERIOD (OPTION PERIOD 4) 07/02/2024 THROUGH 07/01/2025**

ITEM DESCRIPTION	QTY	TYPE	UNIT
CLIN 0401: AUTONOMOUS SENTRY TOWER KIT OR LOOKOUT KIT, LAND BASED	0	FFP	EACH
CLIN 0402: AUTONOMOUS SENTRY TOWER, MARINE BASED	0	FFP	EACH
CLIN 0403: SUAS GHOST CAPABILITY	0	FFP	EACH
CLIN 0404: AUTONOMOUS GROUND SENSOR DUST	0	FFP	EACH
CLIN 0405: AUTONOMOUS SENTRY TOWER KIT, LAND BASED - O&S	201	FFP	EACH
CLIN 0406: AUTONOMOUS SENTRY TOWER, MARINE BASED – O&S	4	FFP	EACH

CLIN 0407: SUAS GHOST CAPABILITY – O&S	7	FFP	EACH
CLIN 0408: AUTONOMOUS GROUND SENSOR DUST - O&S	0	FFP	EACH
CLIN 0409: NEW CAPABILITIES DEVELOPMENT	0	FFP	EACH
CLIN 0410: TRAINING/SUPPORT/PROFESSIONAL SERVICES	0	FFP	EACH
CLIN 0411: TRAVEL (Not To Exceed)	0	NTE	
CLIN 0412: TOWER RELOCATION FEE	0	FFP	EACH
CLIN 0413: COMPLEX COMMUNICATIONS PACKAGE	0	FFP	EACH



IDIQ MINIMUM GUARANTEE: 5 ASTs (During Base Ordering Period)

IDIQ MAXIMUM QUANTITY: UP TO 170 ASTs

TOTAL IDIQ CONTRACT CEILING PRICE (ALL ORDERING PERIODS): \$ 249,550,000.00

Total Funded Value of Award: \$0.00

Total Funded Value of IDIQ Contract Award: \$0.00

### I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0935206110ZNV20500MA1100000000 970702525 TAS# 070202020 0530000	\$0.00
20	6100.2525USCSGLCS0935206110ZNV20560AB2000000000 BPE232525 TAS# 070202022 0532000	\$0.00
30	6100.2525USCSGLCS0935206110Z00020560AB200000ASTR BPE552525 TAS# 070202022 0532000	\$0.00
40	6100.2525USCSGLCS0935206110ZNV20560AB2000000000 BPE232525 TAS# 070202022 0532000	\$0.00

### I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 1331 Pennsylvania Avenue N W Washington, DC 20004	10	1.000	07/01/2021
	20	1.000	07/01/2021
Customs and Border Protection 1300 Pennsylvania Av, NW Washington, DC 20229	30	1.000	07/01/2021
	40	1.000	07/01/2021



## SECTION II CONTRACT CLAUSES

### II.1 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 a clause may be accessed electronically at this/these address(es):  
www.acquisition.gov

#### I. FEDERAL ACQUISITION REGULATION (48 CHAPTER 1) CLAUSES

NUMBER	TITLE
--------	-------

**II.2 52.203-17 CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (APR 2014)**

**II.3 52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011)**

**II.4 52.204-13 SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (OCT 2018)**

**II.5 52.204-18 COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (JUL 2016)**

**II.6 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (OCT 2018)**

**II.7 52.216-18 ORDERING (OCT 1995)**

- (a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued as follows:  
 Base Period – 07/02/2020 – 07/01/2021  
 Option Year 1 - 07/02/2021 – 07/01/2022  
 Option Year 2 - 07/02/2022 – 07/01/2023  
 Option Year 3 - 07/02/2023 – 07/01/2024  
 Option Year 4 - 07/02/2024 - 07/01/2025

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of clause)

**II.8 52.216-19 ORDER LIMITATIONS (OCT 1995)**

(a) *Minimum order.* When the Government requires supplies or services covered by this contract in an amount of less than 5 Autonomous Surveillance Tower Systems, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order.* The Contractor is not obligated to honor--

(1) Any order for a single item in excess of 170 Autonomous Surveillance Tower Systems;

(2) Any order for a combination of items in excess of 170 Autonomous Surveillance Tower Systems ; or

(3) A series of orders from the same ordering office within days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

- (d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

## **II.9 52.216-22 INDEFINITE QUANTITY (OCT 1995)**

- (a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.
- (b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."
- (c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.
- (d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract on delivery orders placed after 07/01/2025, if all options are exercised.

(End of clause)

## **II.10 52.227-20 Rights in Data-SBIR Program (May 2014)**

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

Computer database or "database" means a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

Computer software-

(1) Means.

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

Computer software documentation means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

Data means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing or management information.

Form, fit, and function data means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

Limited rights data means data (other than computer software) developed at private expense that embody trade secrets or are commercial or financial and confidential or privileged.

Restricted computer software means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

SBIR data means data first produced by a Contractor that is a small business concern in performance of a small business innovation research contract issued under the authority of 15 U.S.C. 638, which data are not

generally known, and which data without obligation as to its confidentiality have not been made available to others by the Contractor or are not already available to the Government.

SBIR rights means the rights in SBIR data set forth in the SBIR Rights Notice of paragraph (d) of this clause.

Technical data means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases. (See 41 U.S.C. 116.)

Unlimited rights means the right of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose whatsoever, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause regarding copyright, the Government shall have unlimited rights in-

(i) Data specifically identified in this contract as data to be delivered without restriction;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for SBIR data in accordance with paragraph (d) of this clause or for limited rights data or restricted computer software in accordance with paragraph (f) of this clause.

(2) The Contractor shall have the right to-

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Protect SBIR rights in SBIR data delivered under this contract in the manner and to the extent provided in paragraph (d) of this clause;

(iii) Substantiate use of, add, or correct SBIR rights or copyright notices and to take other appropriate action, in accordance with paragraph (e) of this clause; and

(iv) Withhold from delivery those data which are limited rights data or restricted computer software to the extent provided in paragraph (f) of this clause.

(c) Copyright-

(1) Data first produced in the performance of this contract.

(i) Except as otherwise specifically provided in this contract, the Contractor may assert copyright subsisting in any data first produced in the performance of this contract.

(ii) When asserting copyright, the Contractor shall affix the applicable copyright notice of 17 U.S.C. 401 or 402 and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up nonexclusive, irrevocable, worldwide license to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly, by or on behalf of the Government.

(2) Data not first produced in the performance of this contract. The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data that are not first produced in the performance of this contract unless the Contractor (i) identifies such data and (ii) grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause.

(3) Removal of copyright notices. The Government will not remove any copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) Rights to SBIR data.

(1) The Contractor is authorized to affix the following "SBIR Rights Notice" to SBIR data delivered under this contract and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of this clause, in accordance with the notice:

SBIR Rights Notice (Dec 2007)

These SBIR data are furnished with SBIR rights under Contract No. \_\_\_\_\_ (and subcontract \_\_\_\_\_, if appropriate). For a period of 4 years, unless extended in accordance with FAR 27.409(h), after acceptance of all items to be delivered under this contract, the Government will use these data for Government purposes only, and they shall not be disclosed outside the Government (including disclosure for procurement purposes) during such period without permission of the Contractor, except that, subject to the foregoing use and disclosure prohibitions, these data may be disclosed for use by support Contractors. After the protection period, the Government has a paid-up license to use, and to authorize others to use on its behalf, these data for Government purposes, but is relieved of all

disclosure prohibitions and assumes no liability for unauthorized use of these data by third parties. This notice shall be affixed to any reproductions of these data, in whole or in part.

(End of notice)

(2)The Government's sole obligation with respect to any SBIR data shall be as set forth in this paragraph (d).

(e)Omitted or incorrect markings.

(1)Data delivered to the Government without any notice authorized by paragraph (d) of this clause shall be deemed to have been furnished with unlimited rights. The Government assumes no liability for the disclosure, use, or reproduction of such data.

(2)If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense, and the Contracting Officer may agree to do so if the Contractor-

(i)Identifies the data to which the omitted notice is to be applied;

(ii)Demonstrates that the omission of the notice was inadvertent;

(iii)Establishes that the use of the proposed notice is authorized; and

(iv)Acknowledges that the Government has no liability with respect to the disclosure or use of any such data made prior to the addition of the notice or resulting from the omission of the notice.

(3)If the data has been marked with an incorrect notice, the Contracting Officer may-

(i)Permit correction of the notice at the Contractor's expense, if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii)Correct any incorrect notices.

(f) Protection of limited rights data and restricted computer software. The Contractor may withhold from delivery qualifying limited rights data and restricted computer software that are not identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall identify the data being withheld, and furnish form, fit, and function data instead.

(g) Subcontracting. The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and not proceed with the subcontract award without further authorization in writing from the Contracting Officer.

(h) Relationship to patents. Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of clause)

## **II.11 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)**

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of (DEVIATION) after the date of the clause.

(b) The use in this solicitation or contract of any clause with an authorized deviation is indicated by the addition of (DEVIATION) after the name of the regulation.

(End of clause)

## **II.12 3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)**

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

[The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]

(a) Provisions.

[ ] 3052.209-72 Organizational Conflicts of Interest.

[ ] 3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.

[ ] 3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

(b) Clauses.

3052.203-70 Instructions for Contractor Disclosure of Violations.

3052.204-70 Security Requirements for Unclassified Information Technology Resources.

3052.204-71 Contractor Employee Access.

Alternate I

3052.205-70 Advertisement, Publicizing Awards, and Releases.

3052.209-73 Limitation on Future Contracting.

3052.215-70 Key Personnel or Facilities.

3052.216-71 Determination of Award Fee.

3052.216-72 Performance Evaluation Plan.

3052.216-73 Distribution of Award Fee.

3052.219-70 Small Business Subcontracting Plan Reporting.

3052.219-71 DHS Mentor Protégé Program.

3052.228-70 Insurance.

3052.236-70 Special Provisions for Work at Operating Airports.

3052.242-72 Contracting Officer's Technical Representative.

3052.247-70 F.o.B. Origin Information.

Alternate I

Alternate II

3052.247-71 F.o.B. Origin Only.

3052.247-72 F.o.B. Destination Only.

(End of clause)

**II.13 52.204-23 - PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018) (DEVIATION 20-05)**

(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)

## **II.14 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TLELCOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 2020-05)**

(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 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 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 (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)

## **II.15 52.215-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS -- COMMERCIAL ITEM (JUN 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)(1)(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:

[Contracting Officer check as appropriate.]

(1) 52.203-6, Restrictions on Subcontractor Sales to the Government (June 2020), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

(2) 52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020) (41 U.S.C. 3509)).



(3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

(4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) [Reserved].

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

(7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

(8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Jun 2020) (31 U.S.C. 6101note).

(9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

(10) [Reserved].

(11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Mar 2020) (15 U.S.C.657a).

(ii) Alternate I (Mar 2020) of 52.219-3.

(12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Mar 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

(ii) Alternate I (Mar 2020) of 52.219-4.

(13) [Reserved]

(14) (i) 52.219-6, Notice of Total Small Business Set-Aside (Mar 2020) (15 U.S.C.644).

(ii) Alternate I (Mar 2020).

(15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Mar 2020) (15 U.S.C. 644).

(ii) Alternate I (Mar 2020) of 52.219-7.

(16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).

(17) (i) 52.219-9, Small Business Subcontracting Plan (Jun 2020) (15 U.S.C. 637(d)(4)).

(ii) Alternate I (Nov 2016) of 52.219-9.

(iii) Alternate II (Nov 2016) of 52.219-9.

(iv) Alternate III (Jun 2020) of 52.219-9.

(v) Alternate IV (Jun 2020) of 52.219-9.

(18) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).

(19) 52.219-14, Limitations on Subcontracting (Mar 2020) (15 U.S.C.637(a)(14)).

(20) 52.219-16, Liquidated Damages-Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

(21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Mar 2020) (15 U.S.C. 657f).

- (22) (i) 52.219-28, Post Award Small Business Program Rerepresentation (Mar 2020) (15 U.S.C. 632(a)(2)).
  - (ii) Alternate I (MAR 2020) of 52.219-28.
- (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Mar 2020) (15 U.S.C. 637(m)).
- (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Mar 2020) (15 U.S.C. 637(m)).
- (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).
- (26) 52.219-33, Nonmanufacturer Rule (Mar 2020) (15 U.S.C. 637(a)(17)).
- (27) 52.222-3, Convict Labor (Jun 2003) (E.O.11755).
- (28) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan 2020) (E.O.13126).
- (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- (30) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O.11246).
  - (ii) Alternate I (Feb 1999) of 52.222-26.
- (31) (i) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
  - (ii) Alternate I (Jul 2014) of 52.222-35.
- (32) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C.793).
  - (ii) Alternate I (Jul 2014) of 52.222-36.
- (33) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).
- (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- (35) (i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
  - (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter78 and E.O. 13627).
- (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.)
- (37) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
  - (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).
- (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
- (40) (i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

- (ii) Alternate I (Oct 2015) of 52.223-13.
- (41) (i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).
  - (ii) Alternate I (Jun 2014) of 52.223-14.
- (42) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).
- (43) (i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).
  - (ii) Alternate I (Jun 2014) of 52.223-16.
- (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020) (E.O. 13513).
- (45) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).
- (46) 52.223-21, Foams (Jun 2016) (E.O. 13693).
- (47) (i) 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552 a).
  - (ii) Alternate I (Jan 2017) of 52.224-3.
- (48) 52.225-1, Buy American-Supplies (May 2014) (41 U.S.C. chapter 83).
- (49) (i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
  - (ii) Alternate I (May 2014) of 52.225-3.
  - (iii) Alternate II (May 2014) of 52.225-3.
  - (iv) Alternate III (May 2014) of 52.225-3.
- (50) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).
- (51) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- (52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).
- (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).
- (55) 52.229-12, Tax on Certain Foreign Procurements (Jun 2020).
- (56) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C.4505, 10 U.S.C.2307(f)).
- (57) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C.4505, 10 U.S.C.2307(f)).
- (58) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct 2018) (31 U.S.C. 3332).
- (59) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C.3332).

(60) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C.3332).

(61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

(62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).

(63) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

(ii) Alternate I (Apr 2003) of 52.247-64.

(iii) Alternate II (Feb 2006) of 52.247-64.

(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:

[Contracting Officer check as appropriate.]

(1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

(2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(4) 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).

(5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(7) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).

(9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792).

(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, as defined in FAR 2.101, on the date of award of this contract, 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 disputes 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)

(1) 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)(1) 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 (Jun 2020) (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)(1)(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 the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

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

(vii) 52.222-26, Equal Opportunity (Sep 2015) (E.O.11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C.4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C.793).

(x) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C.4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

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

(xiii)

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

(B) Alternate I (Mar 2015) of 52.222-50(22 U.S.C. chapter 78 and E.O 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E.O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xviii) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).

(xix)

(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx.1241(b) and 10 U.S.C.2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(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)

**II.16 52.217-6 Option for Increased Quantity (MAR 1989)**

The Government may increase the quantity of supplies called for in the Schedule at the unit price specified. The Contracting Officer may exercise the option by written notice to the Contractor within 90 days of expiration of the option period. Delivery of the added items shall continue at the same rate as the like items called for under the contract, unless the parties otherwise agree.

(End of clause)

**II.17 52.217-7 Option for Increased Quantity-Separately Priced Line Item (MAR 1989)**

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within [insert in the clause the period of time in which the Contracting Officer has to exercise the option]. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of clause)

**II.18 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 90 days of expiration of the option period; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 120 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 5 years, 0 months.

(End of clause)

**II.19 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)**

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

**II.20 52.244-6 SUBCONTRACTS FOR COMMERCIAL ITEMS (AUG 2019)**

(a) Definitions. As used in this clause—

Commercial item and “commercially available off-the-shelf item” have the meanings contained in Federal Acquisition Regulation 2.101, Definitions.

Subcontract includes a transfer of commercial items between divisions, subsidiaries, or affiliates of the Contractor or subcontractor at any tier.

(b) To the maximum extent practicable, the Contractor shall incorporate, and require its subcontractors at all tiers to incorporate, commercial items or non-developmental items as components of items to be supplied under this contract.

(c)

(1) The Contractor shall insert the following clauses in subcontracts for commercial items:

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509), if the subcontract exceeds \$5.5 million and has a performance period of more than 120 days. In altering this clause to identify the appropriate parties, all disclosures of violation of the civil False Claims Act or of Federal criminal law shall be directed to the agency Office of the Inspector General, with a copy to the Contracting Officer.

(ii) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5), if the subcontract is funded under the Recovery Act.

(iii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017).

(iv) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (Jun 2016), other than subcontracts for commercially available off-the-shelf items, if flow down is required in accordance with paragraph (c) of FAR clause 52.204-21.

(v) 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).

(vi) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(vii) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C.637(d)(2) and (3)), if the subcontract offers 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.

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

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

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

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

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

(xiii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496), if flow down is required in accordance with paragraph (f) of FAR clause 52.222-40.

(xiv)

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

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xv) 52.222-55, Minimum Wages under Executive Order 13658 (Dec 2015), if flow down is required in accordance with paragraph (k) of FAR clause 52.222-55.

(xvi) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706), if flow down is required in accordance with paragraph (m) of FAR clause 52.222-62.

(xvii)

(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a) if flow down is required in accordance with 52.224-3(f).

(B) Alternate I (Jan 2017) of 52.224-3, if flow down is required in accordance with 52.224-3(f) and the agency specifies that only its agency-provided training is acceptable).

(xviii) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xix) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Dec 2013), if flow down is required in accordance with paragraph (c) of FAR clause 52.232-40.

(xx) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. App.1241 and 10 U.S.C.2631), if flow down is required in accordance with paragraph (d) of FAR clause 52.247-64).

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

(d) The Contractor shall include the terms of this clause, including this paragraph (d), in subcontracts awarded under this contract.

(End of clause)

## **II.21 CONTRACT TYPE (OCT 2008)**

This is an Indefinite Delivery Indefinite Quantity with Firm Fixed Price Orders.

[End of Clause]

## **II.22 SPECIFICATIONS, STATEMENT OF WORK, STATEMENT OF OBJECTIVES OR PERFORMANCE WORK STATEMENT ATTACHED (JUN 2013)**

The Specifications, Statement of Work, Statement of Objectives or Performance Work Statement which describe the work to be performed hereunder, although attached, is incorporated and made a part of this document with the same force and effect of "specifications" as described in the clause, Order of Precedence, FAR 52.215-8 incorporated herein by reference.

[End of Clause]

## **II.23 PERIOD OF PERFORMANCE (MAR 2003)**

The period of performance of this contract shall be from 07/02/2020 through 07/01/2025 as detailed below:

Base Period: 07/02/2020 – 07/01/2021

Option Period 1: 07/02/2021 – 07/01/2022

Option Period 2: 07/02/2022 – 07/01/2023

Option Period 3: 07/02/2023 – 07/01/2024

Option Period 4: 07/02/2024 – 07/01/2025

[End of Clause]

## **II.24 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)**

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

## **II.25 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)**

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP:

- Ref. FAR Part 32.905



The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

## **II.26 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)**

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

## **II.27 SECURITY PROCEDURES (APR 2019)**

### **A. Controls**

1. The Contractor Employee shall comply with the U.S. Customs and Border Protection's (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor Employee shall comply with all security policies contained in CBP Handbook 1400-05D, v.7.0, Information Systems Security Policies and Procedures Handbook, or latest available version.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Sensitive Systems Policy Directive 4300A, v.13.1 and DHS Sensitive Systems Handbook 4300A, v.12.0, or latest available version.
4. All Contractor Employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Representative (COR). The COR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Professional Responsibility, Security Management Division (OPR/SMD) shall be notified if building access is revoked.
5. All Contractor Employees must be entered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COR. The Contractor Project Manager (CPM) shall provide timely start information to the CO/COR or designated government personnel to initiate the CTS entry. Other relevant information will also be needed for record submission in the CTS database such as, but not limited to, the contractor's legal name, contracting company address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COR or designated government personnel shall provide the CPM with instructions for providing required information.
6. The CO/COR may designate responsibility for out-processing to the CPM. This requires that the CPM have an active CBP Background Investigation (BI) and Active Directory (AD) account. CPM shall provide Contractor Employee departure/separation date and reason for leaving to the CO/COR in accordance with CBP Directive 1210-007B, Tracking of Contractor Employees. Failure by the CPM to provide timely notification of Contractor Employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures. Additionally, the CO/COR shall immediately notify OPR/SMD of the contractor's departure/separation.

## B. Security Background Investigation Requirements

1. In accordance with DHS Instruction Handbook 121-01-007-01, Rev. 01, the Department of Homeland Security Personnel Security, Suitability and Fitness Program, Chapter 2, Personnel Security Program Standards, § 13, Citizenship Requirements, Contractor Employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status, § 13E. A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01.
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with Chapter 2, Personnel Security Program Standards, § 13, and Citizenship Requirements, § 13F. (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01.
3. Provided the requirements of DHS Instruction Handbook 121-01-007-01 are met as outlined in paragraph 1, above, Contractor Employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the Contractor Employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor Employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).
4. The Contractor Employee shall submit within ten (10) working days after award of this contract a list containing the full legal name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards. For Contractor employee candidates needing a BI for this contract, the Contractor Employee shall require the applicable Contractor Employees to submit information and documentation requested by CBP to initiate the BI process.
5. Background Investigation information and documentation is usually submitted by proper completion of standard federal and agency forms such as Electronic Questionnaires for investigations Processing (e-QIP), Fingerprint Card, CBP Form 78-Background Investigation Requirements Determination (BIRD), Fair Credit Reporting Act (FCRA) Form, a Contractor Employee Initial Background Investigation (BI) Form (CBP Form 77) (Sections A and B). These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.
6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of its employees who successfully complete the CBP BI or SSBI process to the CO and COR. Failure of any Contractor Employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel Contractor Employees, the Contractor shall propose a qualified replacement employee candidate to the COR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COR shall approve or disapprove replacement employees. Continuous failure to provide Contractor Employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

## C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.
2. The CO/COR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the

solicitation/contract. The Contractor Employee shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.

4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor Employee shall return all sensitive information used in the performance of the contract to the CO/COR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

#### D. Notification of Contractor Employee Changes

1. The CPM shall notify the CO/COR via phone, facsimile, or electronic transmission, immediately after a personnel change becomes known or no later than five (5) business days prior to departure of the Contractor Employee. Telephone notifications must be immediately followed up in writing. CPM's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.
2. The CPM shall notify the CO/COR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. If a security clearance is required, the CO/COR will notify OPR/SMD.

#### E. Non-Disclosure Agreements

As part of the BI package, Contractor Employees are required to execute and submit a Non-Disclosure Agreement (DHS Form 11000-6) as a condition to perform on any CBP contract.

[End of Clause]

### II.28 GOVERNMENT PROPERTY (MAR 2003)

The Contractor will be provided with the following items of property for performance of this contract, in accordance with the Government Property clause(s) contained herein.

Item Description	Property ID Number	Quantity	Delivery Date
------------------	--------------------	----------	---------------

[End of Clause]

### II.29 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:
  - a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
  - b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.

- c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.
2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

## II.30 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

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

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

- (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

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

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

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

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

- (c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:
  - (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
  - (2) DHS Sensitive Systems Policy Directive 4300A
  - (3) DHS 4300A Sensitive Systems Handbook and Attachments
  - (4) DHS Security Authorization Process Guide
  - (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
  - (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
  - (7) DHS Information Security Performance Plan (current fiscal year)
  - (8) DHS Privacy Incident Handling Guidance
  - (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
  - (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
  - (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

- (1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.
  - (2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
  - (3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.
  - (4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.
- (e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.
- (1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.
    - (i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.
    - (ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

- (iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.
- (2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.
- (3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.
- (4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.
- (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)

**II.31 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)**

- (a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.
- (b) Security Training Requirements.
- (1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.
- (2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.
- (c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)