[redacted]

H.1 SUBCONTRACTING PLANS AND GOALS

The Small Business Subcontracting Plan (Attachment 11) should be submitted with the Business Proposal, Volume II as outlined in section L, and must be compliant with FAR Clause 52.219-9 Small Business Subcontracting Plan, Alternate II. The Contractor's Small Business Subcontracting Plan submitted will include, at a minimum, the goals set forth below for each socio-economic grouping listed (if higher subcontracting goals are proposed in the Offeror's Small Business Subcontracting Plan, the higher goals will be incorporated into this section).

Category	Subcontracting Goal
Total Small Business	42.5%
Total Small Disadvantaged Businesses (both Section 8(a) and non-Section 8(a) firms)	5% *
Women Owned Small Business	5% *
Service-Disabled Veteran-Owned Small Businesses	3% *
Historically Underutilized Empowerment Zone Small Businesses	3% *

* Represents a subset percentage of the Total Small Business goal (for examples, if 3% is awarded to Woman-owned SmallBusinesses, that 3% would also apply the Total Small Business' subcontracting goal.

The Small Business Subcontracting Plan, dated (provided at time of award), is attached hereto and made a part of this contract. Failure of any Contractor or subcontractor to comply in good faith with FAR Clause 52.219-8 Utilization of Small Business Concerns, incorporated in this contract, and the attached Subcontracting Plan will be material breach of such contract or subcontract and subject to the remedies reserved to the Government under FAR Clause 52.219-16 Liquidated Damages-Subcontracting Plan.

H.2 OVERTIME

H.3 Contractor is responsible for all overtime within the IDIQ rates of the contract. Any approved overtime and/or extra-pay shifts shall be specified in the task order. Contractors shall perform all task orders without issuing overtime as far as possible, except when lower overall costs to the Government will result or when it is necessaryto respond to an event. Approval of overtime does not authorize the Contractor to violate labor laws specific to the labor categoryand FAR Clause 52.222-4 located in section I.ACCESSIBILITY OF MEETINGS, CONFERENCES, AND SEMINARS TO PERSONS WITH DISABILITIES

The Contractor agrees as follows:

Planning. The Contractor will develop a plan to assure that any meeting, conference, or seminar held pursuant to this contract will meet or exceed the minimum accessibility standards set forth below. This plan shall include a provision for ascertaining the number and types of disabled individuals planning to attend the meeting, conference, or seminar. The plan shall be submitted to the Contracting Officer for approval prior to initiating action. A consolidated or master plan for contracts requiring numerous meetings, conferences, or seminars may be submitted in lieu of separate plans.

Facilities. Any facility to be utilized for meetings, conferences, or seminars in performance of this contract shall be accessible to persons with disabilities. The Contractor shall determine, by an on-site inspection if necessary, that the following minimum accessibility requirements are met, or suitable modifications are made to meet these requirements, before the meeting:

(1) Parking. (i) Where parking is available on or adjacent to the site one 12' wide space must be set aside for the car of each mobility impaired attendee. The space need not be permanently striped but may be temporarily marked by signs, ropes, or other means satisfactory to carry out this provision.

(ii) Where parking is not available on or adjacent to the site, valet parking or other alternative means must be available to assist disabled attendees. Alternate means must be satisfactory in the judgment of the Contracting Officer.
(2) Entrances. (i) "Entrances" shall include at least one accessible entrance from the street/sidewalk level, and at least one accessible entrance from any available parking facility.

The entrance shall be level or accessible by ramp with an incline that allows independent negotiation by a person in a wheelchair.

In general, the slope of the incline shall be no more than 1" rise per foot of ramp length (1:12).

Entrance doorways shall be at least 30" in clear width and capable of operation by persons with disabilities. Revolving doors, regardless of foldback capability, will not meet this requirement.

(3) Meeting Rooms. (i) Meeting room access from the main entrance area must be level or at an independently negotiable incline (approximately 1:12) and/or served by elevators from the main entrance level. All elevators shall be capable of accommodating a wheelchair 29" wide by 45" long.

Meeting rooms shall be on one level or, if on different levels, capable of being reached by elevators or by ramps that can be independently negotiated by a person in a wheelchair. Doorways to all meeting rooms shall be at least 30" in clear width.

The interior of the meeting room shall be on one level or ramped so as to be independently negotiable for a person in a wheelchair.

Stages, speaker platforms, etc. which are to be used by persons in wheelchairs must be accessible by ramps or lifts. When used, the ramps may not necessarily be independently negotiable if space does not permit. However, any slope over 1:12 must be approved by the Contracting Officer. Each case is to be judged on its own merits.

If a meeting room with fixed seating is utilized, seating arrangements for persons in wheelchairs shall be made so that these persons are incorporated into the group rather than isolated on the perimeter of the group.

(4) Restrooms. (i) Restrooms shall have level access, signs indicating accessibility, and doorways at least 30" in clear width.

Sufficient turning space within restrooms shall be provided for independent use by a person in a wheelchair 29" wide by 45" long. A space 60" by 60" or 63" by 56" of unobstructed floor space as measured 12" above the floor is acceptable by standard; other layout will be accepted if it can be demonstrated that they are usable as indicated.

There will be a restroom for each sex or a unisex restroom with at least one toilet stall capable of accommodating a wheelchair 29" wide by 45" long (by standard, the minimum is 3'-0" by 43'- 83"), with out swinging door or private curtains. Wall mounted grab bars are required.

When separate restrooms have been set up for mobility impaired persons, they shall be located adjacent to the regular restrooms and shall be fully accessible.

(5) Eating Facilities. (i) Eating facilities in the meeting facility must be accessible under the same general guidelines as are applied to meeting rooms.

(ii) If the eating facility is a cafeteria, the food service area (cafeteria line) must allow sufficient room for independent wheelchair movement and accessibility to food for persons in wheelchairs, and cafeteria staff shall be available to assist disabled persons.

Overnight Facilities. If overnight accommodations are required:

Sufficient accessible guest rooms to accommodate each attendee who is disabled shall be located in the facility where the meeting, conference, or seminar is held, or in a facility housing the attendees which is conveniently located hereby, whichever is satisfactory to the Contracting Officer.

Overnight facilities shall provide for the same minimum accessibility requirements as the facility utilized for guest room access from the main entrance area shall be level, ramped at an independently negotiable incline (1:12), and/or served by elevators capable of accommodating a wheelchair 29" wide by 45" long.

Doorways to guest rooms, including the doorway to the bathroom, shall be at least 30" in clear width. (iv) Bathrooms shall have wall mounted grab bars at the tub and water closet.
(v) Guest rooms for persons with a disability shall be provided at the same rate as a guest room for other attendees.

Water Fountains. Water fountains shall be accessible to disabled persons or have cup dispensers for use by persons in wheelchairs.

(c) Provisions of Services for Sensory Impaired Attendees.

The Contractor, in planning the meeting, conference, or seminar shall include in all announcements and other materials pertaining to the meeting, conference, or seminar a notice indicating that services will be made available to sensory impaired persons

attending the meeting, if requested within five (5) days of the date of the meeting, conference, or seminar. The announcement(s) and other material(s) shall indicate that sensory impaired persons may contact a specific person(s), at a specific address and phone number(s), to make their service requirements known. The phone number(s) shall include a teletype number for the hearing impaired.

The Contractor shall provide, at no cost to the individual, those services required by persons with sensory impairments to insure their complete participation in the meeting, conference, or seminar.

As a minimum, when requested in advance, the Contractor shall provide the following services:

For hearing impaired persons, qualified interpreters. Provisions will also be made for volume-controlled phone lines and, if necessary, transportation to local teletype equipment to enable hearing impaired individuals to receive and send meeting related calls. If local teletype equipment is not available, the Contractor shall provide on-site teletype equipment. Also, the meeting rooms will be adequately illuminated so signing by interpreters can be easily seen.

For vision impaired persons, readers and/or cassette materials, as necessary, to enable full participation. Also, meeting rooms will be adequately illuminated.

Agenda and other conference material(s) shall be translated into a usable form for the visually and hearing impaired. Readers, braille translations, and/or tape recordings are all acceptable. These materials shall be available to sensory impaired individuals upon their arrival.

The Contractor is responsible for making every effort to ascertain the number of sensory impaired individuals who plan to attend the meeting, conference, or seminar. However, if it can be determined that there will be no sensory impaired person (deaf and/or blind) in attendance, the provision of those services under paragraph (c) for the non-represented group, or groups, is not required.

H.4 REPRODUCTION OF REPORTS

Reproduction of reports, data, or other written material, if required herein, is authorized provided that the material produced does not exceed 5,000 production units of any page and that items consisting of multiple pages do not exceed 25,000 production units in aggregate. The aggregate number of production units is to be determined by multiplying pages times copies. A production unit is one sheet, size 8 1/2x11 inches or less, printed on one side only, and in one color. All copy preparation to produce camera-ready copy for reproduction must be set by methods other than hot metal typesetting. The reports should be produced by methods employing stencils, masters, and plates which are to be used on single-unit duplicating equipment no larger than 11 by 17 inches with a maximum image of 10 3/4 by 14 1/4 inches and are prepared by methods or devices that do not utilize reusable contact negatives and/or positives prepared with a camera requiring a darkroom. All reproducible (camera-ready copies for reproduction by photo offset methods) shall become the property of the Government and shall be delivered to the Government with the report, data, or other written material.

H.5 COORDINATION OF FEDERAL REPORTING SERVICES

In the event that it is a contractual requirement to collect information from 10 or more public respondents, the provisions of 44 U.S.C. Chapter 35 (Coordination of Federal Reporting Requirements), shall apply to this contract. The contractor shall obtain through the COR the required Office of Management and Budget clearance before making public contacts for the collection of data or expending any funds for such collection. The authority to proceed with the collection of data from public respondents and the expenditure of funds therefore shall be in writing signed by the Contracting Officer.

H.6 PUBLICATION

Definition. For the purpose of FAR 27.404-4 Contractor's Release, Publication, and Use of Data includes (1) any document containing information intended for public consumption or (2) the act of, or any act which may result in, disclosing information to the public.

General. The results of the research and development and studies conducted under this contract are to be made available to the public through dedication, assignment to the Government, or other such means as the Director of the Federal Emergency Management Agency shall determine.

Reports furnished the Government. All intermediate and final reports of the research and development and studies conducted hereunder shall indicate on the cover or other initial page that the research and development and studies forming the basis for the report were conducted pursuant to a contract with the Federal Emergency Management Agency. Such reports are official Government property and may not be published or reproduced (in total, in verbatim excerpt, or in a form approximating either of these) as an unofficial paper or article. The contractor or technical personnel (each employee or consultant working under the

administrative direction of the contractor or any subcontractor hereunder) may publish such reports in whole or in part in a non-Government publication only in accordance with this paragraph (c) and paragraph (e)(1) of this clause.

Publication by Government. The Government shall have full right to publish all information, data, and findings developed as a result of the research and development and studies conducted hereunder.
Publication by contractor or technical personnel.

Publication in whole or in part of contractor's reports furnished the Government. Unless such reports have been placed in the public domain by Government publication, the contractor or technical personnel (each employee or consultant working under the administrative direction of the contractor or any subcontractor hereunder) may publish a report furnished the Government, in total or in verbatim excerpt, but consistent with paragraph (c) of this clause may not secure copyright therein, subject to the following conditions and the conditions in paragraph (e)(4) and paragraph (f).

During the first six months after submission of the full final report, if written permission to publish is obtained from the contracting officer.

After six months following submission of the full report, and if paragraph (e)(3) is inapplicable, if a foreword or footnote in the non-Government publication indicates the source of the verbatim material.

Publication, except verbatim excerpts, concerning or based in whole or in part on results of research and development and studies hereunder. The contractor or technical personnel may issue a publication concerning or based in whole or in part on the results of the research and development and studies conducted under this contract and may secure copyright therein, but in so publishing is not authorized thereby to inhibit the unrestricted right of the Director of the Federal Emergency Management Agency to disclose or publish, in such manner as he may deem to be in the public interest, the results of such research and development and studies to the following conditions and the requirement in paragraph (e)(4):

During the first six months after submission of the full final report, and if paragraph (e)(3) is inapplicable, if written waiver of the waiting period is obtained from the contracting officer.

After six months following submission of the full final report, and if paragraph (e)(3) is inapplicable, subject to Government exercise of an option that the publication contain a foreword or initial footnote substantially as follows: The (research) (development) (studies) forming (part of) the basis for this publication were conducted pursuant to a contract with the Federal Emergency Management Agency. The substance of such (research) (development) (studies) is dedicated to the public. The author and publisher are solely responsible for the accuracy of statements or interpretations contained therein.

General conditions if FEMA determines that contractor's final report contains patentable subject matter developed in contract performance. If the contracting officer determines that the contractor's full final report contains patentable subject matter developed in the performance of this contract and so notifies the contractor in writing prior to six months from date of submission of such report, no publication of verbatim excerpts from contractor's reports or publication concerning or based in whole or in part on the results of the research and development and studies hereunder shall be made without the written consent of the contracting officer.

Copies of contractor and technical personnel publications to be furnished the Government. The contractor or technical personnel will furnish the contracting officer six copies of any publications which are based in whole or in part on the results of the research and development and studies conducted under this contract.

Administratively confidential information. The contractor shall not publish or otherwise disclose, except to the Government and except matters of public record any information or data obtained hereunder from private individuals, organizations, or public agencies in a publication whereby the information or data furnished by any particular person or establishment can be identified, except with the consent of such person or establishment.

Inclusion of provisions in contractor's agreements. The contractor shall include provisions appropriate to effectuate the purposes of this clause in all contracts of employment with persons who perform any part of the research or development or study under this contract and in any consultant's agreements or subcontracts involving research or development or study there under.

H.7 OBSERVANCE OF LEGAL HOLIDAYS

The Government hereby provides notice and the Contractor hereby acknowledges receipt that FEMA Government observes all United States of America Holidays.

Any other day designated by Federal statute. Any other day designated by Executive Order. Any other day designated by the President’s proclamation.

When such day falls on a Saturday, the preceding Friday is observed; when any such day falls on a Sunday, the following Monday is observed. It is understood and agreed between the Government and the Contractor that observance of such days by Government Personnel shall not be used as the cause of an additional period of performance, or entitlement of compensation except as a holiday. No form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost. However, this does not preclude reimbursement for authorized overtime work.

In each instance, the Contractor agrees to continue to provide sufficient personnel to perform round-the-clock requirements of critical tasks already in operation or scheduled and shall be guided by the instructions issued by the Contracting Officer or his/her duly authorized representative.

H.8 NON-PERSONAL SERVICES

A non-personal services contract is defined as —a contract under which the personnel rendering the services are not subject, either by the Contract's terms or by the manner of its administration, to the supervision and control usually prevailing in relationships between the Government and its employees.

This is a non-personal services contract.

H.9 DATA MANAGEMENT PROGRAM REQUIREMENTS

The Federal Emergency Management Agency's (FEMA) Data Management Program was established to meet the regulatory requirements of the Information Technology Management Reform Act (a k.a. Clinger Cohen Act), as outlined in the Information Technology Architecture Implementation Plan. FEMA's Data Management Program requires that contractors comply with the requirements of this program when the contract involves tasks to design, develop, or maintain an information system for FEMA. Therefore, in the performance of this contract, the Contractor shall comply with the requirements of the FEMA Data Management Program which follow:

1. Names of database objects and procedural objects shall conform to the naming standards and conventions contained in FEMA's Data Naming Standards. A copy of the standard is available for review at www fema.gov/ofm/bidinfo htm and a copy will be provided to the Contractor, at contract award, upon request.

2. Abbreviations, acronyms, and terms used to develop an information technology system shall be limited to those listed on FEMA's Standard Abbreviations, Acronyms, and **Terms** list. The Standard Abbreviations, Acronyms, and Terms list is available for review at www.fema.gov/ofm/bidinfo htm. Developers, who wish to use an abbreviation, acronym, or term that is not listed on the Standard Abbreviations, Acronyms and Terms list, may request that FEMA's Data Administration Group consider including the abbreviation, acronym, or term as a standard. FEMA's Data Naming Standards detail procedures on the use of abbreviations, acronyms, and terms.

3. Logical and Physical Data Models shall be created for each information technology system using either of FEMA's approved standards for data modeling software, which are Sybase's Power Designer, or Oracle Designer.

4. Comments shall be included in all procedures that are developed and written after the create procedure statement to ensure that comments are available in the database's system catalog and can be input into the Enterprise Data Dictionary automatically. Comments shall include the following at a minimum:
- name of the developer - date procedure was developed - purpose of the procedure - functions performed by procedure - date of any changes made to the procedure - the name of the individual who made a change to the procedure - reason why a change was made to the procedure.

5. Comments shall be included for all tables, views, and columns that are developed. The comments that are written for tables and views shall contain detailed information on the definition, purpose, and use of the table or view. Comments that are written for columns shall precisely describe the data that is authorized for the field so there is a clear understanding of what the data in this field represents. Comments for tables, views, and columns shall be created at the time the database object is created in the database.

6. Data in FEMA's systems which should be available for enterprise-wide access and use will be identified, when required by the contract, so that FEMA's Data Administration Group can include it in FEMA's Enterprise 148 Data Model and in FEMA's Enterprise Data Dictionary and made available to promote systems integration.

FEMA's Enterprise Data Model presents a graphical view of the entities (tables), along with their relationships to other entities, and their attributes (columns). FEMA's Enterprise Data Dictionary will show the characteristics (domain) and meaning of the data (metadata), as well as any constraints (includes permitted values) associated with a data element or column in a table.

7. The FEMA Enterprise Data Dictionary shall contain metadata about the data in the databases of FEMA's enterprise systems. FEMA's enterprise systems that use Oracle as their database management system shall be accessible to FEMA's Enterprise Data Dictionary so that data can be captured and automatically input into
FEMA's Enterprise Data Dictionary.

H.10 CONTRACTOR UTILIZATION OF GOVERNMENT FACILITIES

The effort required to be accomplished will be determined at the Task Order level.

The contractor shall furnish all personnel required for the performance of the resulting IDIQ and task order(s) at the time of award. FEMA will provide to all appropriate personnel and documents pertaining to the project that are under the control of FEMA subject to the requirements of HSPD-12. The work will occur at various locations throughout the United States and U.S. Territories as direct by FEMA at the task order level.

H.11 CONFIDENTIALITY OF INFORMATION

(a) To the extent that the work under this contract requires that the Contractor be given access to sensitive or proprietary business, technical, or financial information belonging to the Government or other companies, the Contractor shall, after receipt thereof, treat such information as confidential and not appropriate such information to its own use or disclose such information to third parties unless specifically authorized by the Contracting Officer in writing. The foregoing obligations, however, shall not apply to information that--

1. At the time of receipt by the Contractor, is in the public domain
2. Is published by others after receipt thereof by the Contractor or otherwise becomes part of the public domain through no fault of the Contractor
3. The Contractor can demonstrate it was already in its possession at the time of receipt thereof and was not acquired directly or indirectly from the Government or other companies
4. The Contractor can demonstrate was received by it from a third party that did not require the Contractor to hold it in confidence.

(b) The Contractor shall obtain from each employee permitted access a DHS Form 11000-6, Non-Disclosure Agreement, stating that he/she will not discuss, divulge or disclose any such information or data to any person or entity except those persons within the Contractor's organization or the Government directly concerned with the performance of the contract. The DHS Form 11000-6 will be provided at time of contract award.

H.12 ORGANIZATIONAL CONFLICT OF INTEREST

The Contractor warrants that, to the best of his/her knowledge and belief, and except as otherwise set forth in this contract, he/she does not have any organizational conflict of interest as defined in the following paragraph. The term "organizational conflict of interest" means a situation where a Contractor has interests, either due to his/her other activities or his/her relationships with other organizations, which place him/her in a position that may be unsatisfactory or unfavorable

(a) from the Government's standpoint in being able to secure impartial, technically sound, objective assistance and advice from the Contractor, or in securing the advantages of adequate competition in its procurement; or

(b) from industry's standpoint in that unfair competitive advantages may accrue to the Contractor in question.

The Contractor agrees that, if after award he/she discovers an organizational conflict of interest with respect to this contract, he/she shall make an immediate and full disclosure in writing to the Contracting Officer that shall include a description of the action that the Contractor has taken or proposes to take to avoid, eliminate or neutralize the conflict. The Government, may, however, terminate the contract for the convenience of the Government if it would be in the best interest of the Government. If the Contractor was aware of organization conflict of interest before the award of this contract and intentionally did not disclose the conflict to the Contracting Officer, the Government may terminate the contract at no cost to the Government.

[redacted]

[redacted]

[redacted]

H.14 TRANSPORTATION PRIORITIES AND ALLOCATIONS SYSTEM REGULATIONS

"Task orders under this contract may include a priority rating under the Health Resources Priorities and Allocations System (HRPAS) regulation (45 CFR, part 101.1). Anyone receiving a HRPAS rated order is required to follow all provisions of the HRPAS regulation."

"Task orders under this contract may include a priority rating under the Transportation Priorities and Allocations System (TPAS) regulation (49 CFR, part 33). Anyone receiving a TPAS rated order is required to follow all provisions of the TPAS regulation."

PART II - CONTRACT CLAUSES
SECTION I - CONTRACT CLAUSES
I.1 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

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): https://www.acquisition.gov/ and https://www.acquisition.gov/hsar

NUMBER	TITLE	
52.202-1	DEFINITIONS	JUN 2020
52.203-3	GRATUITIES	APR 1984
52.203-5	COVENANT AGAINST CONTINGENT FEES	MAY 2014
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	JUN 2020
52.203-7	ANTI-KICKBACK PROCEDURES	JUN 2020
52.203-8	CANCELLATION, RESCISSION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY	MAY 2014
52.203-10	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY	MAY 2014
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	JUN 2020
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	NOV 2021
52.203-14	DISPLAY OF HOTLINE POSTER(S)	NOV 2021
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	JUN 2020
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-4	PRINTED OR COPIED DOUBLE-SIDED	MAY 2011
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-10	REPORTING SUBCONTRACTING AWARDS	JUN 2020
52.204-13	SYSTEM FOR AWARD MANAGEMENT MAINTENANCE	OCT 2018
52.204-15	SERVICE CONTRACT REPORTING REQUIREMENTS FOR INDEFINITE-DELIVERY CONTRACTS	OCT 2016
52.204-19	INCORPORATION BY REFERENCE OF REPRESENTQATIONS AND CERTIFICATIONS	DEC 2014
52.204-23	PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDEDBY KASPERSKY LAB AND OTHER COVERED ENTITIES	NOV 2021
52.204-25	PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT	NOV 2021
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	NOV 2021
52.209-9	UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS	OCT 2018
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2015
52.210-1	MARKET RESEARCH	NOV 202
52.215-2	AUDIT AND RECORDS--NEGOTIATION	JUN 2020
52.215-8	ORDER OF PRECEDENCE--UNIFORM CONTRACT	OCT 1997

52.215-14	INTEGRITY OF UNIT PRICES	NOV 2021
52.215-23	LIMITATIONS ON PASS-THROUGH CHARGES	JUN 2020
52.216-7	ALLOWABLE COST AND PAYMENT	AUG 2018
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	OCT 2018
52.219-9 Alt II	SMALL BUSINESS SUBCONTRACTING PLAN	NOV 2016
52.219-16	LIQUIDATED DAMAGES--SUBCONTRACTING PLAN	SEP 2021
52.222-1	NOTICE TO THE GOVERNMENT OF LABOR DISPUTES	FEB 1997
52.222-3	CONVICT LABOR	JUN 2003
52.222-4	CONTRACT WORK HOURS AND SAFETY STANDARDS ACT-OVERTIME COMPENSATION	MAY 2018
[redacted]	[redacted]	[redacted]
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	JUN 2020
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITES	JUN 2020
52.222-37	EMPLOYMENT REPORTS ON VETERANS	JUN 2020
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER	DEC 2010
52.222-41	THE NATIONAL LABOR RELATIONS ACT SERVICE CONTRACT LABOR STANDARDS	AUG 2018
52.222-43	FAIR LABOR STANDARDS ACT AND SERVICE CONTRACT ACT-PRICE ADJUSTMETNS (MULTIPLE YEAR AND OPTION CONTRACTS)	AUG 2018
52.222-49	SERVICE CONTRACT ACT – PLACE OF PERFORMANCE UNKNOWN	MAY 2014
52.222-50	COMBATING TRAFFICKING IN PERSONS	NOV 2021
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION INFORMATION	NOV 2021
52.223-6	DRUG-FREE WORKPLACE	MAY 2001
52.223-18	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	JUN 2020
52.224-1	PRIVACY ACT NOTIFICATION	APR 1984
52.224-2	PRIVACY ACT	APR 1984
52.224-3 Alt I	PRIVACY ACT TRAINING	JAN 2017
52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES	FEB 2021
52.227-14 Alt V	RIGHTS IN DATA--GENERAL	DEC 2007
52.228-5	INSURANCE-WORK ON A GOVERNMENT INSTALLATION	JAN 1997
52.229-3	FEDERAL, STATE, AND LOCAL TAXES	FEB 2013
52.230-2	COST ACCOUNTING STANDARDS	JUN 2020
52.232-1	PAYMENTS	APR 1984
52.232-7	PAYMENTS UNDER TIME AND MATERIALS AND LABOR HOUR CONTRACTS	NOV 2021
52.232-9	LIMITATION ON WITHHOLDING OF PAYMENTS	APR 1984
52.232-17	INTEREST	MAY 2014
52.232-23	ASSIGNMENT OF CLAIMS	MAY 2014
52.232-25	PROMPT PAYMENT	JAN 2017
52.232-33	PAYMENT BY ELECTRONIC FUNDS—SYSTEMS FOR AWARD MANAGEMENT	OCT 2018
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JUN 2013
52.233-1 Alt I	DISPUTES	DEC 1991
52.233-3	PROTEST AFTER AWARD	AUG 1996
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	OCT 2004
52.237-3	CONTINUITY OF SERVICES	JAN 1991
52.242-3	PENALTIES FOR UNALLOWABLE COSTS	SEP 2021
52.242-13	BANKRUPTCY	JUL 1995
52.243-1	CHANGES -- FIXED -PRICE	AUG 1987
52.243-3	CHANGES--TIME-AND-MATERIALS OR LABOR HOURS	SEP 2000
52.244-2	SUBCONTRACTS	JUN 2020
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS	JAN 2022
52.246-25	LIMITATION OF LIABILITY--SERVICES	FEB 1997
52.247-21	CONTRACTOR LIABILITY FOR PERSONAL INJURY AND/OR PROPERTY DAMAGE	APR 1984
52.248-1	VALUE ENGINEERING	JUN 2020
52.249-2	TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED PRICE)	APR 2012
52.249-4	TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (SERVICES)	APR 1984

52.222-21 & 52.222-26 Removed effective 3/6/25

52.249-8 Alt 1	DEFAULT (FIXED-PRICE SUPPLY AND SERVICE)	APR 1984
52.249-14	EXCUSABLE DELAYS	APR 1984
52.253-1	COMPUTER GENERATED FORMS	JAN 1991
3052.203-70	INSTRUCTIONS FOR CONTRACTOR DISCLOSURE OF VIOLATIONS	SEP 2012
3052.205-70	ADVERTISEMENTS, PUBLICIZING AWARDS AND RELEASES	SEP 2012
3052.219-71	DHS MENTOR-PROTÉGÉ PROGRAM	JUN 2006
3052.222-70	STRIKES OR PICKETING AFFECTING TIMELY COMPLETION OF THE CONTRACT WORK	DEC 2003
3052.222-71	STRIKES OR PICKETING AFFECTING ACCESS A DHS FACILITY	DEC 2003
3052.228-70	INSURANCE	DEC 2003
3052.236-70	SPECIAL PROVISIONS FOR WORK AT OPERATING AIRPORTS	DEC 2003
3052.242-72	CONTRACTING OFFICER'S TECHNICAL REPRESEANTAIVE	DEC 2003

[redacted]

[redacted]

I.3 52.216-18 ORDERING (AUG 2020)

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 from the effective date of contract award through the end of the effective period.

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.

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, or by electronic commerce methods.

[redacted]

[redacted]

I.8 52.222-42 STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES. (May 2014)

Per the Wage Determination attached to each Task Order

Employee Class	Monetary Wage-Fringe Benefits
_ _ _ _ _ _ _	_____ _____ _____

–	
–	
–	
–	
–	
–	
–	
–	
–	
–	
–	
–	
–	
–	
–	
–	

In compliance with the Service Contract Labor Standards statute and the regulations of the Secretary of Labor (29 CFR Part 4), this clause identifies the classes of service employees expected to be employed under the contract and states the wages and fringe benefits payable to each if they were employed by the contracting agency subject to the provisions of 5 U.S.C.5341 or 5 332.

This Statement is for Information Only: It is not a Wage Determination

I.9 52.237-7 INDEMNIFICATION AND MEDICAL LIABILITY INSURANCE. (JAN 1997)

(a) It is expressly agreed and understood that this is a nonpersonal services contract, as defined in Federal Acquisition Regulation (FAR) 37.101, under which the professional services rendered by the Contractor are rendered in its capacity as an independent contractor. The Government may evaluate the quality of professional and administrative services provided but retains no control over professional aspects of the services rendered, including by example, the Contractor's professional medical judgment, diagnosis, or specific medical treatments. The Contractor shall be solely liable for and expressly agrees to indemnify the Government with respect to any liability producing acts or omissions by it or by its employees or agents. [redacted]

(b) An apparently successful offeror, upon request by the Contracting Officer, shall furnish prior to contract award evidence of its insurability concerning the medical liability insurance required by paragraph (a) of this clause.

(c) Liability insurance may be on either an occurrences basis or on a claims-made basis. If the policy is on a claims-made basis, an extended reporting endorsement (tail) for a period of not less than 3 years after the end of the contract term must also be provided.

(d) Evidence of insurance documenting the required coverage for each health care provider who will perform under this contract shall be provided to the Contracting Officer prior to the commencement of services under this contract. If the insurance is on a claims-made basis and evidence of an extended reporting endorsement is not provided prior to the commencement of services, evidence of such endorsement shall be provided to the Contracting Officer prior to the expiration of this contract. Final payment under this contract shall be withheld until evidence of the extended reporting endorsement is provided to the Contracting Officer.

(e) The policies evidencing required insurance shall also contain an endorsement to the effect that any cancellation or material change adversely affecting the Government's interest shall not be effective until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer. If, during the performance period of the contract the Contractor changes insurance providers, the Contractor must provide evidence that the Government will be indemnified to the limits specified in paragraph (a) of this clause, for the entire period of the contract, either under the new policy, or a combination of old and new policies.

(f) The Contractor shall insert the substance of this clause, including this paragraph (f), in all subcontracts under this contract for health care services and shall require such subcontractors to provide evidence of and maintain insurance in accordance with

paragraph (a) of this clause. At least 5 days before the commencement of work by any subcontractor, the Contractor shall furnish to the Contracting Officer evidence of such insurance.

I.10 HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

(a) "Sensitive Information," as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or 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:

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, Pub. L. 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);

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);

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

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

"Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

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

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

Alternate II (JUN 2006) When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:
Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee. Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

[redacted]

I.12 NARA RECORDS MANAGEMENT LANGUAGE FOR CONTRACTS

The following standard items relate to records generated in executing the contract and should be included in a typical Electronic Information Systems (EIS) procurement contract:

Citations to pertinent laws, codes and regulations such as 44 U.S.C chapters 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); 36 CFR Part 1222 and Part 1228.

Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.

Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.

Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act.

Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.

The Government Agency owns the rights to all data/records produced as part of this contract.

The Government Agency owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format (paper, electronic, etc.) or mode of transmission (e-mail, fax, etc.) or state of completion (draft, final, etc.).

No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.

Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

[redacted]

I.14 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 107296, 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 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.

I.15 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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.

Security Training Requirements.
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 31stof each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise

specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

I.16 52.223-99 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRATORS. (OCT 2021) (DEVIATION)

(a) Definition. As used in this clause -
United States or its outlying areas means—

(1) The fifty States;
(2) The District of Columbia;
(3) The commonwealths of Puerto Rico and the Northern Mariana Islands;
(4) The territories of American Samoa, Guam, and the United States Virgin Islands; and
(5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) Authority. This clause implements Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985).

(c) Compliance. The Contractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this contract, for contractor workplace locations published by the Safer Federal Workforce Task Force (Task Force Guidance) at https://www.saferfederalworkforce.gov/contractors .

(d) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part within the United States or its outlying areas.