Subject: Comprehensive Encounter-level Inpatient and Hospital-based Outpatient Billing and Chargemaster Database for Addressing Public Health Priorities

Solicitation Number: 75D30126Q79192

ISSUANCE DATE: August 11, 2026

Response DUE Date/time: NLT 3:00PM ET August 26, 2026

Section A – Description

This is a combined synopsis/solicitation for commercial services prepared in accordance with the format in FAR RFO Subpart 12.6, as supplemented with additional information included in this notice. This announcement constitutes the only solicitation; proposals are being requested and a separate written solicitation will not be issued.

Solicitation number 75D30126Q79192 is issued as a Request for Quote (RFQ) for Comprehensive Encounter-level Inpatient and Hospital-based Outpatient Billing and Chargemaster Database for Addressing Public Health Priorities.

This acquisition is conducted in accordance with FAR Part 12 and FAR Part 13.5 (Simplified Procedures for Certain Commercial Items), as applicable.

This solicitation incorporates provisions and clauses by reference. The full text of the referenced provisions and clauses may be accessed electronically at **www.acquisition.gov**.

The associated North American Industry Classification System (NAICS) code is 518210 – Data Processing, Hosting, and Related Services, with a size standard of $40 Million. The Product Service Code (PSC) is B506 – Special Studies/Analysis (Other than Scientific).

The Government intends to award a single Firm-Fixed-Price contract to the responsible Offeror whose proposal satisfies the Government's minimum requirements and represents the best value to the Government.

NOTICE OF INTENT TO AWARD A SOLE SOURCE CONTRACT

In accordance with FAR RFO 6.103-1, the Centers for Disease Control and Prevention (CDC) intends to award a contract on a sole-source basis to Premier Healthcare Solutions, Inc.

Based on the Government's market research, Request for Information (RFI) responses, and the Justification for Other Than Full and Open Competition (JOFOC), the Government has determined that Premier Healthcare Solutions, Inc. as been determined to be the only responsible source capable of satisfying the Government's minimum requirements described in the Statement of Work.

The Government will consider all timely capability statements and proposals received from responsible sources to determine whether another source can satisfy the Government's minimum requirements. Offerors other than Premier Healthcare Solutions, Inc. should clearly demonstrate in their capability statement and proposal how they satisfy each of the Government's minimum requirements identified in the Statement of Work.

If the Government determines that another responsible source can satisfy the Government's minimum requirements, the Government reserves the right to modify its acquisition strategy and conduct a competitive acquisition if determined to be in the Government's best interest.

RESPONSE INSTRUCTIONS

Interested parties wishing to demonstrate their capability to satisfy the Government's minimum requirements shall submit a capability statement no later than **August 18, 2026, at 3:00 p.m. Eastern Time**.

Offerors wishing to submit a quote shall submit no later than **August 26, 2026, at 3:00 p.m. Eastern Time**.

Capability statements and proposals shall be submitted electronically to the Contracting Officer at the email address identified below.

The Government will evaluate all timely capability statements and proposals received in accordance with this solicitation. A determination that no other responsible source can satisfy the Government's minimum requirements, and the resulting decision not to compete this acquisition, is solely within the discretion of the Government.

POINT OF CONTACT

All questions concerning this solicitation and all capability statements and proposals shall be submitted in writing to:

Latoya Michel
Contracting Officer
Email: zrb5@cdc.gov

Telephone inquiries will not be accepted.

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

ITEM	SUPPLIES / SERVICES	QTY/UNIT	UNIT PRICE	EXTENDED PRICE
0001	Comprehensive and Social Determinants Of Health Data (SDOH) Extracts Task 1: The Contractor shall deliver to CDC the most up-to-date and recent Comprehensive and SDOH data extracts delivered each month in accordance (IAW) the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2026 – 09/13/2027	12 Each	$ TBD	$ TBD
0002	Long Term Mortality Data Table - Includes historical data between 01/01/2016 to Current Task 2: The Contractor shall deliver to CDC the Long Term Mortality Data between 01/01/2016 to current. Data extracts shall be delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2026 – 09/13/2027	12 Each	$ TBD	$ TBD
0003	Training, Monthly Calls, and Technical Support Task 3: Contractor shall provide four (4) hours of virtual, web-based training, support monthly meetings and provide technical support IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2026 – 09/13/2027	Lot	$ TBD	$ TBD
Option Period 1				
1001	Comprehensive and Social Determinants Of Health Data (SDOH) Extracts Task 1: The Contractor shall deliver to CDC the most up-to-date and recent Comprehensive and SDOH data extracts delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2027 – 09/13/2028	12 Each	$ TBD	$ TBD

1002	OPTIONAL Long Term Mortality Data Table - Includes historical data between 01/01/2016 to Current Task 2: The Contractor shall deliver to CDC the Long Term Mortality Data between 01/01/2016 to current. Data extracts shall be delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2027 – 09/13/2028	12 Each	$ TBD	$ TBD
1003	Training, Monthly Calls, and Technical Support Task 3: Contractor shall provide four (4) hours of virtual, web-based training, support monthly meetings and provide technical support IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2027 – 09/13/2028	12 Months	$ TBD	$ TBD
Option Period 2				
2001	Comprehensive and Social Determinants Of Health Data (SDOH) Extracts Task 1: The Contractor shall deliver to CDC the most up-to-date and recent Comprehensive and SDOH data extracts delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2028 – 09/13/2029	12 Each	$ TBD	$ TBD
2002	OPTIONAL Long Term Mortality Data Table - Includes historical data between 01/01/2016 to Current Task 2: The Contractor shall deliver to CDC the Long Term Mortality Data between 01/01/2016 to current. Data extracts shall be delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2028 – 09/13/2029	12 Each	$ TBD	$ TBD

2003	Training, Monthly Calls, and Technical Support Task 3: Contractor shall provide four (4) hours of virtual, web-based training, support monthly meetings and provide technical support IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2028 – 09/13/2029	12 Months	$ TBD	$ TBD
Option Period 3				
3001	Comprehensive and Social Determinants Of Health Data (SDOH) Extracts Task 1: The Contractor shall deliver to CDC the most up-to-date and recent Comprehensive and SDOH data extracts delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2029 – 09/13/2030	12 Each	$ TBD	$ TBD
3002	OPTIONAL Long Term Mortality Data Table - Includes historical data between 01/01/2016 to Current Task 2: The Contractor shall deliver to CDC the Long Term Mortality Data between 01/01/2016 to current. Data extracts shall be delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2029 – 09/13/2030	12 Each	$ TBD	$ TBD
3003	Training, Monthly Calls, and Technical Support Task 3: Contractor shall provide four (4) hours of virtual, web-based training, support monthly meetings and provide technical support IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2029 – 09/13/2030	12 Months	$ TBD	$ TBD
Option Period 4				

4001	Comprehensive and Social Determinants Of Health Data (SDOH) Extracts Task 1: The Contractor shall deliver to CDC the most up-to-date and recent Comprehensive and SDOH data extracts delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2030 – 09/13/2031	12 Each	$ TBD	$ TBD
4002	OPTIONAL Long Term Mortality Data Table - Includes historical data between 01/01/2016 to Current Task 2: The Contractor shall deliver to CDC the Long Term Mortality Data between 01/01/2016 to current. Data extracts shall be delivered each month IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2030 – 09/13/2031	12 Each	$ TBD	$ TBD
4003	Training, Monthly Calls, and Technical Support Task 3: Contractor shall provide four (4) hours of virtual, web-based training, support monthly meetings and provide technical support IAW the SOW. Firm Fixed Price Line Item. Period of Performance: 09/14/2030 – 09/13/2031	12 Months	$ TBD	$ TBD

B1. Total Contract Value Including (Base and All Options):

The total value for this Task Order, inclusive of the Base Period and all Option Periods, is set forth below. *This section will be finalized and incorporated at the time of award based on the successful offeror's price proposal.*

Summary of Pricing		
Base Period	**$**	**-**
Option Period 1	**$**	**-**
Option Period 2	**$**	**-**
Option Period 3	**$**	**-**
Option Period 4	**$**	**-**
Total:	**$**	**-**

B.2 Option CLINs 1001-4003 are Optional Priced Line Items, as described in FAR 52.217-5. Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award

purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

Section C - Description/Specification/Work Statement

Statement of Work

Title: Comprehensive Encounter-level Inpatient and Hospital-based Outpatient Billing and Chargemaster Database for Addressing Public Health Priorities

SECTION 1 – BACKGROUND

The U.S. Centers for Disease Control and Prevention (CDC), Office of Public Health Data, Surveillance, and Technology (OPHDST) leads efforts to modernize public health data, surveillance, and informatics capabilities to ensure timely, accurate, and actionable information for public health decision-making. The CDC routinely uses electronic healthcare data to meet its public health mission. Healthcare data are used to inform situational awareness, predictive modeling, and strategic, tactical, and policy decision making; to help track the spread and intensity of outbreaks and identify areas that are highly impacted by disease; to understand spectrum of illness, disease burden, risk factors for severe disease, and outcomes; and to understand the impact public health threats on healthcare systems and communities.

CDC requires access to a comprehensive, encounter-level healthcare database that combines administrative, healthcare utilization, and financial information from inpatient and hospital-based outpatient encounters with clinical laboratory results and vital measurements. Access to such an integrated healthcare database allows CDC to monitor disease and healthcare utilization trends over time and conduct longitudinal clinical, financial, and outcomes analyses related to public health priorities, including public health emergencies. The database should capture at least 25% of U.S. hospital admissions from a diverse set of hospitals with sufficient hospital-level data to generate reliable and valid national inpatient estimates. To achieve its mission, CDC requires the comprehensive database to contain general and microbiology laboratory results and vital measurements and to be linkable to social determinants of health, long-term mortality, and other potential data. For example, having detailed clinical, cost, and laboratory data within a single, integrated database is absolutely necessary for CDC to calculate burden, death, and attributable cost estimates for the several of the healthcare associated infections for the *Antimicrobial Resistance (AR) Threats Report*, including MRSA, VRE, CRE, carbapenem-resistant *Acinetobacter*, ESC-RE, and multidrug-resistance *Pseudomonas*. The *AR Threats Report* is an important CDC report providing estimates on antimicrobial resistance for the United States. Estimates for the AR Threats Report will be published by CDC at least bi-annually moving forward.

The CDC Data Hub within OPHDST is a full-service enterprise resource connecting CDC staff and other authorized individuals with high-value healthcare data and technical and analytic support to generate actionable insights and inform public health action. CDC Data Hub helps ensure data security, governance, stewardship, and quality assurance; manages data onboarding and access permissions; and provides training, technical assistance, and data analysis and scientific support, including within CDC's cloud-based data platforms. CDC Data Hub will oversee ingestion, management, security, and access to the healthcare data licensed through this procurement and serve as the primary liaison between the vendor and CDC staff using the data.

SECTION 2 – PURPOSE/OBJECTIVE

The purpose of this contract is for CDC to continue to license, obtain, and use a large, comprehensive, U.S.-based, encounter-level inpatient and hospital-based outpatient billing and chargemaster database. The licensed Comprehensive Healthcare Database shall contain detailed encounter-level administrative, healthcare utilization, and financial information data from standard hospital discharge billing files and line-item chargemaster records, as well as general and microbiology laboratory results and vital measurements data from electronic medical records within a single, integrated database. CDC also seeks to license, obtain, and use supplemental Social Determinants of Health data and Long-term Mortality data (Optional Task) that are linkable to the Comprehensive Healthcare Database at the patient level. All data should fulfill the requirements outlined in Sections 3, 4, and 5 of this Statement of Work. In brief, the Comprehensive Healthcare Database

shall be updated and delivered to CDC monthly; available historically from 2016; include majority of healthcare encounters that occurred in the most recent 2-3 months; provide ability to track individual patients longitudinally within a hospital or health system; capture detailed medications, procedures, devices, and services provided in the healthcare setting; include weights to generate national inpatient estimates; and come from a representative sample of at least 1,400 geographically diverse non-profit, non-governmental, and community and teaching hospitals and health systems from rural and urban areas that capture at least 25% of U.S. hospital admissions.

CDC requires pharmacy/medication, microbiology, general laboratory, and vital measurement data for monitoring antimicrobial resistance, sepsis, and other public health concerns. For example, to monitor trends in antimicrobial resistance, consistent hospitalization data with timing of clinical culture and associated susceptibility testing (microbiology and sensitivity data) is critical. To monitor sepsis and implement CDC's adult sepsis event definition, CDC requires data that can identify if and when a blood culture was collected during a hospitalization (microbiology data), several general laboratory measures (e.g., creatinine, lactate, bilirubin), procedures and care level of patients (e.g., mechanical ventilation and intensive care unit status), and medications (e.g., vasopressor and antibiotic use). Measurement and risk-adjustment of important healthcare quality surveillance measures, such as hospital-onset bacteremia or non-ventilator hospital-acquired pneumonia, require detailed clinical information coupled with microbiology data to identify positive blood cultures, other laboratory results (e.g., white blood cell counts), and vital signs (e.g., temperature and oxygen saturation). Other projects to monitor health outcomes after cancer therapies also require vital signs, microbiology, and laboratory information and leverage mortality data from both inside and outside the hospital.

CDC requires information on social determinants of health (SDOH) of patients to better understand the community-level and social factors that are associated with disease occurrence, hospital admission, disease severity, and outcomes. To be most useful, SDOH variables should be based on the patients' place of residence and provided at the lowest (or most granular) geographic level available or permissible.

It is important for CDC to have visibility on deaths that occur both inside and outside of the hospital setting. The ability to track patient-level mortality beyond the hospital encounter can provide more accurate longitudinal analyses and additional insights into outcomes for patients discharged to long-term care facilities, home health, or hospice care as well as for patients who died in other settings.

SECTION 3 – SCOPE OF WORK

The Contractor shall provide CDC with the necessary license(s) for full and complete access to and use of the Comprehensive Healthcare Database, Social Determinants of Health (SDOH) data, and Long-Term Mortality data **(Optional)** delivered to CDC, and shall provide training and technical support.

Requirements of the Comprehensive Healthcare Database:

1. Encounter-level administrative, healthcare utilization, and financial information for inpatient and hospital-based outpatient encounters derived from standard hospital discharge billing files and line-item chargemaster records
2. Encounter-level billing and chargemaster data from >1,400 geographically diverse non-profit, non-governmental, and community and teaching hospitals and health systems from rural and urban areas that capture at least 25% of annual U.S. hospital admissions
3. Includes unique patient identifier to track patients longitudinally over time and across inpatient and outpatient settings within the same hospital or health system
4. Contains consistently robust data from 2016 through the most recent records available;
5. Is relatively recent and includes records for the majority of healthcare encounters that occurred during the most recent 2-3 months at the time data are delivered to CDC
6. Contains the minimum data elements listed in Section 5 Task 1
7. Provides hospital/facility location at state and 3-digit ZIP code level
8. Includes weights for generating national inpatient estimates
9. Contains general laboratory and microbiology (including antibiotic susceptibility) laboratory results data, as specified in Section 5 Task 1, from >350 facilities (25% or more of total)
10. Contain vital measurements data, as specified in Section 5 Task 1, from >140 facilities (10% or more of total)
11. Contains detailed medication/drug/pharmacy data, including brand/generic drug names, strength, dosing, route of administration, day of service, quantity charged, and cost
12. Admission, discharge, and service dates shall be provided as exact dates (mm/dd/yyyy)

13. If available, patients' residential locations at the smallest geographic scale allowable.

Requirements of the contractor-provided Social Determinants of Health data:

1. Linkable to Comprehensive Healthcare Database at the patient level using unique patient identifier
2. At a minimum, include the following measures: American Community Survey average household size, median household income, income inequality, average educational level and CDC/ATSDR Social Vulnerability Index overall and for four themes
3. SDOH variables shall be based on the patients' place of residence (not facility location) at the lowest (or smallest) level of geography allowable (i.e., census tract, ZIP Code Tabulation Areas [ZCTAs], ZIP code, or county).
4. SDOH variables shall be provided at the highest level of resolution allowable (i.e., exact value rounded to whole number). If exact values are not allowable, the Contractor can provide the SDOH variables categorized into deciles (or ten equally sized groups) or other logical groupings for that variable.
5. SDOH variables shall align temporally to the patients' visit (i.e., 2024 SDOH indicators linked to 2024 visits). For more recent visits in which the corresponding year of SDOH indicators are not available, the Contractor shall use the most recent year available (e.g., 2024 SDOH indicators linked to 2025 or 2026 visits).

To support a holistic government approach and response to public health priorities, CDC shall be authorized to share aggregate data products with governmental partners including HHS, other federal agencies, and state, local, tribal, and territorial governments. Additionally, CDC shall be authorized to generate state-level estimates for public dissemination (i.e., sharing outside of CDC), as long as the state-level aggregate data product is reviewed and approved by Contractor's data governance board prior to dissemination outside of CDC.

Additionally, the Contractor shall permit CDC to retain license(s) to use data delivered under this contract for a minimum of an additional 12 months after the period of performance ends. This will allow CDC to complete and disseminate (e.g., in government reports or peer-reviewed publications) important analytic projects that were initiated during the contract period. CDC will not initiate new analytic projects after the period of performance ends.

All routine enhancements to the Contractor's Comprehensive Healthcare Database offering shall be included and provided to CDC at no additional cost. The Contractor may provide CDC with complimentary access to additional data, tool(s), or resource(s) that are available now or become available in the future to test their capabilities and determine if they may be beneficial to CDC. Access may be granted on a complimentary basis during the evaluation period as set by the Contractor. After the evaluation period, CDC may modify the contract to add the data, tool(s) and/or resource(s) if beneficial, cost-effective, and reasonable to the government.

SECTION 4 – TECHNICAL REQUIREMENTS

Personally identifiable information

The data delivered to CDC under this contract shall be record-level anonymized. CDC seeks to obtain the minimum data necessary to accomplish CDC's public health mission. CDC does not seek and will not accept personally identifiable information (PII) that directly identifies individuals, such as patient name, address, social security number or other identifying number or code, date and place of birth, telephone number, email address, or biometric records such as fingerprints. Contractor shall establish robust process to ensure no direct PII is included in data delivered to CDC. If PII is found within the data delivered to CDC, CDC will alert Contractor and users immediately and then request Contractor to scrub the data within their environment to eliminate the PII. Once the PII is removed, the Contractor will send an updated replacement file. CDC will destroy data containing PII.

Technical requirements for monthly data deliveries to CDC

Data Transfer Protocol Requirements:

1. Contractor shall specify their preferred protocol for data transfer.
2. Encryption and security measures for data in transit shall be detailed.
3. Contractor shall specify whether they will push the data or if it will require CDC to pull the data. CDC prefers the contractor to deliver data to CDC's publicly accessible cloud environment.
4. Contractor shall define the frequency and timing of data transfers.
5. See **Appendix A** for CDC preferred data transfer Protocol in details.

Data Transfer Security Requirements:

1. Contractor shall provide detailed protocols for the secure exchange of credentials or secrets.

2. Compliance with security standards such as OAuth or API key usage shall be clearly outlined in the intended methodologies.
3. Contractor shall transfer the data using a secure method in accordance with all applicable CDC and HHS data security and privacy regulations.

Data Content Delivery Requirements:

Contractor shall deliver the cumulative data extracts from 2016 through the most recent data available, with each data delivery following the delivery cadence outlined in the contract (i.e., monthly).

SECTION 5 – TASKS TO BE PERFORMED

C.5.1 Task One (1) – Comprehensive Healthcare Database and Social Determinants of Health (SDOH) Data License and Extracts

The Contractor shall provide CDC with necessary license(s) for full and complete access to and use of the entire Comprehensive Healthcare Database that includes facility data, patient and administrative data, visit-level diagnosis and procedure codes, itemized billing and chargemaster data, general laboratory results data, microbiology laboratory results data, and vital measurement data for inpatient and hospital-based encounters within a single, integrated database. The database shall, at a minimum, meet the requirements specified in Section 3 and include the data elements listed below. If any listed data elements are not available as specified, Contractor shall indicate such in their proposal and provide alternatives.

The Contractor shall also provide CDC with necessary license for full and complete access to and use of the Social Determinants of Health (SDOH) data. The SDOH data shall be linkable to the Comprehensive Healthcare Database at the patient level using unique patient identifier. The SDOH data shall, at a minimum, meet the requirements specified in Section 3 and include the data elements listed below. If any listed data elements are not available as specified, Contractor shall indicate such in their proposal and provide alternatives.

The Contractor shall deliver the most recent, full extracts of the Comprehensive Healthcare Database and SDOH data to CDC each month during the period of performance (12 total deliveries). The Contractor shall deliver the data extracts in accordance with technical requirements provided in Section 4. The Contractor shall provide available metadata with each data delivery to allow CDC to validate and have confidence in data quality. To the degree possible and reasonable, the Contractor shall provide metadata in a CDC-requested format. The Contractor shall provide an electronic data dictionary and contents listing with the initial data delivery and each time there is a change to the database format or contents.

Comprehensive Healthcare Database – minimum data elements

Hospital and Facility Data:

1. De-identified Provider ID;
2. Urban versus rural designation;
3. Teaching status;
4. Bed size;
5. U.S. Census region;
6. U.S. Census division;
7. U.S. State;
8. First three digits of ZIP code (zip3);
9. Monthly number of outpatient and inpatient encounters;
10. Provider and discharge month-level weights.

Patient & Administrative Data:

1. De-identified Discharge ID (use this field to link a patient's hospital visit across data files);
2. De-identified Unique Patient ID (use this field to track a patient across multiple visits within the same hospital system, including inpatient and outpatient visits);
3. Patient Validation Indicator;
4. Discharge date (mm/dd/yyyy);
5. Admission date (mm/dd/yyyy);
6. Discharge month;
7. Provider ID (de-identified);

8. Inpatient versus Outpatient visit indicator;
9. Patient type;
10. Medicare Severity Diagnosis related groups (MS-DRG);
11. MS-DRG major diagnostic category (MDC);
12. Point of Origin;
13. Admission type;
14. Discharge status and disposition;
15. Marital Status;
16. Age at time of admission (if age is greater than 89, age is adjusted to 89);
17. Sex;
18. Race (Reported as White, Black, Asian, Other, Unknown);
19. Ethnicity (Reported as Hispanic, Non-Hispanic, Other/Unknown);
20. Admitting physician specialty;
21. Admitting physician de-identified linking identifier;
22. Attending physician specialty;
23. Attending physician de-identified linking identifier;
24. Primary payer;
25. Length of stay;
26. Total charges;
27. Total cost;
28. Total fixed cost;
29. Total variable cost;
30. Publish type of hospital encounter (indicates whether the encounter has passed all validity checks including financial reconciliation, whether or nor not total bill and costs will be assigned as final)

International Classification of Diseases, Tenth Revision (ICD-10) Diagnosis and Procedure Data:

1. De-identified Discharge ID (use this field to link a patient's hospital visit across data files);
2. ICD-10 Diagnosis related information – ICD-10-Clinical Modification (ICD-10-CM):
    a. Primary ICD-10-CM diagnosis code and description;
    b. All secondary ICD-10-CM diagnosis codes and descriptions reported by the hospital;
    c. Admitting ICD-10-CM diagnosis code (if provided by the hospital);
    d. Major category code and description;
3. ICD-10 Procedure related information – ICD-10 Procedure coding system (ICD-10 PCS):
    a. Primary ICD-10 PCS procedure code and description;
    b. All secondary ICD-10 PCS procedure codes and descriptions reported by the hospital;
    c. Procedure date;
    d. Procedure physician specialty;
    e. Procedure physician de-identified linking identifier;

Current Procedural Terminology (CPT) Data:

1. De-identified Discharge ID (use this field to link a patient's hospital visit across data files);
2. All CPT4 codes and descriptions reported by the hospital.

Billing and Chargemaster Data:

1. De-identified Discharge ID (use this field to link a patient's hospital visit across data files);
2. Hospital specific charge master id and description;
3. Standard Charge Master code and description;
4. Clinical Detail code and description;
5. Date of Service (mm/dd/yyyy);
6. Standard Quantity (to be used with the Standard charge master description);
7. Clinical Detail Quantity (to be used with the Clinical detail description);
8. Billing charges;
9. Billing cost;
10. Billing fixed cost;
11. Billing variable cost;
12. Standard Department Code and description;
13. Pharmacy, Central Supply, Laboratory, Diagnostic Imaging, Surgery, etc.;

14. Pharmacy billing information, including:
    a. Drug name (generic);
    b. Drug strength (from Standard Charge Master Description);
    c. Drug therapeutic class;
    d. Route of administration (oral, parenteral, topical).

General Laboratory Results File from a subset of >350 facilities that submit data:

1. Specimen source SNOMED Code;
2. Specimen source SNOMED Description;
3. Collection Day Number;
4. Collection Time of Day;
5. Lab Test LOINC code;
6. Lab Test LOINC description;
7. Lab Test Result;
8. Result Unit;
9. Flags;
10. Result Day Number;
11. Result Time of Day;
12. Reference Interval;
13. Numeric Value;
14. Numeric Value Operator.

Microbiology Laboratory Results File from a subset of >350 facilities that submit data:

1. Specimen ID;
2. Test day and time of collection;
3. Test name;
4. Observation (test result);
5. Sensitivity data for positive test results;
6. Organism;
7. Drug tested;
8. Interpretation;
9. Minimal inhibitory concentration (MIC).

Vital Measurements Data from a subset of >140 facilities that submit data:

1. Facility Test Name;
2. Systolic Blood Pressure;
3. Pulse;
4. Temperature;
5. Diastolic Blood Pressure;
6. Oxygen Saturation Level;
7. Respiration Rate;
8. Height;
9. Weight;
10. LOINC Description;
11. LOINC;
12. Observation Day and Time;
13. Observation Result.

Social Determinants of Health Data – minimum data elements

American Community Survey data by ZCTA:

1. Value (absolute or decile) of average household size;
2. Value (absolute or decile) of Gini index of income inequality;
3. Value (absolute or decile) of median household income;
4. Value (absolute or decile) of weighted average of highest level of education achieved (less than high school, high school, associate degree, bachelor's degree, and graduate degree)

CDC/ATSDR Social Vulnerability Index variables by County Level:

1. Percentile (absolute or decile) ranking: Theme 1, socioeconomic;
2. Percentile (absolute or decile) ranking: Theme 2, household composition;
3. Percentile (absolute or decile) ranking: Theme 3, minority status/language theme;
4. Percentile (absolute or decile) ranking: Theme 4, housing/transportation;
5. Percentile (absolute or decile) ranking for overall SVI.

C.5.2 Task Two (2) – Long-Term Mortality Data License and Monthly Extracts (OPTIONAL)

The Contractor shall provide CDC with necessary license(s) for full and complete access to and use of the Long-term Mortality data table. Long-term Mortality shall be assessed through privacy-preserving tokenized linkage to multiple third-party mortality data sources (i.e., government mortality databases, private obituary data, private claims data) to capture vast majority of deaths that occur in the United States. The Long-term Mortality data table shall contain: unique patient identifier; date of death for patients who died in-hospital or were identified as deceased through third-party mortality data sources; and an indicator of whether or not patients were able to be tokenized for linkage to the third-party mortality data. The Long-term Mortality data table shall be linkable to the Comprehensive Healthcare Database at the patient level using unique patient identifiers and contain information from 2016 through the most recent records available to the Contractor. The Long-term Mortality data table shall be delivered to CDC monthly and in the same manner as the Comprehensive Healthcare Database and SDOH data table.

Mortality Data:

1. Person Key
2. Date of Death
3. Tokenized Person – Yes, No

C.5.3 - Task Three (3) - Training, Monthly Calls, and Technical Support for Tasks 1 and 2

Contractor shall provide four (4) hours of virtual, web-based training to CDC staff. The trainings shall cover a range of introductory, intermediate, and advanced topics that will be mutually decided upon by Contractor and CDC. Trainings will be scheduled at mutually agreed upon dates and times. Contractor will coordinate with CDC to develop the training agendas, learning objectives, and content, including hands-on training as appropriate.

Contractor shall meet monthly with the CDC COR and other CDC staff (e.g., scientist, training coordinator, data manager) to discuss contractual issues, data related issues, and other topics of interest.

Contractor shall provide technical support to the CDC Data Hub technical teams (e.g., when data delivery issues arise) and to CDC scientific staff on data-related questions, when necessary.

SECTION 6 – PLACE OF PERFORMANCE AND CONTRACT SUPPORT HOURS

SUBSECTION A – PLACE OF PERFORMANCE

All work shall be conducted at the Contractor's worksite / facility.

SUBSECTION B – CONTRACT SUPPORT HOURS

Contractor shall be available Monday through Friday between 9 AM and 5 PM (EST) except for federal holidays.

SECTION 7 – DELIVERABLES/REPORTING SCHEDULE

Contract Work	Associated Deliverable	Description	Required Frequency / Delivery Date	Delivery Method

TASK 1	Comprehensive Healthcare Database and Social Determinants of Health (SDOH) Data Extracts		Monthly, within five (5) business days of the data release date.	CDC cloud environment. Notification to the Contracting Officer's Representative (COR) via email.
TASK 2 (OPTIONAL)	Long-Term Mortality Data		Monthly, within five (5) business days of the data release date.	CDC cloud environment. Notification to the Contracting Officer's Representative (COR) via email.
TASK 3	Trainings/ Monthly Calls /Technical Support	Four (4) hours of virtual, web-based training Monthly Meetings with COR and relevant CDC staff. Technical Support, as needed.	Four (4) hours of training at mutually agreed upon dates for each period of performance.	Virtual via Microsoft Teams or similar platform.
TASKS 1, 2, 3	Monthly Report	Dates of all data deliveries, also indicate any problems with deliveries.	Monthly, by the 5th working day of each month.	Send to the Contracting Officer's Representative (COR) via email.

Contractor shall ensure that data extracts described in Task 1 and Task 2 are delivered to CDC Data Hub each month within five (5) business days of the data release date and that the CDC COR and the Data Management Lead receive an email from Contractor indicating data has been delivered.

SUBSECTION A – QUALITY ASSURANCE PERFORMANCE PLAN (QASP)

Work Requirement / Performance Standard	**Acceptable Quality Level Surveillance Method**	**Incentive for Meeting**	**Performance Standard**
Provision of data in format and within delivery schedule	Deliverables provided in accordance with contract requirements, at an acceptable quality with 90% compliance within each contract period.	Surveillance by Assigned CDC Contracting Officer's Representative (COR)	- Contractor's performance is documented as past performance using CPARS which is considered for future awards. - Performance is considered in determining whether to exercise the option periods.

SECTION 8 – MINIMUM CONTRACTOR QUALIFICATIONS

The Contractor shall have the following:
i. Receiving and managing encounter- and patient-level data from >1,400 geographically diverse hospitals with ability for patients to be tracked longitudinally (both retrospectively and prospectively) across visits within the inpatient and hospital-based outpatient settings, with a unique identifier within a single hospital or healthcare system.
ii. Managing a dynamic healthcare database that is extracted on a regular basis (e.g., weekly, bi-weekly, monthly), is relatively recent (i.e., most encounters incorporated into database within 2-3 months), and can be transferred to CDC every month (for Base and Option Years 1, 2, 3, and 4, if exercised) for timely analysis of public health issues and threats.
iii. Operating as a healthcare improvement organization with a large alliance that includes a geographically diverse and representative subset of U.S. hospitals and other provider organizations that submit a log of billed items, including procedures, medications, laboratory test performed, diagnostic and therapeutic services at the individual patient level, patient demographic information, visit costs and charges, discharge information including length of stay and diagnosis codes, and microbiology laboratory results.
iv. Managing healthcare data containing information on a large number of U.S. hospitals that includes
information on hospital characteristics such as geographic region, three-digit ZIP code, bed size, teaching status, and urban or rural designation.

SECTION 9 – PROPOSED CONTRACT TYPE

The anticipated contract type is a Firm Fixed Priced Supply Contract.

SECTION 10 – POINT OF CONTACT INFORMATION

CDC Contracting Officers Representative (COR):

Ms. Janet Phillips

Telephone: (404) 498-2462

Email: iru5@cdc.gov

SECTION 11 – ADDITIONAL REQUIREMENTS

Information Security and Privacy
A. Baseline Security Requirements
1) Applicability. The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:
a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.
b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) employee will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
2) Safeguarding Information and Information Systems. In accordance with the Federal Information Processing Standards Publication (FIPS)199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) shall:
a. Protect government information and information systems in order to ensure:
• Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
• Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
• Availability, which means ensuring timely and reliable access to and use of information.
b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the

Contractor on behalf of HHS regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, within one (1) hour or less after it is determined that a threat or hazard exists, bring the situation to the attention of the other party.
c. Adopt and implement the policies, procedures, controls, and standards required by the HHS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the HHS Information Security Program security requirements, outlined in the HHS Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing fisma@hhs.gov.
d. Comply with the Privacy Act requirements and tailor FAR clauses as needed.
3) Information Security Categorization. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C, and based on information provided by the ISSO, CISO, or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

	Confidentiality (Low, Moderate, High)	Integrity (Low, Moderate, High)	Availability (Low, Moderate, High)
Security Objectives Impact Level: (NIST SP 800-60)	Moderate	Moderate	Moderate
Security Objectives Impact Level: (If System/Information Owner need to downgraded / upgraded risk)			
Overall Impact Level (Low, Moderate, High)	Moderate	Moderate	Moderate

Based on information provided by the ISSO, Privacy Office, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:
[**X**] No PII [ ] Yes PII
4) Personally Identifiable Information (PII). Per the Office of Management and Budget (OMB) Circular A-130, "PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: social security number, date and place of birth, mother's maiden name, biometric records, etc.
PII Confidentiality Impact Level has been determined to be: **N/A** [ ] Low [ ] Moderate [ ] High
5) Controlled Unclassified Information (CUI). CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with Executive Order 13556, Controlled Unclassified Information, (implemented at 32 CFR, part 2002) when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "handling" refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:
a. marked appropriately;
b. disclosed to authorized personnel on a Need-To-Know basis;
c. protected in accordance with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and
d. returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, Guidelines for Media Sanitization.
6) Protection of Sensitive Information. For security purposes, information is or may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, Protection of Sensitive Agency Information by securing it with a FIPS 140-2 validated solution.
7) Confidentiality and Nondisclosure of Information. Any information provided to the Contractor (and/or any subcontractor) by HHS or collected by the Contractor on behalf of HHS shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.
The confidentiality, integrity, and availability of such information shall be protected in accordance with HHS and [CDC] policies. Unauthorized disclosure of information will be subject to the HHS/[CDC] sanction policies and/or governed by the following laws and regulations:

a. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
b. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
c. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).
8) Internet Protocol Version 6 (IPv6). All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6).
9) Government Websites. All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.
10) Contract Documentation. The Contractor shall use provided templates, policies, forms, and other agency documents to comply with contract deliverables as appropriate.
11) Standard for Encryption. The Contractor (and/or any subcontractor) shall:
a. Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.
b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.
c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and CDC-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).
d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR.
e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to CDC Office of Chief Information Security Officer (OCISO).
12) Contractor Non-Disclosure Agreement (NDA). Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the CDC non-disclosure agreement, as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.
13) Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
a. The Contractor shall assist the CDC SOP or designee in reviewing the PIA at least every three years throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the CDC SOP that a review is required based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are
collected that could introduce new or increased privacy risks), whichever comes first.
B. Training
1) Mandatory Training for All Contractor Staff. All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS/CDC Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete CDC Security Awareness Training (SAT), Privacy, and Records Management training at least annually, during the life of this contract. All provided training shall be compliant with HHS training policies.
2) Role-based Training. All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training (RBT) within 60 days of assuming their new responsibilities. Thereafter, they shall complete RBT at least annually in accordance with HHS policy and the HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum.
All HHS employees and Contractors with SSR who have not completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.
3) Training Records. The Contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records shall be provided to the CO and/or COR within 30 days after contract award and annually thereafter or upon request.
C. Rules of Behavior
1) The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the HHS Information Technology General Rules of Behavior.
2) All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least annually thereafter, which may be done as part of annual CDC Security Awareness Training. If the training is provided by the Contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.
D. Incident Response
FISMA defines an incident as “an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law,

security policies, security procedures, or acceptable use policies. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines incidents as events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an "other than" authorized purpose.

OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) states:

Definition of an Incident:

An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Definition of a Breach:

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

It further adds:

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for an other than authorized purpose.

The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines a breach as "a suspected or confirmed incident involving PII".

Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC shall include the following requirements:

1) The Contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage a suspected or confirmed breach.

2) All Contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all Contractors and subcontractors shall protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.

3) All Contractors and subcontractors shall participate in regular training on how to identify and report a breach.

4) All Contractors and subcontractors shall report a confirmed breach in any medium as soon as possible and no later than 1 hour after it is determined that a breach occurred, consistent with applicable CDC IT acquisitions guidance, HHS/CDC and incident management policy, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines. To this end, the Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) or CDC Computer Incident Response Team (CSIRT) within 24 hours via email at csirt@cdc.gov or telephone at 866-655-2245, whether the response is positive or negative.

5) All Contractors and subcontractors shall be able to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.

6) All Contractors and subcontractors shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with HHS/CDC Policy and the HHS/CDC Breach Response Plan and to assist with responding to a breach.

7) Cloud service providers shall use guidance provided in the FedRAMP Incident Communications Procedures when deciding when to report directly to US-CERT first or notify CDC first.

8) Identify roles and responsibilities, in accordance with HHS/CDC Breach Response Policy and the HHS/CDC Breach Response Plan. To this end, the Contractor shall NOT notify affected individuals unless and until so instructed by the Contracting Officer or designated representative. If so, instructed by the Contracting Officer or representative, all notifications must be pre-approved by the appropriate CDC officials, consistent with HHS/CDC Breach Response Plan, and the Contractor shall then send CDC- approved notifications to affected individuals; and,

9) Acknowledge that CDC will not interpret report of a breach, by itself, as conclusive evidence that the Contractor or its subcontractor failed to provide adequate safeguards for PII.

E. Position Sensitivity Designations

The ISSO in coordination with the requiring activity representative and Personnel Security Offices, determine the applicable position designations using OPM's Position Sensitivity Designation Automated Tool (*https://www.opm. gov/investigations/*). The following are position sensitivity levels that may apply to this solicitation/contract:

Investigation	Position Requirement
NACI	National Agency Check
Tier 1	Low-Risk Non-Sensitive, including HSPD-12 Credentialing
Tier 2 *(with subject interview)*	Moderate-Risk Public Trust (MRPT)

Tier 3	Non-Critical Sensitive, National Security, including Secret and "L" access eligibility
Tier 4	High-Risk Public Trust
Tier 5	Critical Sensitive and Special Sensitive, National Security, including Top Secret, SCI, and "Q" access eligibility
☒**Not Applicable**	**No Requirement**

F. Homeland Security Presidential Directive (HSPD)-12
The Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; and Executive Order 13467, Part 1 §1.2.
For additional information, see HSPD-12 policy at: https://www.dhs.gov/homeland-security-presidential-directive-12)
Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO by the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted immediately upon change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.
If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.
G. Contract Initiation and Expiration
1) General Security Requirements. The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the Contractor shall follow the HHS EPLC framework and methodology and in accordance with the HHS Contract Closeout Guide (2012).
2) System Documentation. Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, Security Considerations in the System Development Life Cycle, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
3) Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization.
4) Notification. The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO before an employee stops working under this contract.
5) Contractor Responsibilities Upon Physical Completion of the Contract. The Contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or CDC policies.
6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Out-Processing Checklist (http://intranet.cdc.gov/od/hcrmo/pdfs/hr/Out_Processing_Checklist.pdf) when an employee terminates work under this contract. All documentation shall be made available to the CO and/or COR upon request.
H. Records Management and Retention
The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS policies and shall not dispose of any records unless authorized by HHS.
In the event that a Contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS policies.

Human Subjects Protections in Research
N/A

Paperwork Reduction Act (PRA)
N/A

Section 508 and Accessibility Requirements

Part A – Provision

Reference HHSAR 352.239-78 Electronic Information and Communication Technology Accessibility Notice.

(Deviation)

(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-79 Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards, offerors must submit an appropriate HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), in accordance with the completion instructions. The purpose of the checklists and conformance reports are to assist HHS acquisition and program officials in determining whether proposed ICT supplies, products, platforms, information, and documentation conform to applicable Section 508 accessibility standards. Checklists and ACRs evaluate—in detail—whether the ICT conforms to specific Section 508 accessibility standards and identifies remediation efforts needed to address conformance issues.

(c) If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies, products, platforms, information, documentation, or services support delivered do not conform to the described accessibility standards, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(d) In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit an Accessibility Conformance Report, in accordance with its completion instructions and tailored to the requirements in the solicitation. The purpose of the Report is to assist HHS acquisition and program officials in determining whether proposed ICT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document, in detail, whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the Template are available at https://www.section508.gov/.

(e) Additionally, offerors must provide enough information to assist the Government in determining that the ICT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(f) Respondents to this solicitation must identify any inability to conform to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(g) Items delivered as electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/. Materials, other than items incidental to contract management, that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Contracting Officer's Representative.

(End of provision)

Part B - Clause

HHSAR 352.239-79 Electronic, Information, and Communication Technology Accessibility.

(Deviation)

(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all information and communication technology (ICT) supplies, products, platforms, information, documentation, and services, or support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508

Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at https://www.access-board.gov/ict/. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) Additional Section 508 accessibility standards applicable to this contract or order are identified as follows:

205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
503 Applications
504 Authoring Tools
602 Support Documentation
603 Support Services

If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(d) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies, products, platforms, information, documentation, or services support will define the specifications and accessibility standards for the order. In those cases, the Contractor shall be required to provide a completed HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an ACR (based on the VPAT see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies, products, platforms, information, documentation, or services support conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) The contractor shall identify to the Contracting Officer any perceived exception or exemption to Section 508 requirements for review by the agency Section 508 Program.

(End Clause)

SECTION G - CONTRACT ADMINISTRATION DATA

352.232-71 Electronic Submission of Payment Requests (APR 2026) (RFO DEVIATION)

(a) Definitions. As used in this clause -

Payment request means a bill, voucher, invoice, or request for contract financing payment with associated supporting documentation. The payment request must comply with the requirements in FAR 32.905(b) and the applicable payment clause included in this contract.

(b) Submission instructions. Except as provided in paragraph (c) of this clause, the Contractor must submit payment requests

electronically using the Department of Treasury Invoice Processing Platform (IPP) or successor system. Information regarding IPP, including IPP Customer Support contact information, is available at www.ipp.gov or any successor site.

(c) Alternate submission procedures. The Contractor may submit payment requests using other than IPP only when the Contracting Officer authorizes alternate procedures in writing.

(d) Submission of alternate payment procedures authorization. If alternate payment procedures are authorized, the Contractor must include a copy of the Contracting Officer's written authorization with each payment request.

(End of clause)

CDCG.02 Contracting Officer's Representative (COR) (Jul 2017)

Performance of the work hereunder shall be subject to the technical directions of the designated COR for this contract.

As used herein, technical directions are directions to the Contractor which fill in details, suggests possible lines of inquiry, or otherwise completes the general scope of work set forth herein. These technical directions must be within the general scope of work and may not alter the scope of work or cause changes of such a nature as to justify an adjustment in the stated contract price/cost, or any stated limitation thereof.

In the event that the Contractor believes full implementation of any of these directions may exceed the scope of the contract, he or she shall notify the originator of the technical direction and the Contracting Officer, immediately or as soon as possible, in a letter or e-mail separate of any required report(s). No technical direction, nor its fulfillment, shall alter or abrogate the rights and obligations fixed in this contract.

The Government COR is not authorized to change any of the terms and conditions of this contract. Contract changes shall be made only by the Contracting Officer through properly written modification(s) to the contract.

The Government will provide the Contractor with a copy of the COR delegation memorandum upon request.

CDCG.03 Contracting Officer (Jul 1999)

(a) The Contracting Officer is the only individual who can legally commit the Government to the expenditure of public funds. No person other than the Contracting Officer can make any changes to the terms, conditions, general provisions, or other stipulations of this contract.

(b) No information, other than that contained in an authorized modification to this contract, duly issued by the Contracting Officer, received from any person employed by the United States Government, or otherwise, shall be considered grounds for deviation from any stipulation of this contract.

CDCG.07 Payment by Electronic Funds Transfer (Jan 2026)

(a) The Government shall use electronic funds transfer to the maximum extent possible when making payments under this contract. FAR 52.232-33, Payment by Electronic Funds Transfer –System for Award Management, requires the contractor to designate in writing a financial institution for receipt of electronic funds transfer payments.

(b) In the case that EFT information is not within the System of Award Management, FAR 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management, requires mandatory submission of Contractor's EFT information directly to the office designated in this contract to receive that information (hereafter: "designated office"); see below. The contractor shall submit the EFT information within the form titled "ACH Vendor/Miscellaneous Payment Enrollment Form" to the address indicated below. Note: The form is either attached to this contract (see Section J, List of Attachments) or may be obtained from the CDC Office of Financial Resources at 678-475-4500 or cpbapinv@cdc.gov.

(c) In cases where the contractor has previously provided such information, i.e., pursuant to a prior contract/order, and been enrolled in the program, the form is not required unless the designated financial institution has changed.

(d) The completed form shall be mailed or sent via facsimile after award, but no later than 15 calendar days before an invoice is submitted, to the following address:

The Centers for Disease Control and Prevention Office of Financial
Resources (OFR)
P.O. Box 15580 Atlanta, GA 30333

SECTION H - SPECIAL CONTRACT REQUIREMENTS

352.239-73 Electronic Information and Technology Accessibility Notice (DEC 2015).

SECTION 508 COMPLIANCE

Electronic and Information Technology Accessibility Notice

(a) Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 and the Architectural and Transportation Barriers Compliance Board Electronic and Information (EIT) Accessibility Standards (36 CFR part 1194), require that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

(b) Accordingly, any Contractor responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at http://www.hhs.gov/web/508. The complete text of the Section 508 Final Provisions can be accessed at http://www.access-board.gov/sec508/standards.htm.

(c) The Section 508 accessibility standards applicable to this contract are: 1194
205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
504 Authoring Tools
602 Support Documentation
603 Support Services

In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, Contractors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows Contractors or developers to self-evaluate their supplies and documentation detail - whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS Web site http://hhs.gov/web/508.

(d) Respondents to this solicitation must identify any exception to Section 508 requirements. If an Contractor claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(e) Electronic content must be accessible to HHS acceptance criteria. Checklist for various formats is available at http://508.hhs.gov/, or from the Section 508 Coordinator listed at https://www.hhs.gov/web/section-508/additional-resources/section-508-contacts/index.html. Materials that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Representative.

Part A – Provision

Reference HHSAR 352.239-78 Electronic Information and Communication Technology Accessibility Notice.

(Deviation)

(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-79 Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards, offerors must submit an appropriate HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), in accordance with the completion instructions. The purpose of the checklists and conformance reports are to assist HHS acquisition and program officials in determining whether proposed ICT supplies, products, platforms, information, and documentation conform to applicable Section 508 accessibility standards. Checklists and ACRs evaluate—in detail—whether the ICT conforms to specific Section 508 accessibility standards and identifies remediation efforts needed to address conformance issues.

(c) If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies, products, platforms, information, documentation, or services support delivered do not conform to the described accessibility standards, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(d) In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit an Accessibility Conformance Report, in accordance with its completion instructions and tailored to the requirements in the solicitation. The purpose of the Report is to assist HHS acquisition and program officials in determining whether proposed ICT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document, in detail, whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the Template are available at https://www.section508.gov/.

(e) Additionally, offerors must provide enough information to assist the Government in determining that the ICT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(f) Respondents to this solicitation must identify any inability to conform to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(g) Items delivered as electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/. Materials, other than items incidental to contract management, that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Contracting Officer's Representative.

Part B - Clause

HHSAR 352.239-79 Electronic, Information, and Communication Technology Accessibility.

(Deviation)

(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all information and communication technology (ICT) supplies, products, platforms, information, documentation, and services, or support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508

Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at https://www.access-board.gov/ict/. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) Additional Section 508 accessibility standards applicable to this contract or order are identified as follows:

205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
503 Applications
504 Authoring Tools
602 Support Documentation
603 Support Services

If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(d) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies, products, platforms, information, documentation, or services support will define the specifications and accessibility standards for the order. In those cases, the Contractor shall be required to provide a completed HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an ACR (based on the VPAT see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies, products, platforms, information, documentation, or services support conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) The contractor shall identify to the Contracting Officer any perceived exception or exemption to Section 508 requirements for review by the agency Section 508 Program.

CDCH.10 Artificial Intelligence Compliance and Risk Management Plan (May 2026)

The use of Artificial Intelligence (AI), including GenAI, is prohibited without an approved AI Compliance and Risk Management Plan. The contractor is responsible for updating the AI Compliance and Risk Management Plan throughout the life of the contract as changes occur. If a change to AI use, AI functionality, AI model, or deployment configuration is anticipated, the contractor must notify the contracting officer and Contracting Officer's Representative (COR) immediately and provide a revised plan. The government will issue approval or disapproval before AI can be incorporated. The offeror must identify whether the planned or potential AI use may involve a high-impact AI use case (as defined in defined in Appendix A of OMB-M-25-21) and must provide sufficient descriptive information for the Government to complete any required AI impact or high-impact assessment.

The AI Compliance and Risk Management Plan must:

1. Identify the specific tasks or functions where AI will be used.
2. Explain how logs, audits, or other forms of AI generated data will be stored, used, retained, or deleted.
3. State whether the AI technologies are open-source, proprietary, or any other type.
4. Include applicable model cards or system documentation describing the AI technologies used.
5. Describe how bias in AI models and outputs will be identified, monitored, and mitigated, including the origin, quality, and weighting of data.
6. Explain the AI safeguards in place, including compliance and risk management practices, protections against unauthorized data access, and steps taken to manage bias and reduce risk in alignment with applicable AI policies and directives.
7. Describe internal policies governing AI use, including transparency, accountability, data integrity, accuracy, protection of sensitive or proprietary information, foreseeable risks, and potential social impacts.
8. Explain how the contractor will assess and prevent unfair or disparate impacts, address privacy, civil rights, and civil liberties concerns, and prevent misuse, unauthorized use, or corruption of AI systems.
9. Confirm that the AI solution will not make or support decisions based on unlawful discrimination in violation of federal civil rights laws, including Title VII of the Civil Rights Act, the Americans with Disabilities Act (ADA), and the Age Discrimination in Employment Act (ADEA).
10. Describe how applicable technological or voluntary consensus standards will be incorporated to reduce acquisition and operational risk
11. The plan must describe how Government data, outputs, prompts, logs, and outputs be accessed, used, protected, retained, deleted, and transferred, and identify any proposed limitations on Government rights, access, or reuse.
12. The AI Compliance and Risk Management Plan will be reviewed by the Government and an approval or disapproval issued.

CDCH.14 Records Management Obligations (Jun 2020)

A. *Applicability*

The following applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. *Definitions*

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes Centers for Disease Control and Prevention (CDC) records.
2. does not include personal materials.
3. applies to records created, received, or maintained by Contractors pursuant to their CDC contract.
4. may include deliverables and documentation associated with deliverables.

C. *Requirements*

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.
3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient

technical documentation to permit understanding and use of the records and data.

4. CDC and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of CDC or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to the Contracting Officer and the Contracting Officer's Representative. The agency must report promptly to NARA in accordance with 36 CFR 1230.
5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to CDC control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
6. The 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, contracts. The Contractor (and any sub-contractor) is required to abide by Government and CDC guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.
7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with CDC policy.
8. The Contractor shall not create or maintain any records containing any non-public CDC information that are not specifically tied to or authorized by the contract.
9. The 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 from public disclosure by an exemption to the Freedom of Information Act.
10. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take CDC-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. *Flowdown of requirements to subcontractors*

1. The Contractor shall incorporate the entire substance of the terms and conditions herein, including this paragraph, in all subcontracts under this contract, and must require written subcontractor acknowledgment of same.
2. Violation by a subcontractor of any provision set forth herein will be attributed to the Contractor.

CDCH.23 Evaluation of Contractor Performance Utilizing CPARS (Apr 2026)

In accordance with FAR 42.11, Centers for Disease Control and Prevention (CDC) will review and evaluate contract performance. FAR 42.802 and 42.1102 requires agencies to prepare evaluations of contractor performance and submit them to the Contractor Performance Assessment Reporting System (CPARS). CDC utilizes this web-based system to prepare and report contractor performance evaluations. All information contained in these assessments may be used by the Government, within the limitations of FAR 42.11, for future source selections in accordance with FAR 15.104 where past performance is an evaluation factor.

The CPARS system requires a contractor representative to be assigned so that the contractor has appropriate input into the performance evaluation process. The CPARS contractor representative will be given access to CPARS and will be given the opportunity to concur or not-concur with performance evaluations before the evaluations are complete. The CPARS contractor representative will also have the opportunity to add comments to performance evaluations.

The assessment is not subject to the Disputes clause of the contract, nor is it subject to appeal beyond the review and comment procedures described in the guides on the CPARS website. Refer to: www.cpars.gov for details and additional information related to CPARS, CPARS user access, how contract performance assessments are conducted, and how contractors participate. Access and training for all persons responsible for the preparation and review of performance assessments is also available at the

CPARS website.

The contractor must provide the CDC contracting office with the name, e-mail address, and phone number of their designated CPARS representative who will be responsible for logging into CPARS and reviewing and commenting on performance evaluations. The contractor must maintain a current representative to serve as the contractor representative in CPARS. It is the contractor's responsibility to notify the CDC contracting office, in writing (letter or email), when their CPARS representative information needs to be changed or updated. Failure to maintain current CPARS contractor representative information will result in the loss of an opportunity to review and comment on performance evaluations.

SECTION I - CONTRACT CLAUSES

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 2024)

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):

Federal Acquisition Regulation Overhaul (RFO) - https://www.acquisition.gov/far-overhaul

FAR SOURCE TITLE AND DATE
52.204-13 System for Award Management Maintenance (DEVIATION April 20, 2026)

52.212-4 Terms and Conditions—Commercial Products and Commercial Services (DEVIATION DATE April 20, 2026).

TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DEVIATION DATE)

(a) *Definitions*. The clause at Federal Acquisition Regulation (FAR) 52.202-1, Definitions, is incorporated by reference.

(b) *Inspection/Acceptance*. The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post acceptance rights—

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(c) *Assignment*. The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (*e.g.,* use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(d) *Changes*. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(e) *Disputes*. This contract is subject to 41 U.S.C. chapter 71, Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal, or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause FAR 52.233-1, Disputes, which is incorporated in this contract by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(f) *Excusable delays*. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence. Examples of occurrences include acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. When an excusable delay occurs, the Contractor shall—

(1) Notify the Contracting Officer in writing as soon as possible;

(2) Remedy the delay as quickly as possible; and

(3) Notify the Contracting Officer when the occurrence is over.

(g) Invoice. The Government will handle invoices according to the Prompt Payment Act (31 U.S.C. 3903) and 5 CFR part 1315. The Contractor shall submit invoices to the address designated in the contract to receive invoices. An invoice must include the information required by 5 CFR part 1315.9(b).

(h) *Patent indemnity*. The Contractor shall indemnify the Government and its officers, employees, and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark, or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) *Payment*—

(1) *Items accepted*. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) *Prompt payment*. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(3) *Discount*. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date that appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(4) *Overpayments*. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall—

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—

(A) Circumstances of the overpayment (*e.g.*, duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected line item or subline item, if applicable;

(D) Contractor point of contact; and

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(5) *Interest*.

(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) *Final decisions*. The Contracting Officer will issue a final decision as required by FAR part 33 if–

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see FAR part 32).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a termination for cause.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on-

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures for interest credits prescribed in FAR part 32 in effect on the date of this contract.

(j) *Risk of loss*. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon—

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes*. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience*. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause*. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. The Government will send a cure notice to the Contractor, unless the reason for the termination is late delivery. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title*. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty*. The Contractor warrants and implies that the items delivered under this contract are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability*. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Compliance with laws unique to Government contracts*. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 49 U.S.C. 40118, Government-financed air transportation; and 41 U.S.C. chapter 21 relating to procurement integrity.

(r) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services;

(2) The Disputes, Payments, Invoice, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause;

(3) Other contract clauses incorporated in the solicitation or contract;

(4) Addenda to this solicitation or contract;

(5) Solicitation provisions incorporated in the solicitation;

(6) Other paragraphs of this clause;

(7) Other documents, exhibits, and attachments; and

(8) The specification.

(s) *Unauthorized obligations*.

(1) Except as stated in paragraph (s)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(i) Any such clause is unenforceable against the Government.

(ii) Neither the Government nor any Government-authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(2) Paragraph (s)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(t) *Comptroller General examination of record*. This paragraph applies if this contract was awarded using other than sealed bid procedures and is in excess of the simplified acquisition threshold on the date of award of this contract.

(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 part 4, longer period required by statute, or periods specified in 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 clause 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.

(u) *Incorporation by reference*. The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of clause)

52.217-8 Option to Extend Services (Nov 1999).

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed ***6 months***. The Contracting Officer may exercise the option by written notice to the Contractor within ***30 days***.

(End of clause)

52.217-9 Option to Extend the Term of the Contract (Mar 2000).

(a) The Government may extend the term of this contract by written notice to the Contractor within ***1 day***; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least ***30*** **days** before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed ***5 years***.

(End of clause)

52.227-14 Rights in Data-General, Alternate II (Dec 2007).

(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 means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

Limited rights data means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

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.

Restricted rights, as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

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 rights 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, and to have or permit others to do so.

(b) Allocation of rights.

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

(i) Data first produced in the performance of this contract;

(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 limited rights data or restricted computer software in accordance with paragraph (g) 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) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) Copyright-

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

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices 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 in such copyrighted data 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 (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor-

(i) Identifies the 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 or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

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

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except-

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) Unauthorized marking of data.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g) (4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the

Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable 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. 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 proposed notice is authorized; and

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

(3) If 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.

(g) Protection of limited rights data and restricted computer software.

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall-

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) Notwithstanding paragraph (g)(1) of this clause, the contract may identify and specify the delivery of limited rights data, or the Contracting Officer may require by written request the delivery of limited rights data that has been withheld or would otherwise be entitled to be withheld. If delivery of that data is required, the Contractor shall affix the following "Limited Rights Notice" to the data and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of this clause, in accordance with the notice:

Limited Rights Notice (Dec 2007)

(a) These data are submitted with limited rights under Government Contract (**TBD)**. These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure.

(b) This notice shall be marked on any reproduction of these data, in whole or in part.

(h) *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 shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* 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)

52.240-91 Security Prohibitions and Exclusions Alternate I *(*April 20, 2026).

As prescribed in 40.205(b), insert the following clause:

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

American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the System for Award Management (SAM) at https://www.sam.gov (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Covered article, as defined in 41 U.S.C. 4713(k), means:

(1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;

(2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or

(4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

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).

FASC-prohibited unmanned aircraft system means an unmanned aircraft system manufactured or assembled by an American Security Drone Act—covered foreign entity.

FASCSA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSA) requiring removing covered articles from executive agency information systems or excluding one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201-1.303(d) and (e):

(1) The Secretary of Homeland Security may issue FASCSA orders that apply to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSA order may be referred to as a Department of Homeland Security (DHS) FASCSA order.

(2) The Secretary of Defense may issue FASCSA orders that apply to the Department of Defense (DoD) and national security systems other than sensitive compartmented information systems. This type of FASCSA order may be referred to as a DoD FASCSA order.

(3) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;

(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;

(9) The Bureau of Intelligence and Research of the Department of State;

(10) The Office of Intelligence and Analysis of the Department of the Treasury;

(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or

(12) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connecting a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Kaspersky Lab-covered article means any hardware, software, or service that—

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

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

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

Kaspersky Lab-covered entity means—

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., “Kaspersky”;

(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.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.

Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.

Subsidiary means an entity in which more than 50 percent of the entity is owned directly by a parent corporation or through another subsidiary of a parent corporation.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

Unmanned aircraft means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (49 U.S.C. 44801(11)).

Unmanned aircraft system means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12)).

(b) *Prohibitions on providing or using specific products or services in performance of contract*. Unless a waiver or exception applies, the Contractor is prohibited from providing any products or services to the Government or using in the performance of the contract any of the following:

(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor’s employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));

(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91));

(3) Covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)). This does not prohibit contractors from providing—

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

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

(c) Prohibition on unmanned aircraft systems manufactured or assembled by American Security Drone Act—covered foreign

entities.

(1) Prohibition. The Contractor is prohibited from—

(i) Delivering any FASC-prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (sections 1823 and 1826 of American Security Drone Act of 2023, within the National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.);

(ii) On or after December 22, 2025, operating a FASC-prohibited unmanned aircraft system in the performance of the contract (section 1824 of Pub. L. 118-31); and

(iii) On or after December 22, 2025, using Federal funds to procure or operate a FASC-prohibited unmanned aircraft system (section 1825 of Pub. L. 118-31).

(2) *Procedures*. The Contractor shall search SAM for the FASC-maintained list of American Security Drone Act—covered foreign entities before proposing, or using in performance of the contract, any unmanned aircraft system. Also, the Contractor shall ensure any effort or expenditure associated with a FASC-prohibited unmanned aircraft system is consistent with a corresponding exemption, exception, or waiver determination expressly stated in the contract.

(3) *Exemptions, exceptions, and waivers*. The prohibitions in paragraph (c) of this clause do not apply where the agency has determined an exemption, exception, or waiver applies, and the contract indicates that such a determination has been made. See sections 1823 through 1825 and 1832 of Public Law 118-31 for statutory requirements pertaining to exemptions, exceptions, and waivers.

(d) *Prohibition on using or providing specific products or services or conducting certain transactions regardless of connection to contract*.

(1) *Certain telecommunications and video surveillance equipment, systems, or services*.

(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot use any equipment, systems, or services 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 (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).

(ii) This prohibition applies to using covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. This does not prohibit the contractor from using—

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

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

(2) *Office of Foreign Assets Control Restrictions*.

(i) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

(ii) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas.

(A) For lists of entities and individuals subject to economic sanctions, see OFAC's List of Specially Designated Nationals and Blocked Persons at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

(B) For more information about these restrictions, as well as updates, see OFAC's regulations at 31 CFR chapter V and at https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.

(C) To conduct electronic screens of potential parties to regulated transactions, see the consolidated screening list at https://www.trade.gov/consolidated-screening-list, which consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury.

(3) *Sudan prohibition*. The Contractor is prohibited from conducting any restricted business operations in Sudan in accordance with Accountability and Divestment Act of 2007 (Pub. L. 110-174).

(4) *Iran prohibitions*.

(i) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, the contractor shall not engage in certain activities or transactions relating to Iran (section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note).

(ii) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, contractor shall not export certain sensitive technology to Iran, as determined by the President, and has an active exclusion in SAM (22 U.S.C. 8515).

(iii) The prohibition in paragraphs (d)(4)(i) and (d)(4)(ii) do not apply if the acquisition is subject to trade agreements and the

offeror certifies that all the offered products are designated country end products or designated country construction material (see part 25).

(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over $15,000) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked according to the International Emergency Economic Powers Act (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(e) *Governmentwide exclusion and removal orders*.

(1) Contractors are prohibited from providing or using as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by any applicable FASCSA orders identified by the checkbox(es) in this paragraph (e)(1).

Yes X No □ DHS FASCSA Order

Yes □ No X DoD FASCSA Order

Yes □ No X DNI FASCSA Order

(2) The Contractor shall search for the phrase "FASCSA order" in the System for Award Management (SAM) at https://www.sam.gov to locate applicable FASCSA orders.

(3) The Government may identify in the solicitation other FASCSA orders that are not in SAM, which are effective and apply to the solicitation and resulting contract.

(4) A FASCSA order issued after the date of solicitation applies to this contract only if added by an amendment to the solicitation or modification to the contract (see FAR 40.204-1(c)).

(f) *Reasonable inquiry*. The contractor shall conduct a reasonable inquiry to determine if there are any prohibited products or services. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(g) *Removal of prohibited products and services*. For Federal Supply Schedules, Governmentwide acquisition contracts, multi-agency contracts or any other procurement instrument intended for use by multiple agencies, upon notification from the Contracting Officer, during the performance of the contract, the Contractor shall promptly make any necessary changes or modifications to remove any product or service produced or provided by a source that this clause prohibits.

(h) *General report*.

(1) If the Contractor identifies or is notified by any source, (including a subcontractor at any tier), that any product or service provided or used (or to be provided or used) during contract performance does not comply with any prohibition in this clause, then the Contractor shall report the following information, or as much information is known, in writing to the contracting office as identified in paragraph (h)(2) within 72 hours:

(i) Contract number and order number, if applicable;

(ii) The specific prohibition the product or service is not complying with;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the contractor would like the Government to consider a waiver, and asks for such a waiver);

(vii) Whether alternative products or services are available that would comply with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions implemented or recommended.

(2) If a report must be submitted to a contracting office, the Contractor shall submit the report as follows:

(i) If a Department of Defense contracting office, the Contractor shall report to the website at https://dibnet.dod.mil.

(ii) For all other contracting offices, the Contractor shall report to the Contracting Officer.

(iii) For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order.

(3) If the report provided does not contain any of the information required by paragraph (h)(1) of this clause, and the contractor later discovers new information that is required by paragraph (h)(1) of this clause, then the contractor shall submit a subsequent report within 72 hours of discovering the new information.

(4) The contractor shall also report the information in paragraph (h)(1) if the contractor wishes to ask for a waiver of the requirements of a new FASCSA order being applied through modification.

(i) *New FASCSA orders report*.

(1) During contract performance, the Contractor shall review SAM at least once every three months, or as advised by the Contracting Officer, to check for covered articles subject to FASCSA order(s), or for products or services produced by a source subject to FASCSA order(s) not currently identified under paragraph (e) of this clause.

(2) If the Contractor identifies a new FASCSA order(s) that could impact their supply chain, then the Contractor shall conduct a reasonable inquiry to identify whether a covered article or product or service produced or provided by a source subject to the FASCSA order(s) was provided to the Government or used during contract performance. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(3) The Contractor shall submit a report to the contracting office identified in paragraph (h)(2) of this clause if the Contractor identifies, including through any notification by a subcontractor at any tier, that a covered article or product or service produced or provided by a source was provided to the Government or used during contract performance and is subject to a FASCSA order(s). For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order. The Contractor shall report the following information within 72 hours for each covered article or each product or service produced or provided by a source, where the covered article or source is subject to a FASCSA order:

(i) Contract number and order number, if applicable;

(ii) Name of the covered article or source subject to a FASCSA order;

(iii) The specific FASCSA order the product or service does not comply with;

(iv) The elements of (h)(1)(iii) through (ix) of this clause.

(j) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (j) but excluding subparagraphs (d)(1) and (i)(1), in all subcontracts and other contractual instruments, including subcontracts for acquiring commercial products or commercial services.

(End of clause)

Section K - Representations, Certifications, And Other Statements Of Offerors

52.240-90 Security Prohibitions and Exclusions Representations and Certifications (April 20, 2026).

(a) *Definitions.* As used in this provision-—
Backhaul, covered article, covered telecommunications equipment or services, critical technology, FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.
Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.
Marginalized populations of Sudan means—
(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and
(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can

demonstrate—
(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;
(2) Are conducted under specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;
(3) Consist of providing goods or services to marginalized populations of Sudan;
(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;
(5) Consist of providing goods or services that are used only to promote health or education; or
(6) Have been voluntarily suspended.

Sensitive technology—
(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—
(i) To restrict the free flow of unbiased information in Iran; or
(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and
(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

(b) *Procedures*.
(1) *Covered telecommunications and video surveillance*. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at https://www.sam.gov for entities excluded from receiving federal awards for "covered telecommunications equipment or services."
(2) *FASCSA Orders*.
(i) The Offeror shall search in SAM for the phrase "FASCSA order" for any covered article, or any products or services produced or provided by a source, if there is an applicable FASCSA order described in paragraph (e) of FAR 52.240-91, Security Prohibitions and Exclusions.
(ii) The Offeror shall review the solicitation for any FASCSA orders that are not in SAM but are effective and apply to the solicitation and resultant contract (see FAR 40.204-1(c)(2)).
(iii) FASCSA orders issued after the date of solicitation do not apply unless added by an amendment to the solicitation.
(c) *Covered telecommunications equipment or services representations*. By submission of its offer, the Offeror represents that, after conducting a reasonable inquiry (that looks at any information in the Offeror's possession but does not need to include an internal or third-party audit)—
(1) It will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation, except as waived by the solicitation, or as disclosed in paragraph (g); and
(2) It does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, except as waived by the solicitation, or as disclosed in paragraph (g).
(d) *FASCSA Representation*. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror's possession but does not need to include an internal or third-party audit.
(e) *Sudan certification*. By submission of its offer, the offeror certifies, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), that the offeror does not conduct any restricted business operations in Sudan.
(f) *Iran Representation and Certifications*.
(1) Except as provided in paragraph (f)(2) of this provision or if a waiver has been granted in accordance with FAR 40.203-3, the offeror, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), by submission of its offer—
(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;
(ii) Certifies that the offeror, or any person (as defined at section 15 of the Iran Sanctions Act of 1996, Pub. L. 104-172, 50 U.S.C. 1701 note) owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Act. These sanctioned activities are in the areas of development of the petroleum resources of Iran, production of refined petroleum products in Iran, sale and provision of refined petroleum products to Iran, and contributing to Iran's ability to acquire or develop certain weapons or technologies; and
(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $15,000 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and

interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)
(2) Exception for trade agreements. The representation and certification requirements of paragraph (f)(1) of this provision do not apply if—
(i) This solicitation includes a trade agreements notice or certification (e.g., 52.225-6, Trade Agreements Certificate); and
(ii) The offeror has certified that all the offered products to be supplied are designated country end products or designated country construction material.
(iii) The offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.
(g) *Disclosure*.
(1) If the Offeror is not able to represent compliance with the prohibitions in paragraphs (c) or (d), then the Offeror shall disclose within 72 hours to the contracting office identified in paragraph (g)(2) the following information for each product or service not compliant:
(i) Contract number and order number, if applicable;
(ii) Identification of whether this disclosure relates to paragraph (c) on covered telecommunication equipment or services, or to paragraph (d) on FASCSA orders;
(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);
(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));
(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;
(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the offeror would like the Government to consider a waiver);
(vii) Whether alternative products or services are available that would be compliant with the prohibition;
(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:
(A) Brand;
(B) Model number, OEM number, manufacturer part number, or wholesaler number; and
(C) Item description, as applicable.
(ix) Any readily available information about mitigation actions undertaken or recommended.
(2) If a disclosure is required to be submitted to a contracting office, the offeror shall submit the disclosure as follows:
(i) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at https://dibnet.dod.mil.
(ii) For all other contracting offices, the Offeror shall submit the disclosure to the Contracting Officer.
(3) If the disclosure provided does not contain any of the information required by paragraph (1), and the Offeror later discovers new information that is required by paragraph (1), then the Offeror shall submit a subsequent disclosure within 72 hours of discovering the new information.
(h) *Executive agency review of disclosures*. The Contracting Officer will review disclosures provided in paragraph (g) to determine if any applicable waiver may be sought. The Contracting Officer may choose not to pursue a waiver and may instead make an award to an Offeror that does not require a waiver.
(End of provision)

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

ADDENDUM TO FAR RFO 52.212-1: INSTRUCTIONS TO OFFERORS

This section serves as an addendum to the provision at FAR RFO 52.212-1, Instructions to Offerors—Commercial Products and Commercial Services.

L.1 GENERAL PROPOSAL INSTRUCTIONS

1. This solicitation is issued as a Request for Quote(RFQ) under FAR RFO Subpart 12.2. In accordance with FAR RFO 12.201-1.
2. Offerors shall submit one (1) electronic proposal to the Contracting Officer identified in Section A no later than the date and time specified in this solicitation.
3. Proposals shall remain valid for a minimum of 60 calendar days after the proposal due date.

L.2 PROPOSAL ORGANIZATION AND FORMAT

Offerors shall prepare their proposals in two (2) separate volumes:

1. Volume I: Technical Proposal
2. Volume II: Price Proposal

L.3 VOLUME INSTRUCTIONS

Volume I: Technical Proposal

The Technical Proposal shall not contain any pricing information. It must clearly demonstrate the Offeror's ability to meet all requirements outlined in the Statement of Work (SOW). A written technical proposal must demonstrate that the offered commercial data subscription meets all minimum requirements in the SOW. Specifically, the proposal must demonstrate the capability to provide:

1. A single integrated database linking encounter-level inpatient/outpatient billing, chargemaster data, and microbiology lab results.
2. Data from at least 1,400 diverse U.S. hospitals (representing ~25% of annual admissions).
3. Linkable Social Determinants of Health (SDOH) data.
4. Longitudinal patient tracking via unique identifiers.
5. Monthly cumulative data extracts covering 2016 to present.
6. Required training and ongoing technical support.

Volume II: Price Proposal

The Price Proposal shall be submitted in a separate file and must include:

1. **CLIN Pricing:** A Firm-Fixed-Price (FFP) quote detailing a completed CLIN schedule (from Section B of the solicitation) in MS Excel format. Pricing must be provided for the base period, all option periods, and all optional CLINs.

2. **Price Narrative and Price Buildup Supporting Data (FAR RFO 15.403-1):** To assist the Contracting Officer in performing a price analysis and determining price reasonableness, the offeror shall submit a detailed price narrative and supporting commercial data. The offeror may submit this data in the format regularly maintained as part of its commercial operations. The submission must include:

   a. **Commercial Sales History:** Data on the prices at which the same or similar data packages/subscriptions have previously been sold to other commercial, academic, or non-governmental entities under comparable terms and conditions.

   b. **Supporting Price Buildup:** If commercial sales data is insufficient to determine price reasonableness, the offeror shall provide other supporting information. This shall include an uncertified breakdown of the proposed FFP price, such as a summary of the labor categories and hours that form the basis of support services, and a description of the methodology used to develop data licensing and platform access fees.

   c. **Insufficient Data:** A proposal may be found unacceptable if the offeror fails to provide sufficient data to allow the Contracting Officer to determine price reasonableness.

3. **Security Certifications:** Offerors shall include a statement in Volume I certifying compliance with FAR RFO 52.240-90, Security Prohibitions and Exclusions Representations and Certifications. If applicable, offerors shall provide any disclosures required by paragraph (g) of the provision.

4. **Corporate Identifiers:** The company's Unique Entity Identifier (UEI), CAGE Code, and authorized Point of Contact (POC) name, title, phone number, and email.

CDCL.02 Alternate Protest Procedures (Jan 2026)
(a) In accordance with FAR 33.104-4(a)(5), interested parties may request an independent review of their agency protest at a level above the contracting officer. This independent review is available as an alternative to consideration by the contracting officer of a protest or is available as an appeal of a contracting officer decision on a protest. A protest must clearly identify any request regarding the above.

(b) Protests or appeals described in (a) shall be submitted to the Associate Director for Acquisition Services, Office of Acquisition Services, Office of Financial Resources, Centers for Disease Control and Prevention by email at ftg4@cdc.gov.
(c) Protests will not be considered if the interested party has a protest on the same or similar issue(s) pending with the Contracting Officer.

CDCL.03 – Disclosure of Artificial Intelligence Use in Contract Performance (May 2026)
Offerors must affirmatively identify in their proposal whether or not Artificial Intelligence (AI), including Generative AI, is planned, expected, or may be used in the performance of this contract. If planned or potential AI use is identified, offerors must submit an AI Compliance and Risk Management Plan in accordance with **CDCH.10** using the template provided.

CDCL.09 Contractor Performance Assessment Reporting System (CPARS) Requirements (Jan 2026)

In accordance with FAR 42.11, Centers for Disease Control and Prevention (CDC) will review and evaluate contract performance. FAR 42.1101 and 42.1102 requires agencies to prepare evaluations of contractor performance and submit them to the Contractor Performance Assessment Reporting System (CPARS). CDC utilizes this web-based system to prepare and report contractor performance evaluations. All information contained in these assessments may be used by the Government, within the limitations of FAR 42.11, for future source selections in accordance with FAR 15.104 where past performance is an evaluation factor.

The CPARS system requires a contractor representative to be assigned so that the contractor has appropriate input into the performance evaluation process. The CPARS contractor representative will be given access to CPARS and will be given the

opportunity to concur or not-concur with performance evaluations before the evaluations are complete. The CPARS contractor representative will also have the opportunity to add comments to performance evaluations.

The assessment is not subject to the Disputes clause of the contract, nor is it subject to appeal beyond the review and comment procedures described in the guides on the CPARS website. Refer to: www.cpars.gov for details and additional information related to CPARS, CPARS user access, how contract performance assessments are conducted, and how contractors participate. Access and training for all persons responsible for the preparation and review of performance assessments is also available at the CPARS website.

The contractor must provide the CDC contracting office with the name, e-mail address, and phone number of their designated CPARS representative who will be responsible for logging into CPARS and reviewing and commenting on performance evaluations. The contractor must maintain a current representative to serve as the contractor representative in CPARS. It is the contractor's responsibility to notify the CDC contracting office, in writing (letter or email), when their CPARS representative information needs to be changed or updated. Failure to maintain current CPARS contractor representative information will result in the loss of an opportunity to review and comment on performance evaluations.

Provide the current CPARS representative information below.

_____

PRINT OR TYPE NAME

_____

EMAIL ADDRESS AND PHONE NUMBER

SECTION M – EVALUATION FACTORS FOR AWARD

ADDENDUM TO RFO 52.212-2: EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

This section serves as an addendum to the provision at RFO 52.212-2, Evaluation—Commercial Products and Commercial Services.

M.1 BASIS FOR AWARD

The Government intends to award a single Firm-Fixed-Price contract to the responsible offeror whose proposal is determined to be technically acceptable and whose price is determined to be fair and reasonable. No trade-off process will be utilized. To be eligible for award, a proposal must receive a rating of "Acceptable" for Factor 1 (Technical Proposal) and be determined fair and reasonable for Factor 2 (Price).

The Government reserves the right to award without conducting discussions.

Compliance with FAR RFO 52.240-90, Security Prohibitions and Exclusions Representations and Certifications, will be evaluated on a Pass/Fail basis. A proposal that receives a "Fail" rating for this factor will be ineligible for award.

M.2 EVALUATION FACTORS

The Government will evaluate the proposal based on the following two (2) evaluation factors:

a. Factor 1: Technical Proposal (Rated on an Acceptable / Unacceptable basis)

b. Factor 2: Price (Evaluated for Fairness and Reasonableness)

M.2.1 Factor 1: Technical Acceptability

The Government will evaluate the Technical Proposal on an Acceptable / Unacceptable basis. The proposal must demonstrate a clear understanding of the requirements in the Statement of Work (SOW). A proposal that fails to meet one or more of the minimum standards below will be rated "Unacceptable" and will be ineligible for award.

1. A single integrated database linking encounter-level inpatient/outpatient billing, chargemaster data, and microbiology lab results.
2. Data from at least 1,400 geographically diverse U.S. hospitals (representing ~25% of annual admissions).
3. Linkable Social Determinants of Health (SDOH) data.
4. Longitudinal patient tracking via unique identifiers.
5. Monthly cumulative data extracts covering 2016 to present.
6. Required training and ongoing technical support.

M.2.2 Factor 2: Price Evaluation

The Government will evaluate the total proposed price (Base Period + All Option Periods and Optional CLINs) for fairness and reasonableness in accordance with FAR 15.404-1. The analysis will be based on the supporting data submitted in the offeror's Price Proposal as required by Section L of this solicitation. The Government reserves the right to request additional supporting data if necessary to determine that the price is fair and reasonable. An award will not be made to an offeror whose price is determined to be unreasonable.

The Government will evaluate the Offeror's certification of compliance with FAR 52.240-90, Security Prohibitions and Exclusions Representations and Certifications, on a Pass/Fail basis. Failure to provide the required certification or any applicable disclosure required by the provision may render the proposal ineligible for award. Failure to provide or representing a prohibited source will render the proposal Unacceptable.

CDCM.04 Evaluation of Artificial Intelligence Compliance and Risk Management Plan (May 2026)
The Artificial Intelligence (AI) Compliance and Risk Management Plan submitted as a part of the offeror’s proposal will be evaluated for quality and completeness. The AI Compliance and Risk Management Plan will be rated on a “Pass/Fail” basis considering the clearness, appropriateness, and inclusiveness of the elements described under CDCH.10.
All proposals that contain planned or potential AI use and do not contain an acceptable AI Compliance and Risk Management Plan will be considered non-responsive and ineligible for award.

The AI Compliance and Risk Management Plan may require later revision during contract performance as described in CDCH.10.