Statement of Work
Policy Training

Note that this sample has been revised from the source document on the Government Point of Entry as necessary to align formatting and applicable FAR procedures.

SECTION 1 – BACKGROUND

The mission of CDC's Office of the Associate Director for Policy & Strategy (OADPS) is to identify and advance opportunities to use policy and leverage health system transformation and other sectors to improve the public's health. To achieve its mission, OADPS needs to support CDC-wide work to translate and effectively communicate research and analysis of proposed/recommended public health programs, policies and interventions to enable its audiences to understand their value in improving health, reducing health inequalities, and averting healthcare and productivity costs. OADPS addresses the CDC strategic directive to "use scientific and program expertise to advance policy change that promotes health". One way of accomplishing this task is per a training we call the "The Policy Academy".

SECTION 2 – PURPOSE

The Policy Academy is intended to enhance the skills of participants in five primary competencies: policy analysis, policy evaluation, strategic planning & systems thinking, stakeholder engagement, and communicating policy recommendations (translating science to policy). The Academy's curriculum provides learning opportunities through a small variety of means, including classroom instruction, a mentored team research project (the teams identify their own mentors, hereafter referred to as "team coaches"), web-based training, and outside reading. The classroom portion will be limited to seven days/approximately 40 classroom contact hours distributed across three separate sessions of two or three days each. Those sessions are tentatively slated for late April/early May, late June, and mid-October.

SECTION 3 – SCOPE OF WORK

The CDC Policy Academy is a unique capacity-building program initiated in 2015. Its original goal was to improve CDC workforce capacity to evaluate the potential impact of policy on the public's health at all levels of government, including state, tribal, local and territorial. The focus on policy analysis strengthens participants' skills to identify and analyze policy issues related to public health priorities.

SECTION 4 – TASKS TO BE PERFORMED

- Identify overarching objectives for the Academy professional development program and create a robust and challenging learning structure for participants in order to enhance their ability to apply policy in public health
- Some specific activities may include:
    - Develop and deliver a course curriculum. Curriculum planning and structuring the nomination and selection process in collaboration with the CDC program coordinator should occur early in the PoP and in accordance with the "Deliverables/Reporting Schedule" (Section 8 of this SOW).
- Conduct key informant interviews with CDC senior staff to identify critical policy skills for the public health workforce
- Identify core competencies on which the Academy professional development program will be based
- Establish learning objectives to support the competencies
- Develop a program of instruction consisting of multiple learning sessions of two or three days each that addresses the competencies, complemented by outside reading, online courses, and/or experiential activities
- Acquire the guest speakers for these trainings (per the guidance of CDC)

- Assist with the identification of and invitation to public health and government experts with relevant experience to offer their insight via individual and panel presentation, including drafting speaker invites for CDC review, sending invitations, and tracking responses.
- Provide online workspace for posting and sharing Policy Academy Materials and various information.
- Schedule and facilitate periodic calls with the planning team (consisting of vendor and designated CDC personnel) and provide notes from these meetings.
- Arrange and pay for Travel, Accommodations, and Per Diem (if necessary) for the guest speakers.
    - **Planning Note:** 2 guest speakers per training on average.
- Identify and Secure Training Locations and Material Support.
    - The Contractor shall secure training sites using CDC space and support. In the event that CDC training space is unavailable, with prior approval from CDC, the Contractor shall negotiate and implement the necessary agreements and contracts with an outside training location.
    - The Contractor, with CDC approval, shall be responsible for all training logistics including procuring and preparing training materials (textbook, binders, hard copies of presentations, etc.) and securing staff for training support as needed, name badges, participant packets, signs and registration systems if needed.
        - **Planning Note:** Up to 25 students will be present for these trainings. Each student will receive a textbook and training binder.
- Provide facilitation for each of the classroom sessions

Duties of the co-coordinator/facilitator would include, but are not necessarily limited to, the following:

- **Assist the CDC program coordinator with development of the classroom curriculum structure** overall and session agendas specifically. The coordinators would jointly identify potential topics and instructors and where they should appear in the classroom agendas. The CDC coordinator would invite and secure instructor participation unless the co-coordinator is acquainted with a potential instructor and would be better-suited to make the invitation. Additionally, the co-coordinator would:
    - **Help prepare and participate in a "virtual open house" webinar as directed by CDC. The webinar is** normally conducted in late January or early February. The Policy Academy team, including the facilitator, provides an overview of the structure and curriculum, and describes the application process to interested CDC staff.
    - **Participate in a kickoff webinar for participants** in mid-April. The CDC program coordinator will provide the bulk of the presentation to give participants an idea of what to expect and what the Academy entails for completion requirements. The co-coordinator is expected to describe his/her role and provide guidance to team coaches.
    - **Attend and participate in the three classroom sessions full-time.** The three classroom sessions will be two or three days each. The co-coordinator can anticipate an 8AM-5PM schedule each day (from set-up to end-of-day debrief), a total of approximately 63 hours, including an hour for lunch. The co-coordinator may need to meet with teams during that time to discuss their project progress (see related "head coach" item below).
    - **Assist in the drafting of general learning objectives for each session**. Invited instructors normally offer learning objectives for their specific modules of instruction (which would be included in the agendas. See the attached agendas for examples).
    - **Assist with the identification of and invitation to public health and government experts** with relevant experience to offer their insight via panel presentations. At

least one panel presentation per classroom session is envisioned for the 2020 Academy.
    - **Act as lead facilitator as required during the three classroom sessions** whether during instructor or panel presentations, small group (team) exercises, or during feedback/evaluation discussions held at the end of each day and session. On occasion the facilitator responsibility is limited to being a "master of ceremonies" as some instructors require no assistance of that sort.
    - **Present on at least one current public health topic** (usually a minimum of one hour) mutually agreed-upon with the program coordinator and which would be of interest and relevant to the participants. The application of policy to the designated topic must be clearly evident in the instruction.
    - **Participate in multiple meetings** (in-person or via phone) to plan each classroom session. Some of the planning will occur via email.

- **Act as a "head coach" for the teams** (four-five teams, four participants each). This responsibility involves checking in periodically with each team to assess progress on their projects, identifying what assistance they might need above/beyond what their team mentor/team coach may do for them, and providing insight on how they might proceed (if asked) based on the co-coordinator's public health experience and expertise. This assistance includes meeting with teams during the classroom sessions and receiving team updates via email or phone in between classroom sessions.
- **Attend the 2020 Academy graduation ceremony which normally occurs in December.** The co-coordinator may be asked to jointly plan the ceremony with the coordinator. The ceremony has followed a standard structure that includes an OADPS master of ceremonies, team project presentations, a guest speaker keynote, and presentation of certificates.
- **Offer suggestions for improvement for the current Academy or future Academies.** OADPS continually seeks to improve the quality of the "Academy experience" and would welcome suggestions from the co-coordinator. OADPS employs a program evaluator who will likely interview Academy staff as part of this continuous quality improvement process.

NOTE:
It is imperative that the co-coordinator is available to assist with planning and execution of the three classroom sessions. The time estimated for planning and executing each classroom session is broken down as follows:

- Minimum of three planning meetings per session, one hour each. Total: 9 hours
- Facilitator/presentation preparation time: 10 hours
- Classroom session execution, 7 days @ 9 hours/day: 63 hours

Additional time estimates:

- Head coach engagement with teams, four teams at 2 hours/tm total: 8 hours
- Miscellaneous email and phone communications October 2019 –December 2020: 30 hours

Total estimated time requirement: Approximately 120 hours. Planning meetings will be scheduled as jointly agreed upon by the coordinators. The classroom session schedules will be determined depending on selected instructor availability. Tentatively, the schedule for the classroom sessions is:
- Session 1: Early May, two days
- Session 2: Late June, three days
- Session 3: Mid October, two days

- Outputs:

- Rigorous classroom curriculum consisting of multiple instructional sessions based on identified core competencies
- Team project deliverables (e.g., manuscript; white paper; policy brief) articulating successful strategies at state and local levels to address public health priorities through policy
- Evaluation report that summarizes participant responses in order to capture lessons learned and provide recommendations for improving the Academy curriculum and experience

SECTION 5 – GOVERNMENT FURNISHED MATERIALS

No Government Furnished Materials will be needed for the vendor per this contract

SECTION 6 – PERIOD OF PERFORMANCE

9/28/2019-9/27/2020

SECTION 7 – PLACE OF PERFORMANCE

It is estimated that approximately 0% of the contract will be performed on-site at CDC facilities and 100% will be performed off-site at the contractor's facilities.

SECTION 8 – DELIVERABLES/REPORTING SCHEDULE

Task Number	**Deliverable Description**	**Date of Delivery [Time after the Award of the Task Order]**
	Kick-off Meeting	Within 2 weeks of task order award
	Progress Reports	Monthly, By day 10 of the following month
	Work Plan, Timeline, and Cost Estimate	Within 2 weeks of kick-off meeting (modified throughout period)
	Bi-weekly Project Team Calls	Bi-Weekly, to begin within 3 weeks of task order award
	Identify and Secure Training Location(s) and Identify Material and Staff Supports for capacity building meetings	Within 4 months of task order award
	Provide Support for Training Content and Planning	Fully completed within 12 months of task order award; individual deliverable due dates in work plan.
	Identify and Provide Qualified Instructors	Within 1 month of task order award
	Identify CDC Needs and Develop Capacity Building Plan	Within 3 months of task order award

SECTION 9 – TRAVEL

The contractor shall arrange and pay for speaker/instructor travel, lodging, and per diem (as appropriate). The speakers/instructors will be offered a stipend for their services.

SECTION 10 – SPECIAL REQUIREMENTS

N/A

SECTION 10 – REFERENCE MATERIALS

- The following link provides resources on translating science into evidence-based policies and provides an example of a package of products and services

http://www.mcmasterhealthforum.org/home

- The following link provides information on CDC's Winnable Battles

http://www.cdc.gov/WinnableBattles

- CDC Office of the Associate Director for Policy information/OADPS Policy Research, Analysis and Development Office for information on policy and economic analysis functions

http://www.cdc.gov/policy/od/index.html
http://www.cdc.gov/policy/prado/

- The following link provides access to one sample set of products from within CDC

http://www.cdc.gov/stltpublichealth/products/index.html

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**, 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 *insert email here*.

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:	[X] Low [ ] Moderate [ ] High
Integrity:	[X] Low [ ] Moderate [ ] High
Availability:	[X] Low [ ] Moderate [ ] High
Overall Risk Level:	[X] Low [ ] Moderate [ ] High

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: [ ] 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 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "h*andling"* 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 *[CDC-provided delivery date]*.

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)* 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 PU 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 PU and portable electronic storage media that store PU, the inadvertent disclosure of PU 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 PU 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 suspected or confirmed breach in any medium as soon as possible and without unreasonable delay, 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 *insert email here* or telephone at 555-5555, 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

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR).

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.*

.

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.

Schedule of Deliverables

Deliverable Title/Description	Due Date
Roster	Before effective date of this contract
Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS
Assist in the completion of a PTA/PIA form	In conjunction with contract award
Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery
Incident and Breach Response Plan	Upon request from government
List of Personnel with defined roles and responsibilities	Prior to performing any work on behalf of HHS
Off-boarding documentation, equipment and badge	Prior to performing any work on behalf of

when leaving contract	HHS
Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS
Form or deliverables required by CDC.	At contract expiration.
If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan	At contract expiration.