**DRAFT**

**PERFORMANCE WORK STATEMENT (PWS)**

# Wellness Health Promotion Portal (WHPP) III

1. **DESCRIPTION OF SERVICES**
   1. **Background.** This is a contract to acquire a web-based, Contractor-Owned/Contractor Operated (COCO) health promotion web portal that includes comprehensive self-management tools, targeted interventions, and interactive contacts to foster program engagement. It shall include an online health risk appraisal (HRA), personalized healthy lifestyle information, and other tailored tracking and assessment tools to deliver a complete, interactive health and wellness and health promotion system.
   2. **Scope.** The Contractor shall provide a web-based, COCO health promotion web portal. This online wellness tool will support mission objectives to improve the health and safety of the government workforce. This tool will provide a central access point for wellness programming as well as access to information and support for the Civilian Health Promotion Services (CHPS) and related resilience/wellness services/support. By extending these programs into the virtual domain, the online wellness tool will permit web administrators, CHPS health promotion professionals, and prevention staff to manage the provision, customization, and reporting of

high-quality health, wellness, and benefits information. It will also support participants with virtual tools that help them create a more personalized approach to lifestyle improvement. The tool will provide access to a broad range of native content as well as content from CHPS, the Employee Assistance Program (EAP), and other approved sources to the Government (HQ AFMC/A1).

* + 1. The Contractor shall have professional and technical expertise in health promotion online data systems, website management and HRA development and implementation. Work shall be in accordance with Air Force policies and procedures and be of high quality and consistency and available worldwide through the internet.
    2. The interactive web portal shall be fully operational at time of award, provide an online administrative function for assigned staff/administrator use to manage their health promotion program and an HRA which shall include an array of healthy lifestyle information with personalized wellness features. The HRA shall be a valid and reliable tool.
    3. The interactive web portal shall include services to engage the population, HRA provisions, and the ability to identify and tailor programs to meet Government needs. This solution shall also include self-management tools to help individuals stay healthy and reduce risk; health coaching tools; individual and team challenges; incentive management; screenings and attendance tracking; and provide performance reporting, when applicable.
    4. The web-based system that is provided shall be reliably available as a secure web- based application that is accessible through the internet via a personal computer, or a mobile smartphone/tablet device and delivered from a service environment having an Authorization to Operate (ATO) or Authority to Connect (ATC) from an Air Force Authorizing Official (AO). The network for the server must remain FedRAMP+ approved for the duration of the contract.

1. **GENERAL INFORMATION**
   1. **Security Requirements.** The contractor shall have a favorable background investigation/security check (Tier 2, Level 5 Public Trust with subject interview).
      1. Physical Security: The contractor shall be responsible for safeguarding all government information and property provided for contractor use.
      2. Government records, copies of original results and reports, verified original data, corrected data, and corrected supporting final reports are maintained by the contractor, but remain the property of the US Government.
      3. Neither the contractor nor any of its personnel shall disclose or cause to disseminate any information concerning operations of military activities. Such actions could result in violation of the contract terms and possible legal actions.
   2. **Post Award Conference/Periodic Progress Meetings.** The Contractor shall attend any post award conference convened by the contracting activity or contract administration office in accordance with FAR Subpart 42.5. The Government Program Manager (PM) and Contracting Officer (CO) may meet periodically with the contractor to review the contractor's performance. At these meetings the CO will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. The contractor shall take and publish the minutes of these meetings and submit them to the PM and CO for approval within 2 working days of the meeting. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.
2. **TASK REQUIREMENTS**

# Task A – Health Promotion Web Portal Platform

* + 1. The web portal platform shall consist of multiple, branded ‘micro-sites’ on a single platform – up to 75 separate ‘micro-sites’ by location - with Government web administrator capabilities to brand, customize ‘live’ features, update with regular programming.
    2. The web portal platform shall have separate accountability for units/organizations, status.
    3. The web portal platform shall have capacity to hold accounts for all eligible users and administrators. An administrative web tool shall be available to allow the

Government web administrator to easily identify and disable individual accounts that have had no activity for 365 days or more.

* + 1. At onset of contract, the Contractor shall complete an import of all current and historical web portal platform data and tables into the new platform. This data will be supplied in 32bit and 64bit formats that can be imported into Microsoft SQL Server and Oracle. Data includes health promotion records for approximately 100,000 or more active web portal users plus additional historical data from inactive accounts from the last 14 years.
    2. Web portal users shall have the ability to set their own login information (i.e. user ID and password) upon account creation to control future access to their information. The system is expected to enforce government password policies that encourage best security practices. These policies will require use of hardened passwords and force web portal users to periodically change their password. Web portal users shall also be able to perform a self-recover of their login information (i.e. ‘forgot’ function), using key information provided during initial account creation (e.g. answers to 3 or more unique questions about personal details).
    3. The platform shall use enhanced login security so that after several failed login attempts, the web portal user account is temporarily disabled. Disabled accounts can only be re-enabled by a government web administrator.
    4. Any contact attempt made through the website by web portal users, to include replying to automated/customized emails and notifications sent through the platform, shall be forwarded to an email address as designated by the Government.
    5. The Contractor shall incorporate Government provided Uniform Resource Locator (URL), program logos, and customized headers to establish the Government desired branding of the platform.
    6. The Contractor shall allow the Government Program Manager an opportunity to review and approve the new platform branding prior to launch.
    7. The Contractor shall create a tool so that the Government/COR can assign specified government web administrator(s) for access to provide additional customization, control content, etc. of the site.
    8. The platform shall allow government web administrator access at a staff/admin account level via two-factor login (e.g. user ID and password with key fob security token).
    9. The Contractor shall have available a means for the government web administrator to check work via a ‘web portal user-side window’ for each ‘micro-site’ when making adjustments to the site, assisting with troubleshooting, etc.
    10. The platform shall have options for ‘consent, privacy and about text that is viewable upon creation, whereas the web portal user will be asked to accept as part of the conditions for using the site. This content shall be highly customizable by the Government and government web administrator.
    11. The platform shall be in compliance with Section 508 of the Rehabilitation Act (29 U.S.C. 749d).

# Task B – Highly Configurable and Customizable Web Portal Platform

* + 1. The Contractor shall provide government web administrator(s) administrative access rights to the web portal platform. Web administrators are determined by the program office.
    2. The Contractor shall provide Government web administrator access to manage categorization of ‘micro-sites’ to add/delete locations and set landing/homepage content, time zone, etc.; add/delete units/organizations per each location ‘micro-site’ as parameters change annually; update ‘micro-sites’ based on status of Civilian vs. Active Duty vs. Spouse; add/delete pay grade categories; ability to create, delete, and manage groups to use for reports/queries (e.g. setting multiple location ‘micro-sites’ into a universal MAJCOM group for aggregate population data, etc.). Additionally, government web administrator(s) shall be able to manage settings for each ‘micro-site’ with landing/homepage theme and content (color scheme, images, program logos, pertinent program information, etc.); event calendars; content available to web portal user; display options; ability to turn features on/off.
    3. The Contractor shall provide Government web administrator access to customize the website to alter workflow through the site, i.e. require some accounts to complete a Health Risk Appraisal questionnaire before able to utilize the tool. The software shall have the ability to allow the employee to be threaded through the system based on what the government web administrator(s) have set up per Government preference.
    4. The web portal shall permit staff to create a custom workflow, or ‘Campaign’, that guides participants in the completion of a set of tasks related to health and productivity. The inputs shall consist of one or more tasks from a set that includes: completing an HRA, completing a lifestyle questionnaire, completing an achievement (incentive) program, making entries in a Reflection Journal, creating a personalized Wellness Plan, connecting a personal fitness/health device, engaging in a mindfulness practice, registering for a challenge, completing a challenge, completing a chronic disease management course, or signing up for an appointment (e.g. for training or instruction).
    5. The Contractor shall provide Government web administrator access to customize content areas of web portal user display to include main area of landing/homepage that allows for ability to upload location specific content specific to that location (i.e. office location, contact info, hours of operation, etc.), announce awareness campaigns and wellness challenges and other important info (able to set dates for info to be visible,

pinned on page and priority order of multiple informational blocks, ability to insert images and links into blocks, etc.; ability to upload documents that are location and/or status specific.

* + 1. The Contractor shall provide Government web administrator access to search for specific web portal user accounts and view details, temporarily disable and delete accounts, merge duplicate accounts, troubleshoot account issues (e.g. reset password, update mail, etc.); also able to view analytics for account access (e.g. number of logins, last login, what features are being accessed, etc.).
    2. The Contractor shall provide Government web administrator access to enter web portal user blood panel screenings into website log (e.g. blood pressure, weight, various cholesterol values, triglycerides, and blood sugar).
    3. The Contractor shall provide Government web administrator access to upload/delete documents (PDF, DOC, DOCX, TXT, XSL, XLSX, PPT, PPS, MOV, SWF, MP4, CSV) and images (GIF, JPG, JPEG, PNG) to internal site wide library and use internal site links to incorporate these items into notifications, emails, build web portal user document area on landing/homepage, etc.
    4. The Contractor shall provide Government web administrator access to manage staff/admin accounts, including type of access (i.e. ability to turn various access areas on/off per account).
    5. The Contractor shall provide Government web administrator access to import/export data for members, steps, attendance, blood panels, biometrics, preventive care, and achievement tasks/earned.
    6. The Contractor shall provide Government web administrator access to upload data from other sources such as blood panel data from CSV file, multiple biometric data from CSV file, pedometer steps from app/device, preventive care upload.

# Task C – Web Portal Platform User Interface/Attractiveness of Landing/Homepage

* + 1. The platform shall be a mobile-first platform, meaning accessible from any device with a web browser – computer, tablet, and phone.
    2. If the Contractor utilizes an ‘app’ for mobile accessibility, they shall ensure the application is available from the iOS and Android stores through normal public distribution mechanisms (i.e. iTunes, Google Play, Amazon Marketplace, etc.), and shall not require an additional fee for the employee to download or use. Access through the web or a mobile client will require authentication using the login credentials assigned to the web portal user’s account during initial creation. This mode of engagement would be in addition to the web portal user’s ability to access the web portal from a work or personal home computer via a web browser.
       1. Mobile applications that are used to manage personal information and/or health information shall be implemented in a secure manner. The contractor will be required to adhere to guidance in the established Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act requirements.
    3. The Contractor’s product shall be customizable for the Government to include site name, URL address, color theme and other branding, content, landing/homepage elements.
    4. The web portal platform shall contain an ‘easy-to-use’ menu for accessing main dashboard, news and announcements, location specific event calendar, tracking logs, challenges and other programs, health promotion library with searchable up-to-date content, documents (e.g. health risk appraisal report, other items loaded to the site by government web administrator, etc.).
    5. The government web administrator shall be able to post news and announcements that contain informational content, links to educational resources, and URL links for additional reference.
    6. The Contractor shall provide the government web administrator access to customize what is permanently ‘pinned’ to landing/homepage, plus set parameters for additional customization for the look of the landing/homepage that is available to web portal user customization. This includes capability to turn features on/off to control what is visible/available to web portal users.
    7. The web portal shall have mechanisms whereby the web administrators can create graphical and/or textual links to programs, announcements, or offerings from their organization or other, allied sources that bear upon the health and safety of the government workforce. The web portal shall serve as a central hub for distributing health- related information and programming.

# Task D – Health Risk Appraisal (HRA)

* + 1. The platform shall use a research-based/validated HRA written at a 5th grade literacy level and in plain language. The HRA shall be linguistically, age, gender and culturally appropriate for all employees.
    2. The Contractor shall provide the government web administrator capability to customize questions to build a short or long version HRA from the following topic areas: overall health, family history, cardiovascular heart disease warning signs, blood pressure, current weight/height/abdominal circumference, recent medical services and usage, presenteeism/absenteeism, physical activity/exercise, nutrition, tobacco/alcohol/medication use, driving habits, psychological health, sleep, social/spiritual health, self-care behaviors, life/job satisfaction, self-rating of health, stress, cholesterol risk, blood panel, readiness for change, health-related productivity loss.
    3. The HRA shall be compliant with the Genetic Information Non-Discrimination Act (GINA) when collecting family history information.
    4. The HRA shall be reviewed no less than every 2 years to ensure compliance with best practices.
    5. The HRA shall be capable of being tailored to determine readiness for behavior change.
    6. The government web administrator shall have the ability to turn HRA on/off for different types of accounts (e.g. Civilian vs. Active Duty vs. Spouse).
    7. The HRA shall be able to integrate government web administrator blood chemistry readings to adjust risk level/results.
    8. The HRA shall have a completion status bar visible for web portal user while taking the questionnaire.
    9. Web portal users shall receive immediate feedback from their HRA in a comprehensive and personalized wellness report that also shows year-to-year risk to track progress over time. This report will have the capability to be saved/printed for reference.
    10. The Contractor shall include up-to-date resources for each risk factor in the Health Information Library and link web portal users to these resources as applicable from HRA results. This information can include web links, educational materials, referrals, and program marketing.
    11. The Contractor shall include a separate ‘Doctor’s Report’ that will be accessible to web portal users after completing the HRA. The ‘Doctor’s Report’ shall display the users most recent biometric data values and detailed risk areas in a report designed to be printed and shared with the web portal users primary care physician.
    12. The Contractor shall provide the government web administrator the ability to upload HRA completion certificate to be available for web portal user to print.
    13. The Contractor shall provide the government web administrator access to be able to run analytics on population health data from HRA responses (e.g. create specific web portal user groups by location to view aggregate results for programming purposes).
    14. The Contractor shall provide the government web administrator access to view current and historical HRA and biometric data to track individual health outcomes and risk status over time in the event the data is used for one-on-one health coaching service.

# Task E – Web Portal Platform Communication Capabilities

* + 1. The Contractor shall provide the government web administrator the capability to send outbound customized group messages specified by location, pay grade, HRA results, web portal user groups, etc. Messaging capabilities shall consist of bulk emails, bulk direct messages, push notifications, target group messages, surveys, announcements, HTML based newsletters, motivational messages, and reminders generated automatically by the system and/or initiated by the government web administrators. All email messages should be sent in a manner that identifies the system domain and since sent unsecured will need to utilize protocols to prevent the inclusion of sensitive personal of health information.
    2. The Contractor shall provide the government web administrator the ability to turn on/off automated messaging for wellness challenges/achievement programs, send push notifications.
    3. The Contractor shall provide the government web administrator the ability to push one-on-one messaging to web portal user accounts for health coaching service, HRA requests for help, etc.
    4. Web portal users shall have an ‘opt out’ box available to have personal preference options for receiving - or not – web portal communications.

# Task F – Web Portal Platform Content Management Tool

* + 1. The platform shall have an event calendar that is highly customizable by the government web administrator. Calendars shall be configurable per 'micro-site’ and will include the ability to turn features on/off, to create a library of events, create calendars by location. The calendar shall permit participants to request appointments and to reserve a slot in a class or event. Administrators will also have the ability to search reservations and print rosters, etc. to find the participants that have enrolled or to review attendance. The calendar will have an easy-to-use interface for web portal users with the ability to view calendar by day/week/month, view event details easily, reserve/mark events as favorites as a reminder to attend, etc.
    2. The platform shall have a Health Information Library that the contract shall keep filled with current, relevant, evidence-based health education information that directly complements, explains, and/or enhances the risk factors identified through the HRA, health promotion activities, national health observances, lifestyle improvement tools, and wellness challenges available for employee participation. The government web administrator shall also have the ability to add content based on Government needs.
    3. The platform shall offer wellness challenges that simultaneously target one or more risk factors.
    4. The Contractor shall provide the government web administrator the ability to create individual and team challenges with performance (steps, minutes, distance, points, etc.)

and improvement (weight, body fat, etc.) goals, and customize challenge parameters to include program goals, title, display, dates, set locations/web portal users.

* + 1. The Contractor shall provide the government web administrator access to be able to customize challenges by location, pay grade, etc.
    2. The platform shall be capable of both custom-built challenges per specifications of the Government as well as built-in/canned challenges.
    3. The platform shall have capabilities for communicating with challenge web portal users (weekly informational emails with current status, etc.) that the government web administrator can customize.
    4. The Contractor shall provide the government web administrator access to run detailed report analytics for entire platform and ‘micro-sites’ to view enrollment, challenge completion, etc.
    5. Wellness challenges in the platform shall have both the capability for web portal users to self-enroll, as well as government web administrator ability to enroll web portal users.
    6. The platform shall offer health and wellness tracking tools for web portal users to input health and wellness information and monitor goal achievement over time in areas such as biometrics (blood pressure, blood panel – cholesterol/triglycerides/blood sugar, weight management), physical activity minutes, pedometer steps, body composition (InBody and BOD POD measurements), strength workouts, nutrition/food/water, sleep, stress, stress management/mindfulness practices.
    7. The platform shall allow web portal users to input data into the platform’s health and wellness trackers manually, as well as be compatible with the use of personal health and wellness tracking devices for automated data capture and synchronization with devices such as Fitbit, Garmin, iHealth, MapMyFitness, MyFitnessPal, PredictBGL, Runkeeper, Strava, Under Armour Record, and others.
    8. The platform shall offer customizable achievement programs that are highly interactive for web portal user engagement and intrinsically motivational.
    9. The Contractor shall provide the government web administrator access to be able to customize achievements by choosing specific tasks from canned lists and creating own tasks to incorporate into program for web portal users to complete various items, levels, etc., both for short-term and long-term requirements/programs.
    10. Achievement programs shall be based on points a web portal user could earn in areas such as completing annual check-up, logging set amount of exercise minutes or pedometer steps, logging activity or nutrition for set number of consecutive days, safety areas like wearing a seatbelt, healthy lifestyle behaviors like not smoking, etc.
    11. The Contractor shall provide the government web administrator the capability to load a completion certificate that will populate upon completion intervals for the web portal user to utilize. Additionally, the capability shall exist for the government web administrator to upload own marketing for images, flyers, rules.
    12. The Contractor shall provide the government web administrator access to run detailed report analytics for entire platform and ‘microsites’ to view enrollment, completion levels, etc.
    13. The platform shall offer a feature for daily pursuits where web portal users will have the option to work on short-term health and wellness goals in areas such as physical activity, nutrition, mindfulness/stress management, and resiliency.
    14. The platform shall offer a feature for interactive learning programs for web portal users to educate themselves about a condition or wellness goal and take steps towards building a long lasting, healthy habit in areas such as tobacco free, managing diabetes, heart health, and weight management.
    15. The platform shall offer a feature for fitness assessments where web portal users can read a ‘how to’ and record results and track progress over time for body fat (abdominal girth, bioelectrical impedance body fat, body mass index, skinfold caliper pinch fat %, waist-hip ratio, weight), cardiovascular (1 mile run/walk, 3 minute step test, submax/max treadmill, direct VO2, peak expiratory flow, resting heart rate), flexibility (sit-n-reach, shoulder rotation, hamstring/hip flexion, reach-over shoulder, trunk extension), strength (1 minute timed sit-ups, endurance bench press, grip strength test, handgrip strength, submax/max bench/leg press, curl-ups, pull-ups, push-ups, vertical jump, arm/leg muscle strength).
    16. The platform shall offer a feature for workout prescriptions where web portal users can work through a planning log template to create workout prescriptions from a library of current exercise descriptions/pictures.
        1. The platform shall offer options health and wellness materials such as streaming fitness options, customized workout goals, fitness and nutrition information and resources.
    17. The platform shall have a healthy lifestyle coaching tool that is highly customizable by the government web administrator, including ability to turn feature on/off. The tool shall provide evaluation of the web portal user’s Exercise Risk based on the American College of Sports Medicine (ACSM) guidelines and shall provide pictures and descriptions of exercises that can be incorporated into a personalized wellness plan.
    18. The Contractor shall provide the government web administrator access to be able to document coaching sessions in the system, secure 2-way messaging system for government web administrator to communicate with web portal users, access to tools in

Health Information Library to send web portal users, access to other items such as a goals tracker, etc. for use during sessions.

3.6.23: The Contractor shall provide an option for custom development work to be completed by Contractor staff when areas of the web portal require increased utility and customization to best meet Government needs.

# Task G – Web Portal Platform Analytics

* + 1. The platform shall have an available dashboard stats section that the government web administrator can access at any time, with ability to update time period and compare (e.g. last/this year, last/this month, last/this week, yesterday/today) for entire since and ‘micro-sites’; active users, site visits, milestones reached, points earned, steps, exercises, foods logged, goals recorded, site usage (new enrollments, incomplete enrollments, HRAs completed); % of population reporting significant health measures (tobacco use, blood chem risk, hypertension, self-rating of health).
    2. The platform shall have a member management area for the government web administrator to access at any time to search specific web portal user accounts (search account by user ID and other identifying information, resent password, update email, update category for type of account, etc.).
    3. The platform shall have a master analytics area for government web admin to access at any time and ability to run ad-hoc analytics according to hierarchical levels including: location, unit/organization, pay grade, plus any combination of data field(s) captured by the platform (e.g. health outcome data including, but not limited to, BMI, physical activity, tobacco cessation, nutrition, stress management, etc., the number of employees, frequency of access among employees, community engagement quantification, point or equivalent accrual, message board posts, usage patterns, and other related web analytics).
    4. The platform shall have query capabilities whereas data can be viewed/exported for demographics, HRA, readiness for change, Physical Activity Readiness Questionnaire (PAR-Q) and ACSM readiness for exercise results, specific programming reports (smoking cessation, interactive learning programs, points programs, biometrics, calendar event reservations/attendance, web portal user short-term goals/completed wellness plan goals, workout history, pedometer log history, social interactions summary, coaching records, site usage statistics (login count, activity log account, last login date, check count/date, etc.), fitness assessments/test summaries, audit records, staff/admin account privileges).
    5. The platform shall have report capabilities whereas data can be viewed/exported for general reports (member list, login frequency, system statistics, biometric averages), wellness plan and medical reports (HRA summary, HRA results by answer, count of HRA completions, where web portal users abandon HRA, HRA data analysis using Health-Related Productivity Loss Instrument (HPLI), analysis of HPLI absenteeism data,

blood panel population), fitness assessment reports (group averages, group comparison), year-to-year comparison (HRA, biometrics), events (reservations and attendees).

* + 1. The platform shall have analytics capabilities whereas data can be viewed on a monthly, quarterly, and annual basis and be exportable for program use (e.g. PDF, Excel, CSV, Word, etc.).
    2. The platform shall have analytics clearly defined for all data outputs that can be included in reports/queries and the method(s) used to calculate them.

# Task H – Technical/Training Support

* + 1. The Contractor shall provide a high level of access and support to the Government for the web portal. The Contractor shall provide, at Government request, availability/downtime statistics.
    2. The Contractor shall deliver the web portal within the periods specified in this contract.
    3. The web-based system shall have response times that are sufficiently fast to support routine access and utilization of the system when accessing through broadband or other high-speed internet services.
    4. The Contractor shall keep the system operational 24 hours a day, 7 days a week, and 365 days per year. The web portal site shall have minimal downtime during Government business hours of 6:00am (EST) to 11:00pm (EST) (less than 15 minutes), and no more than 1 hours during non-business hours.
    5. The website service availability shall operate 99.95% of the time. Service availability is defined as uptime during defined required availability of

hours. NOTE: Service Availability = [(total number of minutes in the quarter) – (total number of minutes in the quarter that website not available)] / number of minutes in the quarter.

* + 1. The Contractor system design shall ensure that there is never to be a service outage for more than 4 hours. In the event of a catastrophic event at the hosting facility, the system should have a 4 hour stop loss on potential data loss and be able to return to service within 2 business days or less.
    2. The Contractor shall perform all scheduled system maintenance and system updates outside of required availability time periods. Actions to perform routine maintenance or update the system shall not be more than 1 hour per instance.
    3. The Contractor shall notify the Government at least 5 days in advance for all planned maintenance actions affecting access to the system that occur during critical or

non-critical availability time frames and obtain written consent from the Government for approval of the maintenance action.

* + 1. The Contractor shall post a notice of temporary unavailability on the impacted website, in the event maintenance is performed and/or part or all of the system is unavailable for use. This message shall explain the outage and when the system is expected to be available for use.
    2. The Contractor shall provide technical support and have a process for submitting work tickets for website issues (i.e. help desk) and have accessible web developer staff who can assist Government with troubleshooting (e.g. account issues, access errors, configurations not performing properly, content not displaying properly, etc.).
    3. The Contractor shall respond via telephone or email within 24 hours for technical assistance and problem resolution from Government notifying of an issue.
    4. The Contractor shall respond within 72 hours of request for new website and customization requirements (e.g. report queries, addition/removal of HRA questions, custom incentive design, etc.) and provide estimated hours required, as well as a timeline for completion of request.
    5. The Contractor shall respond within 72 hours of request to provide other data reports (e.g. utilization) which may be requested on an as needed basis.
    6. The Contractor shall provide mechanisms (e.g. ‘how to’ videos and documents) that will assist web portal users with key features of site to make more user friendly, as well as assist Government with ‘how to’ operational trainings (e.g. tele-/video-conference trainings, electronic resource manual, resource videos, documents) to explain key features, configurations, report/query pulls, etc.

# Task I – Information Security and/or Physical Access Security Requirements

* + 1. 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:
          1. Access (Physical or Logical) to Government Information. A contractor employee shall have or shall be given the ability to have routine physical (entry) or logical (electronic) access to government information.
          2. Operate a Federal System Containing Information. A contractor shall operate a federal system and information technology containing data that supports the Government 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.

* + - 1. 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 shall:
         1. 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;

* + - * 1. Provide security for any contractor systems, and information contained therein, connected to an Air Force network or operated by the contractor on behalf of the Government regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or contractor, if existing safeguards have ceased to function, the discoverer shall immediately, within 1 hour or less; bring the situation to the attention of the other party.
        2. Adapt and implement the policies, procedures, controls, and standards required by the Government to ensure the confidentiality, integrity, and availability of government information and government information systems for with the contractor is responsible under this contract or to which the contractor may otherwise have access under this contract.
      1. 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 Air Force 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: MODERATE
* Integrity: MODERATE
* Availability: MODERATE
* Overall Risk Level: MODERATE
  + - * 1. Based on the information provided by the Government security/privacy representative, it has been determined that this solicitation/contract does involve 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 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.
      1. 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 shall comply with Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR, part 2002) when handling CUI. 32 CFR 2002.4(aa) as implemented the term "handling" refers to "...any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, reusing, and disposing of the information." 81 Fed Reg 63323. All sensitive information that has been identified as CUI by a regulation or statue, handled by this solicitation/contract, shall be:
         1. Marked appropriately.
         2. Disclosed to authorized personnel on a Need-To-Know basis;
         3. Protected in accordance with NIST SP 800-534, 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 systems; and;
         4. Returned to Air Force 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.
      2. 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 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, “Security Requirements for Cryptographic Modules”, validated solution.
         1. Any information provided to the contractor by Air Force or collected by the contractor on behalf of Air Force 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 shall be under the

supervision of the Contractor. Each Contractor employee to whom Air Force records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee can be used only for that purpose and to the extent authorized herein.

* + - * 1. The confidentiality, integrity, and availability of such information shall be protected in accordance with Air Force policies. Unauthorized disclosure of information will be subject to the Air Force sanction policies and/or governed by the following laws and regulations:
* 18 USC 641 (Criminal Code: Public Money, Property or Record);
* 18 USC 1905 (Criminal Code: Disclosure of Confidential Information); and
* 44 USC, Chapter 35, Subchapter I (Paperwork Reduction Act).
  + - 1. 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)”.
      2. Government Websites. All new and existing government websites shall 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 insecurity 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.
      3. Contract Documentation. The contractor shall use provided templates, policies, forms and other Government documents provided to comply with contract deliverables as appropriate.
      4. Standard for Encryption. The contractor shall:
         1. Comply with procedures and standards set forth in AFMAN 17-1301 to prevent unauthorized access to government information.
         2. 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 device, backup media, etc.) with FIPS 140-2 validated encryption solution.
         3. Secure all devices (i.e. desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet Air Force-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computer, and other mobile devices and portable media that store or process sensitive government information (including PII).
         4. Verify 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 validated documentation to the Government upon request.
         5. Use the Common Access Card to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys.
      5. System of Records Notice (SORN)/Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA). The contractor shall assist the system owner in submission of a SORN if required.
         1. The contractor shall also assist Air Force security professionals with conducting the PTA for the information system and/or information handled under this contract to determine whether or not a fill PIA needs to be completed.

If the results of the PTA show that a full PIA is needed, the contractor shall assist the Air Force with completing a PIA for the system or information handled after completion of the PTA in accordance AFI 33-332, Air Force Privacy and Civil Liberties Program.

The contractor shall assist the Air Force security professionals in reviewing the PIA at least every 3 years throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

* + 1. Security Training for contractor staff with CAC cards
       1. Mandatory Training for All Contractor Staff with CAC cards. All contractor employees assigned to a CAC card to work on this contract shall complete CyberAwareness Challenge training located on the Advanced Distributed Learning Service (ADLS) prior to being granted access to the AF Network. CyberAwareness Challenge training will be re-accomplished annually.
       2. Training Records. The contractor shall maintain records for all its employees with CAC cards working under this contract in accordance with Air Force policy.
    2. Security Rules of Behavior. The contractor shall ensure that all employees performing on the contract comply with the Air Force Information Technology General Rules of Behavior, and any Air Force policies as applicable.
       1. All contractor employees performing on the contract shall 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 Computer Security (COMPUSEC) and Information Security (INFOSEC) training. The

contractor shall submit to the Government a signed signature page for each employee prior to employees performing any work under this contract and annually thereafter.

* + 1. Security Incident Response. The Contractor shall respond to all alerts/Indicators of Compromise (IOCs) provided by Air Force Computer Security Incident Response Center (CSCIRT) team within 24 hours, whether the response is positive or negative. Federal Information Security Modernization Act (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.
       1. The Air Force 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 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. The Air Force Policy for IT Security and Privacy Incident Reporting and Response further defines a breach as "a suspected or confirmed incident involving PII." In the event of a suspected or confirmed incident or breach, the contractor shall:
          1. Protect all sensitive information, including any PII created, stored, or transmitted in performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.
          2. NOT notify affected individuals unless so instructed by the Government. If so instructed by the Government, the contractor shall send recommended notifications to the Government first for approval before sending.
          3. Report all suspected and confirmed information security and privacy incidents and breaches to the Government COR, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible without unreasonable delay, no later than one (1) hour, and consistent with the applicable Air Force policy and procedures, NIST standards and guidelines, as well as United States Computer Emergency Readiness Team (US-CERT) notification guidelines.
       2. The types of information required in an incident report shall include at a minimum company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:
          1. Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
          2. NOT include any sensitive information in the subject or body of any reporting e-mail;
          3. Encrypt sensitive information in attachments to email, media, etc.
       3. Comply with OMB Memorandum 17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information”, and Air Force incident response policies when handling PII breaches.
       4. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks, or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.
    2. Contract Security Initiation and Expiration.
       1. General Security Requirements. The Contractor shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, and Air Force 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 Air Force EPLC framework and methodology and in accordance with the Air Force Contract Closeout Guide (2012).
       2. System Documentation. Contractors shall 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 shall provide all required documentation to the COR to certify that, at the government's discretion, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with remanence security in AFMAN 17-1301, COMPUSEC and NIST SP 800-88, Guidelines for Media Sanitization.
       4. Notification. The Contractor shall immediately notify the Government COR when a Contractor no longer requires agency access due to transfer, completion of a project, retirement, removal from work on the contract, or termination of employment. Return all Government property to include Common Access Card and computer equipment.
       5. Contractor Responsibilities upon Physical Completion of the Contract. The Contractor 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 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 Remanence Security guidelines set forth in AFMAN 17- 1301.
       6. Records Management and Retention. The Contractor 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 Air Force policies and shall not dispose of any records unless authorized by Air Force. In the event that a Contractor accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with Air Force policies.
       7. Confidentiality of Medical Records. The Contractor shall treat all records containing employee medical information as confidential and maintain them in accordance with 5 U.S.C. 552a, the Privacy Act of 1974, and Air Force guidelines.
    3. Requirements for Privacy Act Records. This contract is subject to the Privacy Act of 1974, because in order to carry out the required services the contractor may retrieve personal health information about an employee who participates in an agency sponsored health and wellness program by the employee's name. The federal employee medical, wellness and similar records are owned by the office of Personnel Management (OPM) but are administered on behalf of OPM by Air Force (and its contractors) and by employing federal agencies (and their contractors).
       1. At the end of contract performance, the Government shall provide disposition instructions to the contractor for securely transferring and/or destroying (in accordance with NISP SP 800-88) any Privacy Act records used in performing this contract that are then in the contractor's custody or control. The disposition schedule that applies to federal employee medical, wellness, and similar records is GRS 2.7 Employee Health and Safety Records.

# Task J – Security Assessment and Authorization (SA&A)

* + 1. Security Requirements for COCO Systems.
       1. Federal Policies. The Contractor shall comply with applicable federal laws that include, but are not limited to, the Air Force Information Security and Privacy Policy (IS2P); Federal Information Security Modernization Act (FISMA) of

2014, (44 U.S.C. 101); National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”; Office of Management and Budget (OMB) Circular A-130,

“Managing Information as a Strategic Resource”; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.

* + - 1. Authorization to Operate (ATO).

A valid ATO certifies that the Contractor's information system meets the contract's requirements to protect the agency data. The Contractor shall work with the agency to obtain an ATO as soon as possible. The process should have been done with the previous contract and the government is now aware of the task this is and will work with the contractor to accomplish this within the first 6 months. The contractor shall serve as the Information System Security Manager (ISSM) and perform the duties outlined in DoDI 8500.01, Cybersecurity and AFI-17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT). The Contractor shall have an account in Enterprise Mission Assurance Support Service (eMASS) which requires a secret clearance.

* + - * 1. SA&A Package Deliverables - The Contractor shall be required to provide an ATO package submitted within the eMASS. A secret clearance will be required prior to receiving an eMASS account. The majority of work involved with compiling an ATO package will occur in the year prior to expiration of a current ATO, if relevant. The following SA&A deliverables are required to complete the SA&A package in addition to the Air Force baseline listed below:

System Categorization. 3.10.1.2.1.2. System Security Plan (SSP). 3.10.1.2.1.3. Privacy Impact Assessment (PIA). 3.10.1.2.1.4. IT Contingency Plan (ITCP).

ITCP Test Results.

Configuration Management Plan (CMP). 3.10.1.2.1.7. Incident Response Plan (IRP).

Service Level Agreements (SLA), as required.

Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU), as required.

Plan of Action and Milestones (POA&M) - due after the final SCA has been provided in the Air Force template format.

* + - * 1. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the COCO systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, and Air Force IS2P. The minimum requirements for ISCM will be followed.
        2. Government Access for Security Assessment. In addition to the Inspection Clause in the contract, the Contractor shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and

personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of Air Force, including but are not limited to:

At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract. The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the Air Force Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross-site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

Cooperate with inspections, audits, investigations, and reviews.

Government inspection and access to FedRAMP-certified cloud computing environments will conform to FedRAMP certification rules and regulations.

* + - * 1. Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor. The Contractor shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of Air Force are deployed and operated in accordance with approved security configurations and meet the following minimum requirements.

Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with Air Force and FIPS 140-2 encryption standards.

Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), and Air Force Minimum Security Configuration Standards;

Maintain the latest operating system patch release and anti-virus software definitions;

Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and

Automate configuration settings and configuration management in accordance with Air Force security policies, including but not limited to configuring its systems to allow for periodic Air Force vulnerability and security configuration assessment scanning.

* + 1. Technical Requirements. The following are specific technical requirements that apply to the service that will be delivered to the Government and its website users.
       1. Administrative Security Requirements
          1. The service provided by this contract shall be a web application able to be administered by Government/CHPS program staff, and accessed by Government website users that are the recipients of the service that is being offered.
          2. The Contractor shall be responsible for all development & maintenance of this system. The contractor will also host this system at their site &/or via a commercial hosting facility.
       2. Technical Application Requirements
          1. The web application shall support access via personal computers running Windows 10 or newer Microsoft operating systems as they become commercially available, and be fully functional when accessed from a Windows PC using Google Chrome, Microsoft Edge or other appropriate web browsers.
          2. Reports from the web application shall be accessible as HTML, or via a current copy of Adobe Acrobat Reader.
          3. Users that access the application using other browsers shall, at a minimum, receive basic functional support, as well as direction to use the defined baseline system to receive access to full functionality.
          4. Users shall be able to access the site from anywhere that they have an Internet network connection. The system should be fully functional on network connections as low as 2MBPS.
          5. The web application shall not require any installed components. It shall not require use of plug-ins, Active-X components, or Java components.
       3. Technical Domain Requirements.
          1. The web application shall be accessible via one (1) URL that Air Force will define and own.
          2. Each domain shall have a designated group of Air Force/CHPS staff administrators that will be responsible for administering content and controlling configurable elements of the service under that domain.
          3. Government web administrators for a domain shall be able to access reports on people that gained services under the domain they oversee.
       4. Authentication Requirements.
          1. The web application shall allow users to log into the web site to make use of web portal features.
          2. The web site will use SSL certificates so that interaction with the site is performed in a secure manner.
          3. New users that do not have an account will be allowed to register and request a new account. The system will allow users to reset their own password by following a link in an email sent to their registered email address.
          4. When users register, the system shall be configurable to require that they provide a registration code. That registration code may be used to authenticate that they are legitimate registrants &/or to identify a specific subgroup that they belong to.
          5. The registration process shall provide the capability for government web administrators to collect a limited set of custom information that is unique to their set of Government website users (i.e. location or other organizational identifiers).
       5. Record Security.
          1. The contractor shall ensure that all information voluntarily entered into the system is assumed to contain Personal Identification Information (PII), as well as Personal Health Information (PHI).
          2. Government web administrators may gain access to trend analysis reports, as long as the population being reported on is significantly large enough as to not disclose personal or health details about individual staff.
          3. The web portal system shall keep some form of record of who accesses the account and/or the information associated with the account.
       6. Requirements for Cloud Services.
          1. The Contractor shall utilize government owned cloud environments or a commercial FedRamp-compliant GOVCLOUD which provides for Government-specific regions in which to deploy Infrastructure as a Service (Iaas) or Platform as a Service (PaaS).
          2. The Contractor shall also ensure that all data in transit to and from the cloud provider is encrypted using the latest standards. Data stored on a cloud provider's premises shall conform to encryption standards for data at rest according to NIST Special Publication 800-144.

# Task K – Position Sensitivity Requirements

* + 1. To perform the work specified herein, some contractor personnel shall require access to proprietary, privacy protected and/or sensitive data, regular access to Air Force- controlled facilities and/or access to Air Force information systems.
    2. The Contractor shall have an approved background investigation/security check (Tier 2, Level 5 Public Trust with subject interview).
    3. The Contractor personnel appointed as ISSM shall have a SECRET clearance (Tier 3 investigation) in order to acquire an account in eMASS.
    4. The Contractor shall comply with the instructions and timeframes provided by the Contracting Officer's Representative (COR) regarding the handling of the security requirements specified in this section.
    5. Within 7 calendar days after the contract expiration, the contractor shall return all identification badges, Government Furnished Equipment, Government Furnished Data and Government Furnished Property (GFE/GFD/GFP) if applicable, to the COR. Within seven (7) days after employee departure at any time during the contract, the contractor shall return all identification badges, and GFE/GFD/GFP if applicable, to the COR.
    6. Identification Card Custody and Control.
       1. The Contractor is responsible for the custody and control of all forms of Homeland Security Presidential Directive 12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors”, credentials issued by Air Force to Contractor employees. The Contractor shall immediately notify the COR when a Contractor employee no longer requires agency access due to transfer, completion of a project, retirement, removal from work on the contract, or termination of employment. Return all Air Force HSPD-12 Credentials to the appropriate credentialing office.
       2. The Contractor shall also ensure that Contractor employees comply with Air Force requirements concerning the renewal, loss, theft, or damage of an ID card. Failure to comply with the requirements for custody and control of Air Force issued ID cards may result in a delay in withholding final payment or contract termination, based on the potential for serious harm caused by inappropriate access to Air Force facilities, sensitive information, information systems or other Air Force resources.
       3. Renewal: A Contractor employee's Air Force issued ID card is valid for a maximum of five (5) years and 9 months or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin six weeks before the ID card expiration date by contacting the COR. If an ID card is not renewed before it expires, the Contractor employee will be required to sign-in daily for facility access and may have limited access to information systems and other resources. Contractor ID card certificate(s) require yearly updates from the issuance date. The yearly updates should be coordinated between the contractor and the COR. Air Force reserves the right to impose annual expiration dates on Air Force issued ID Cards at any time.
       4. Lost/Stolen: Immediately upon detection that an ID card is lost or stolen, the Contractor or Contractor employee shall submit an Incident Report within 24 hours for any and all lost or stolen Air Force Credential to the Government COR and the local security servicing organization. The Incident Report shall describe the circumstances of the loss or theft. If the loss or theft is reported by the Contractor to the local police, a copy of the police report shall be provided to the COR The Contractor employee shall sign in daily for facility access and may have limited access to information systems and other resources until the replacement card is issued.
       5. Replacement: A Credential will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than three (3) days, provided there is a continuing need for agency access to perform work under the contract.
       6. Surrender Credentials/Access Cards, Government Equipment.
          1. The Government reserves the right to suspend or withdraw access at any time for any reason. Access will be restored upon the resolution of the issue(s).
          2. Upon notification that access to Government facilities, proprietary, privacy protected and/or sensitive information, federally controlled information systems or other Government resources is no longer required, the Contractor shall surrender the Government issued Credentials, access card, keys, computer equipment, and other government property to the COR.
          3. Contractor personnel who do not return their government issued property within 48 hours of the last day of authorized access to Government facilities/systems, may be permanently barred from Government systems and facilities and may be subject to fines and penalties, as authorized by applicable Federal or State laws.

# Task L – Transition In/Out Plans.

* + 1. Upon contract award, the contractor shall provide a comprehensive transition in/out support plan within 30 days of contract award when transitioning to another contractor. The transition in and out period will be completed within 90 days.
    2. Prior to the expiration of the contract, the contractor shall provide an encrypted export of all data and tables in 32bit and 64bit formats that can be imported into Microsoft SQL Server and Oracle to the Government with updates after the contract end. This data includes health promotion records for approximately 100,000 or more active web portal users plus additional inactive web portal user historical data from the past 13 years.
    3. To ensure continuity of services, the Contractor shall provide a transition plan, transition training, and services. During this period, staff from the incumbent contract shall be available to familiarize and train the successor Contractor staff with program operations. The Contractor's transition plan shall provide adequate coverage to ensure uninterrupted service to the Government and be effectively and efficiently administered. Contractors shall cooperate fully with each other to ensure that all services continue without interruption.
    4. ATO. The purpose of the ATO is to establish security accreditation for the Contractor's data system. Specifically, Air Force security and privacy management policies require security accreditation for any contracts that use a data system to manage sensitive information. The accreditation process ensures that the Contractor's system complies with policies, procedures, controls, and standards of the Air Force Information Security Program.
       1. Immediately upon award of the Base contract, the successor Contractor shall begin the Information Technology (IT) certification process to receive an ATO. Please see Task J for the steps to obtain an ATO.
       2. The Contractor shall attend a planning meeting within ninety (90) days of contract award to meet with the Government COR and other key organizational contacts to discuss the ATO requirements, policies, procedures, information technology interfaces, and government organization nuances.
       3. After the Government grants the ATO, the contractor shall transition data into the production system(s) and execute test cases and exception protocol. The government PM/COR will review these reports and accept the transition process.