Sample Task #1

Medical Treatment Facility (MTF) Military Construction (MILCON) Cybersecurity Engineering and Cybersecurity Assessments.

This sample task is similar in format to a typical United States Army Information Systems Engineering Command (USAISEC) Task Order. This is a Cost Plus Fixed Fee (CPFF) Task Order. The Background Section includes information about the sample task and is intended to provide sufficient information to the Offerors. The Applicable Documents Section is representative of the documents that would be pertinent to conducting the Task Order work. The Requirements Section contains several products typical for most Task Orders.

In response to this sample task, include a detailed technical approach describing how you would solve the requirements. For this sample task, the period of performance (PoP) will be 12 months as that is representative of USAISEC Task Orders. The Offerors will use January 1, 2020, as a start date for this sample task.

The Offeror shall provide a narrative response describing the Technical Approach, as described in Section 3 of this sample task. The sample task response shall be accompanied by the documents detailed below.

a) Quality Control Plan and associated task checklist(s) tailored for this sample task;
b) Work Breakdown Structure (WBS) for this sample task (which shall include the Basis of Estimate (BOE));
c) Project work schedule (using MS Project) for this sample task; and
d) Risk Mitigation Plan tailored for this sample task.

The WBS shall include a minimum of a three-level breakdown and a BOE. The BOE shall include the labor categories and hours required to complete the Sample Task as proposed and the rationale to support the labor estimates. ***The BOE shall NOT include any labor rates or cost information inclusive of material, travel or other direct costs (ODCs).*** *The Offeror shall populate the Government-provided spreadsheet in Volume IV – Cost/Price Factor, with all costs for this sample task. NOTE: The Quality Control Plan and the Risk Mitigation Plan are included within the Sample Task 25 page limitation. The associated task checklist(s), the WBS and BOE file and the Project Work Schedule file are NOT included in the Sample Task page limitations. A notional work breakdown structure is included to illustrate a sample three-level breakdown.*

1. BACKGROUND.

NOTE: The work to be performed for this sample task will only cover Cybersecurity Security Engineering (SE) for the replacement Medical Treatment Facility (MTF) network and Security Control Assessments (SCA) for 3 systems.

The tasks are described in Section 3 of this document. All other MILCON phases such as furnish, install, and system test are being performed by the US Army Corps of Engineers (USACE) or other stakeholders. Section 1 is strictly initial background information collected by USAISEC from the MTF staff of the MILCON effort. The MILCON background information is subject to change as the MILCON is under a design/build approach. Additional information that the Offeror feels is needed for its proposal will need to be gathered via performance of the sample task.

1.1 USAISEC has a requirement to provide Cybersecurity support services for the additions, alterations, renovations, and relocations the Defense Health Agency (DHA) is undertaking for its clinics, laboratories, medical centers, and hospitals. A relocation is a complete/new replacement. A renovation is an update to an existing building or a return to a new condition. An alteration is a change to an existing facility. An addition is adding to an existing facility.

1.2 The Colorado Springs Military Health System is an integrated military health care delivery system that combines the services from all military hospitals and clinics in an area. The MTFs for the Colorado Springs Military Health System are:

- Evans Army Community Hospital (EACH) located at 1650 Cochrane Circle,
  Building 7500 Colorado Springs, CO 80913-4604. Facility is undergoing relocation/replacement.
- Premier Army Health Clinic located at 3920 North Union Blvd, Colorado Springs, CO 80907. Undergoing renovations and not part of this effort.
- Mountain Post Medical Home located at 565 Space Center Drive, Colorado Springs, CO 80915. Undergoing alterations and not part of this effort.
- U.S. Air Force Academy Clinic (10th Medical Group) located at 4102 Pinion Drive, Colorado Springs, CO 80840-4000. Undergoing additions and not part of this effort.
- Peterson Air Force Base Clinic (21st Medical Group) located at 559 Vincent Street Building 959, Colorado Springs, CO 80914-1540. Undergoing renovations and not part of this effort.
- Schriever Air Force Base Clinic located at 220 Falcon Parkway, Colorado Springs, CO 80912. Undergoing renovations and not part of this effort.

NOTE: For the purpose of this Sample Task, the Offerors will only perform Cybersecurity Security Engineering (SE) tasks for the Replacement EACH network and Security Control Assessor – Validator (SCA-V) Security Control Assessments (SCA) for 3 systems. These tasks are in section 3.

1.3 The United States Army Corps of Engineers (USACE) is utilizing a design/build model for the replacement MTF design and construction.

The design/build approach allows construction to commence before full detailing of the drawings is complete. The design/build approach also allows portions of the project to be designed and/or changed on site to expedite the design and construction process. The USACE has hired an Architect and Engineering (A/E) firm which has produced the overall building design. They are teamed with a construction firm that is implementing this design. The Beneficial Occupancy Date (BOD) of the Replacement EACH is currently scheduled for 1 June 2020.

1.4 Applicable Federal, Department of Defense (DoD), Department of the Army (DA), and DHA requirements shall be followed while the MTF maintains duel operations in the older existing facilities. The Replacement EACH will be 750,000 gross square feet; nearly double the size of the previous hospital. It will contain 90 inpatient beds, 5 acuity adaptable Intensive Care Units (ICUs), 4 step down ICU's, 25 medical surgical beds, 15 mother baby beds, and 25 psychiatric beds. In addition, the new ICU will contain 8 rooms with the capability to expand up to 24 acuity adjustable beds. The new hospital will be seeking Leadership in Energy and Environmental Design (LEED) Silver certification from the United States Green Building Council upon completion. The Green features will include a vegetative roof, energy-efficient lighting systems and views of nature. The facility will consist of a main hospital, inpatient and outpatient clinics, administrative building, research building, central utility plant, two access control points and surface parking. The facility will also include a modern world-class 45,000 square foot data center. The data center will contain unclassified communications equipment areas for SENSITIVE BUT UNCLASSIFIED Internet Protocol Data (SBU IP), and a SECRET Internet Protocol (IP) Data room. Also planned for the replacement MTF are the Commercial Communications Equipment Room (CCER) which demarks the Government and the commercial points of presence; the Audio-Visual (A/V) equipment room which houses the A/V control system; and an operations center which includes the command center, environment & physical security center, and crisis action team areas.

1.5 The following information for the Replacement EACH has been identified to date.

1.5.1 **General Characteristics:** a) approximately 2,800 users will occupy the Replacement EACH; b) the Replacement EACH data center will be a SBU IP data facility with one SECRET IP data room containing two Secure Terminal Equipment (STE); c) the facility will include a critical operations area for a medical crisis action team. The facility will include support for physical security in accordance with the installation physical security program which includes physical Intrusion Detection Systems (IDS), facility access control, alarms, Protective Distribution Systems (PDS) and other elements as required. The facility will include a centralized Physical Access Control System (PACS). The PACS will provide access

control to the facility and any areas designated restricted or controlled access within the facility. The PACS will include the DoD Common Access Card requirement and will meet the differing security/access needs for sensitive areas such as maternity wards, emergency departments, intensive care units, and asset protection.

1.5.2 **Data Characteristics:** All users will require access to the SBU IP data with approximately 2-5 users requiring access to SECRET IP data. Access will be for messaging services, e-mail, internet, and access to various enterprise and medical information systems.

The plan for the replacement data center is to accommodate existing data requirements plus allow for 25% growth. Information gathered to date is as follows:

- Staff Accounts in Active Directory - Estimate 2,800.
- Each user will receive 50 Gigabytes (GB) of User Data.
- Virtual Desktop Infrastructure (VDI).
  - 2000 VDI Images.
  - 30 GB Images.
  - 2 Chassis.
    - 1 Spare Failover Blade for each Chassis.
    - Each Blade is configured to have 20% head room.
  - Virtual Tier 1-3 Storage Area Network (SAN) – Redundant Array of Independent Disks (RAID) 10.
  - Tier 1 Solid State Drive (SSD) – 400 GB.
    - Percent of image – 15%.
  - Tier 2 10K Rotation Per Minute (RPM) - 600 GB.
    - Percent of image – 25%.
  - Tier 3 7200 RPM - 2-3 TB.
    - Percent of image – 60%.
- User and Public Data SAN.
  - Public SAN.
    - 12 Terabytes (TB) of Storage.
    - Public files, regulations, and command historical files.
  - End Users Data Storage.
    - Assumed 2800 users.
    - 50 GB each of storage.
  - 3 Tier SAN – RAID 10.
- 1 Print server for each 50 Printers.
  - # of print servers to be determined and depends on the final number of network printers to be identified.
- SQL.
  - Multiple versions of SQL. Need to be identified/vetted as approved.
  - There will be Central Load Balancing SQL servers that manage the different versions.
- Applications.

- Will be redundant with Load Balancing.
- Blades will be configured with 20% head room.

- Datacenter Servers Design.
  - 99.999% Server and SAN uptime.
  - All applications will be load balanced and have the potential for failover. Fail system will live migrate to a different virtual host.
    - Servers will patch with minimal impact to users.
  - Data will be virtualized across Tier 1-3 Disk array.
    - RAID 10 disk drives.
  - Planned - Virtual Disk Backup, off-site storage of public files, user data, and Structured Query Language (SQL) databases.
  - Planned - Servers and disk space for hospital Real Time Location System (RTLS) and Smart Suite.

1.5.3 **Voice Characteristics:** a) users will require access to commercial and Defense Switched Network (DSN) telephone services, with approximately five critical users requiring precedence capability to the FLASH level; b) approximately 2 - 5 users will require secure voice access.

1.5.4 **Video Characteristics:** a) conference rooms will be capable of displaying the following video inputs: high-resolution graphics, cable television (CATV), and Common Operational Picture (COP); b) The plan currently is for there to be 3 small conference rooms, 2 medium conference rooms, and 2 large conference rooms (with one capable of a SECRET VTC).

1.5.5 **Access Control Characteristics:** a) Access-control for segmented specialties, such as cardiac, research, emergency and maternity wards, have different needs and requirements. The use of door-opening technologies that do not require an individual to touch a door handle or crash bar will be implemented in key areas. Door readers will be used in other areas and will read a credential, authenticate the user, and open the door automatically; b) the access control system will integrate patient-wandering detection, infant-monitoring systems, and IP and Closed Circuit Television (CCTV).

1.5.6 **Network Characteristics:** The replacement MTF network will initially be an extension of the current hospital Information Management Division (IMD) network that will require periodic connection to the internet for updates, patches and data through-put testing. This requirement creates a need for monitoring the physical and logical access to the network devices to ensure that the accepted configurations are not altered. The following has been identified to date for the replacement MTF’s network:

- Physical Access Restrictions: The data center and Telecommunication Rooms (TRs) will be restricted to authorized personnel only. The key lock cores during construction will be changed and keys will be issued to a limited number of personnel to be determined (TBD). Designated personnel will sign for the key and will be listed on an access roster. The MILCON Contracting Officer's Representative (COR) will be notified when additional personnel need access to restricted areas since the replacement hospital is still in a construction area.
- Logical Access Restrictions: The replacement network, during construction, will be temporarily configured on a Virtual Local Area Network (VLAN) that is non-routable. Initially there will be no routing gateway included to prevent information being passed into the production network at the current/old facility. This will be further restricted by managed connection/disconnection of the trunk effectively isolating the replacement hospital segment from all data transmission when not testing.
- Uninterruptable Power System (UPS): UPS testing will include the Power Monitoring Units that will connect to the network. The Power Monitoring Units have a web interface that will be configured in accordance with applicable security requirements to limit access to authorized personnel.
- Wireless Access Points: There will be 328 Cisco Access Points (APs) located throughout the facility and connected to a Cisco controller module. The access points will be tested to ensure that they are functioning and being identified by the management console.
- Cisco Prime Wireless Management: The Cisco Prime Infrastructure is a software application that provides management capabilities for the wireless AP. This application is hosted on a Redhat Enterprise server 64 bit Operating System (OS). This system can be joined to an Active Directory (AD) domain and the smartcard capability can be activated for two-factor authentication.
- System Updates and Patch Management: When possible, the general system updates and Information Assurance Vulnerability Alert (IAVA) compliance patches will be applied as the systems are being configured. Configuration management information will be updated to reflect any changes to the established installation configuration as they occur.
- Network Traffic Logs: Switches will be monitored and traffic will be logged to identify the ports and services that are being used. This will aid in the refinement of the PPSM. This will also ensure that deny statements contained in the access

control list (ACL) are functioning as designed.

- Temperature and Humidity Controls: The temperature and humidity controls have been installed and are functional. This capability will provide the environment necessary to stabilize the ambient temperature while the infrastructure systems are powered on.
- Overview: Two core switches and the server farm switch will be located in the data center. The layer 2 switches will be located in the head end room and various TR's throughout the replacement hospital. It is anticipated that the MILCON installation team(s) will need an active network link to the internet on several occasions during installation/testing and during the cut-over period. The replacement hospital will have a physical cabling design that provides system connectivity and the ability to communicate to the external enclaves. This will be accomplished by designing and constructing information technology (IT) spaces, pathways, and a structured cabling system (SCS) that meets or exceeds standards set forth in ANSI/TIA-568-D, ANSI/TIA-569-D, ANSI/TIA/-606-B, and J-STD-607-B. The wireless portion of the implementation will consist of the access points, wireless controllers, and the Prime Infrastructure. The critical systems will be connected to an American Power Conversion (APC) UPS for power management.

1.6 The MILCON stakeholders have identified the following 3 systems for Type Accreditation. These systems will be implemented in the Replacement EACH facility.

1.6.1 **Electronic Security System (ESS)**.
General System Description: The ESS will protect staff, patients, and visitors by providing access cards with photo, employing video surveillance, controlling access to sensitive areas of the facilities, initiating duress alarms, protecting infants from abduction, and allowing emergency communications.
Technical System Description: The ESS consists of the following subsystems:

- Access Control System (ACS): The ACS provides controlled access to specified facility doors from a single integrated security system. Designated doors use a proximity reader while more sensitive areas are protected with a proximity card reader and a keypad to allow only authorized persons entry. Unauthorized entry causes an alarm to be received at the security center for security response. Where available, CCTV images are automatically displayed for the responding security forces. A typical access controlled door consists of a door position switch, electronic locking hardware, proximity card reader, and request-to-exit device.

- CCTV System: The CCTV and recording system provides general surveillance throughout the facilities from operator workstations. Cameras are continually recording and stored via centralized servers.
- Emergency Call Station (ECS) System: The ECS system provides voice communication and alarms in parking lots and garages in the event of an emergency. Upon activation of the “talk” button, the station provides alarm notification and voice communications from the associated ECS back to the security management office / emergency department security desk. ECSs can be located throughout the staff, clinic and hospital parking lots as well as the staff, clinic, and hospital garages. Each ECS will be clearly identified with “EMERGENCY” indicated on it. Upon an ECS being activated, an automated camera call-up is activated for visual coverage of the associated event; reports and exported video will be able to be saved to media.
- Radio-Frequency Identification (RFID) Asset Tracking System: A radio frequency identification system will track equipment throughout the hospital and the clinics. The system utilizes a 433MHz active RFID infrastructure consisting of Radio Frequency (RF) antennas/tag readers, exciters, and asset tags. These devices can be installed and configured to track tagged equipment on a zonal basis with each floor defining a zone. One thousand (1,000) asset tags will be provided for implementation and testing, and additional tags can be acquired depending on the volume of equipment to be tracked. The RFID system allows personnel to search for specific items and/or specific types of tagged equipment.
- Infant Protection Alarm System (IPAS): The Infant Protection Alarm System (IPAS) protects infants under the care of the facility personnel in secured areas. A tag can be placed on each infant under the care of the facility. The IPAS will detect and report alarms if an attempt is made to move an infant being tracked by the system from the mother, labor and delivery, neonatal ICU, or Inpatient Pediatric Unit (IPU); or if there is an unauthorized removal of the tag from an infant being tracked.

System Dependency: The ESS system will be operationally independent from the facility’s network enclave. The ESS can be interfaced to numerous hospital systems to transmit alarm information and alerts.

System Interface: Interfaces between subsystems will occur by means of an Integrator Network Subsystem (INS). Alarms from all systems will be routed to the ACS for display and annunciation. Servers for the ACS, ECS, IPAS and CCTV will communicate via software integration. Selected alarms received at the ACS will be

relayed to the radio paging system to alert the appropriate facility personnel (security staff and/or nurses) of the alarm condition. The system is designed such that when an alarm occurs, the video from the camera(s) in the vicinity of the alarm will be displayed at the operator workstation.
System Accreditation Status: None.
See attachments #.

- ATT022 1.6.1A_ESS Network HW-SW List
- ATT023 1.6.1B_ESS Network Diagram
- ATT024 1.6.1C_ESS Ports and Protocols List

1.6.2 **Interactive Television System (ITV)**.
System General Description: The ITV system will utilize a dedicated Ethernet IP- switch-based Local Area Network (LAN) for the distribution of educational material for both staff and patients, live broadcasts, CATV, entertainment (which will be selected programs by the Hospital IMD), Video-On-Demand (VOD), informational messaging services and surveys. Location of system equipment and outlets will be coordinated with the USACE/hospital user representative and as specified within DOD medical equipment room guide plates.
System Technical Description: The ITV will have a dedicated LAN including network switches, patch panels, fiber optic and unshielded twisted pair (UTP) cable, and modular TV outlet jacks. Components of the ITV system also include: a) channel processors to translate live program; b) components to interconnect with the post CATV system trunk line; c) equipment components and cabling to connect to the system distribution networks; d) network time synchronization, rack cabinet, and a Multimedia Interactive Network Center (MINC) which is comprised of a host computer, required application computers, video monitors, Keyboard, Video, Mouse (KVM) switcher, keyboard, mouse, printer, UPS, digital video servers and storage, Video Cassette Recorder (VCR) / Digital Video Disc (DVD) recorder, data switches/routers, network adapters, TV channel modulators, combiners, TV sets, and equipment rack cabinets.
System Dependency: System’s connectivity will be managed and is described as having a few very well defined data exchanges in fixed formats.
Interface: The ITV system is capable of accepting input from the hospital patient information system via an Admission, Discharge, and Transfer (ADT) stream, as well as a Video on Demand (VOD) feed (via an Internet connection), as allowed by the hospital IMD. Distribution will consist of interconnecting a core Ethernet switch to multiple access switches, via single mode fiber, in designated telecom rooms. Each access switch will connect ITV outlets by means of a Category 6 UTP data cable.
System Accreditation Status: None.

See attachments #.

- ATT025 1.6.2A_ITV HW-SW List
- ATT026 1.6.2B_ITV CONOPS Diagrams
- ATT027 1.6.2C_ITV Ports and Protocols List

1.6.3 **Nurse Call (NC) System**.

System General Description: The NC system is an integrated system that provides patient and caregiver communications while utilizing industry standard protocols. The Nurse Call Television (NCTV) (television/nurse-call remote) will be located in patient treatment rooms and patient recovery rooms. This is a system comprised of code blue duty stations, emergency call stations and dome lights connected to an annunciator panel. Similar to the NCTV, the NC Audio/Video (AV) will be located in the emergency department and patient bedrooms in the hospital bed tower. Features include a patient pillow speaker that allows the patient to control reading lights, assigned television channels as well as full duplex intercom capability to allow for two-way communication. For psychiatric patient bedrooms, the nurse call system will be activated by a key switch located outside of the patient bedroom. All nurse call devices for the psychiatric unit will be made of tamperproof materials or constructed using tamperproof methods.

System Technical Description: The NC system consists of: Ethernet switches; NC server; electronic white boards; radio paging server; vital touch NCTV Annunciator / NCAV master station; NC logging workstation; NC maintenance workstations; and NC main/code blue annunciator.

System Dependency: System connectivity will be managed and is described as having only a few very well defined data exchanges in fixed formats. Patient nurse calls will be monitored at nurse team centers located within each respective hospital department. Upon activation of an emergency call, the annunciator panel visually and audibly displays the type of call, point of origination, and the patient that initiated the nurse call; in addition the corresponding room and zone dome lights provide visual and audible alerts to enable nurse personnel in that department to rapidly locate the patient. The nurse call remains active until assigned nursing staff initiates a manual acknowledgement. In the event that no acknowledgement has been initiated after a predetermined period of time, the nurse call system forwards the emergency call to a secondary annunciator panel that summons assigned secondary personnel to respond and provide acknowledgement. Staff assignments can be entered at the master stations that will be located at the department nurse team center and department head nurse’s office. Assignment will be password protected allowing only authorized staff to change the staffing assignments. When the code blue nurse call is activated, the nurse call system summons assigned hospital staff to that

patient via the nurse call radio paging system and sends an alphanumeric message to assigned staffs pagers. If the code blue emergency call is not acknowledged over a set period of time, the nurse call system forwards the nurse call to secondary assigned personnel.
System Interface: The NC system will interface with the hospital's patient information database through the Hospital Information System (HIS) network to display patient and caregiver information. This information will be available at the master stations as well as whiteboards located at the department's main nurse's team center. Patient information will be displayed using a variety of graphic symbols and icons. Patient information can also be inserted through the master stations. Coordination will take part with the hospital user representatives to coordinate graphical symbols, icons and the format that the information is displayed.
Accreditation Status: None.
See attachments #.

- ATT028 1.6.3A_NC HW-SW List
- ATT029 1.6.3B_NC Block Diagram Layout
- ATT030 1.6.3C_NC Ports and Protocols List

2. APPLICABLE DOCUMENTS. The most current version of the following documents shall be used.

(As part of the response to this Sample Task Order, the Offeror may consider and list additional references that could also be appropriate for this Sample Task Order.)

2.1 Army Regulation (AR) 25-1, Army Information Technology. https://armypubs.army.mil/

2.2 AR 25-1, Army in Europe Supplement 1 - Army Information Technology. https://media.defense.gov/

2.3 AR 25-2, Information Assurance - Rapid Action Revision (RAR). https://armypubs.army.mil/

2.4 AR 25-13, Army Telecommunications and Unified Capabilities. https://armypubs.army.mil/

2.5 AR 190-13, The Army Physical Security Program. https://armypubs.army.mil/

2.6 AR 190-51, Security of unclassified Army Property (Sensitive and Non-sensitive). https://armypubs.army.mil/

2.7 AR 380-5, Department of the Army (DA) Information

Security Program. https://armypubs.army.mil/

2.8 AR 380-27, Control of Compromising Emanations. https://armypubs.army.mil/

2.9 AR 380-53, Information Systems Security Monitoring. https://armypubs.army.mil/

2.10 AR 380-67, Personnel Security Program. https://armypubs.army.mil/

2.11 AR 381-12, Threat Awareness and Reporting Program. https://armypubs.army.mil/

2.12 AR 525-13, Antiterrorism. https://armypubs.army.mil/

2.13 AR 530-1, Operations Security. https://armypubs.army.mil/

2.14 All Army Activities (ALARACTS), https://www.us.army.mil/suite/page/550282

2.15 Army Cybersecurity Best Business Practices https://www.milsuite.mil/wiki/Portal:Army_Cybersecurity/Best_Business_Practices

2.16 Army Directive 2014-05, Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors. https://armypubs.army.mil/

2.17 Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance, Version 2.0. http://www.afcea.org/education/courses/archfwk2.pdf

2.18 Department of Defense Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB). http://www.esd.whs.mil/

2.19 DoDI 8100.04, DoD Unified Capabilities. http://www.esd.whs.mil/

2.20 DoD Directive 8140.01, Cyberspace Workforce Management. http://www.esd.whs.mil/

2.21 DoDI 8500.01, Cybersecurity. http://www.esd.whs.mil/

2.22 DoDI 8510.01, Risk Management Framework (RMF) for

DoD Information Technology (IT). http://www.esd.whs.mil/

2.23 Department of Defense Directive 8570.01-M, Information Assurance Workforce Improvement Program. http://www.esd.whs.mil/

2.24 Department of Defense Unified Capabilities Requirements 2013 (UCR 2013) . https://disa.mil/

2.25 Defense Health Agency (DHA) Directives and Guidelines, https://www.health.mil/

2.26 Defense Information Systems Agency (DISA) STIGs, http://iase.disa.mil/stigs

2.27 Risk Management Framework (RMF) Knowledge Service, https://rmfks.osd.mil/

2.28 Federal Information Processing Standard (FIPS) Module Validation Lists, http://csrc.nist.gov/

2.29 Health Insurance Portability and Accountability Act (HIPAA), http://www.hhs.gov/ocr/privacy/

2.30 National Institute of Standards and Technology (NIST) Pubs (drafts included); FIPS Pubs (drafts included); Special Pubs; IRs. http://csrc.nist.gov/

2.31 NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. https://csrc.nist.gov/

2.32 The Federal Risk and Authorization Management Program, https://www.fedramp.gov/

2.33 Public Law 93-579, Privacy Act of 1974 (Section 552a of title 5, United States Code). http://www.justice.gov/opcl/privstat.htm

2.34 Public Law 100-235, Computer Security Act of 1987 (Section 278g-3 of title 15, United States Code). https://www.csp.noaa.gov/policies/csa-1987.htm

2.35 OMB Circular A-130, Management of Federal Information Resources, Transmittal 4, 28 November 2000. http://www.whitehouse.gov/omb/

2.36 U.S. Food and Drug Administration (FDA) Directives and

Guidelines, http://www.fda.gov/MedicalDevices/default.htm

2.37 Cyber Security Reference Architecture (CSRA), https://www.milsuite.mil/wiki/DoD_Cybersecurity_Reference_Architecture

2.38 Army Directive 2014-05, Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors, http://www.apd.army.mil.

2.39 USAISEC Cybersecurity Assessment and Security Engineering Manual

3. REQUIREMENTS.

(The Offeror shall utilize the "plain text" *portion of this Sample Task as the basis for developing the cost proposal for this Sample Task. The Offeror shall utilize the italics portion of this Sample Task as directions for the writing of a description of their technical approaches for developing the required products or completing the tasks. There will be no actual performance or deliverables required on this sample task. For details and information not provided the Offeror shall state assumptions.)*

(Describe your approach to support the USAISEC Cybersecurity tasks and deliverables in support of the MILCON effort for the Replacement EACH and 3 identified medical systems in this Sample Task Order. Include in your approach discussion of team composition (e.g., number of personnel and required skill sets), what steps will be taken to ensure that quality control standards are met, and what will be done to overcome risks to schedule and cost. As part of the response, the Offeror may consider and list additional contract data requirement list (CDRL) that could also be appropriate. The Offeror shall perform the role of the Security Engineer (SE) in the below sections.)

Cybersecurity Consultation. Provide technical insight and regulatory guidance in the areas of: Security engineering; Cybersecurity requirements; Planning, oversight, and execution of the DoD RMF processes. Participate in weekly, biweekly, and monthly meetings such as the Engineering Review Board (ERB), technical reviews, System Registration Reviews (SSR), and Integrated Product Team meetings (IPT). A Weekly Project Report CDRL SE001 (ATT031) and Monthly Contractor's Progress, Status, and Management Report CDRL A001 (ATT011) will be required for all section 3 tasks. Historically, this task has been performed by one Senior Security Engineer (SSE) for one year.

Note: For the purpose of this sample task the following 3.0 subtasks are to be performed by the offeror 1 time.

3.1 **Security Engineering.** Perform information systems security

engineering to identify and integrate required security characteristics, requirements, and Cybersecurity processes into the performance objectives and functional capabilities of the Replacement EACH network. Assist vendors, developers, and system owner in preparing systems and organizational Cybersecurity processes for the transition/cutover to the Replacement EACH and for its assessment and authorization.

3.1.1 **Security Engineering Assessments.** Perform comprehensive Security Engineering Assessment (SEA) for the Replacement EACH network. The SEA will identify and quantify risk elements to the assigned project and their potential impact. This will include: a) Identifying, quantifying, and prioritizing the vulnerabilities; b) Identifying the techniques, policies, and procedures that need updating in order to increase the likelihood of a successful RMF authorization. The end result will be to determine if security controls are or will be implemented correctly, operate as intended, and produce the desired outcome. This effort requires the SE to work independently however the SE shall work alongside Government and vendor stakeholders at the site when required. This task includes the following CDRLs:

- Pre Deployment Meeting Checklist, CDRL SE003 (ATT032)
- Test Readiness Review Questionnaire, CDRL SE004 (ATT033)
- In-Brief, CDRL SE005 (ATT034)
- Daily Project Report, CDRL SE006 (ATT035)
- Out-Brief, CDRL SE007 (ATT036)
- Post-Deployment Meeting Checklist, CDRL SE008 (ATT037)
- Data/Collection Archive Folder Structure (DCAFS), CDRL SE009 (ATT038)
- eMASS upload/download, CDRL SE011 (ATT039)
- Test Data, CDRL SE012 (ATT040)
- Data Analysis Work Products, CDRL SE013 (ATT041)
- IAVA Compliance Report, CDRL SE014 (ATT042)

- STIG Compliance Report, CDRL SE015 (ATT043)
- Security Engineering Assessment Report (SEAR), CDRL SE016 (ATT044)

3.1.2 **Security Engineering Implementation and Compliance Checking of Cybersecurity Requirements.** Provide Security Engineering implementation assistance and Compliance Checking with the Replacement EACH's network. The purpose is to have the Replacement EACH achieve security control compliance. Security Engineering Implementation and Compliance Checking will be conducted at the System Owner (SO) location. This effort requires the SE to work independently however the SE shall work alongside Government and vendor stakeholders at the site when required. This task includes the following CDRLs:

- eMASS upload/download, CDRL SE011 (ATT039)
- IAVA Compliance Report, CDRL SE014 (ATT042)
- STIG Compliance Report, CDRL SE015 (ATT043)
- Documentation Evaluation Report, CDRL SE017 (ATT045)
- Plan of Action & Milestones (POA&M), CDRL SE018 (ATT046)
- Executive Summary, CDRL SE019 (ATT047)

3.1.3 **Cybersecurity Documentation and Artifacts.** Ensure all Cybersecurity documentation and artifacts will be representative of the Replacement EACH. Develop or update all required Cybersecurity documentation and artifacts for the transition to the Replacement EACH. Historically, ISEC has found that 75% of MTF Cybersecurity Documentation/Artifacts were in a poor or outdated state. The remaining 25% were non-existent. Any existing Cybersecurity documentation and artifacts of the current EACH will be located in eMASS. If no eMASS entry exists, any available Cybersecurity documentation and artifacts will be provided by the Technical Monitor (TM), system owner, or the vendor of the Replacement EACH facility's IT. This effort requires the SE to work independently however the SE shall work alongside Government and vendor stakeholders at the site when required.

- Documentation Evaluation Report, CDRL SE017 (ATT045)

3.1.4 **RMF Self-Assessment.** Perform the RMF Self-Assessment in conjunction with the SO of the Replacement EACH. The RMF self-assessment process will follow the rules/guidance of the appropriate department, service and command. In general the steps will be to select, implement, and document security controls. This effort requires the SE to function independently and interact/work alongside Government and vendor stakeholders at the site when required. Historically ISEC has found that 50% of the RMF Self-Assessment needed to be performed in-tandem with the SO while the remaining 50% only needed to be confirmed as being completed by the SO.

- Data/Collection Archive Folder Structure (DCAFS), CDRL SE009 (ATT038)
- eMASS upload/download, CDRL SE011 (ATT039)
- Test Data, CDRL SE012 (ATT040)
- Data Analysis Work Products, CDRL SE013 (ATT041)
- Documentation Evaluation Report, CDRL SE017 (ATT045)

3.1.5 **eMASS.** Perform eMASS functions ranging from creating, maintaining or updating RMF artifacts such as the POA&M. This task includes working in-tandem with designated MTF Cybersecurity Staff or performing the ISO/PM role. For this sample task the offeror will perform all eMASS functions that are needed for the subtasks under 3.1 to be completed. This task includes the following CDRLs:

- POA&M, CDRL SE018 (ATT046)

3.2 **Security Control Assessor – Validator (SCA-V) Security Control Assessment (SCA).** Perform Security Control assessments (SCAs) for type accreditation of the 3 systems identified in this sample task (ESS, ITV, & NC). The SCAs will consist of all applicable security controls and Control Correlation Identifiers (CCI) using the appropriate RMF regulations, directives, and instructions as they apply to the system(s) accreditation boundary.

The following are the minimum record requirements that are assumed as being met prior to the start of the sample task SCAs:

- System Registration has been completed IAW the service command's Assess and Authorize (A&A) Tactics, Techniques, and Procedures (TTP) or appropriate DoD

component equivalent.
- The appropriate control overlays have been correctly applied.
- All assessment procedures have at least one test result.
- All security controls have been submitted to step 2 of the Control Approval Chain (CAC).
- All applicable STIGs, as determined by the SCA-V, are applied to system components and Assured Compliance Assessment Solution (ACAS) vulnerability scans are uploaded to the artifacts section in eMASS.
- The appropriate SCA-V group is added to the second role of the CAC.
- Security categorization and National Security System (NSS) designation is in accordance with the A&A TTP and approved by the Authoring Official (AO) with supporting evidence uploaded to the artifacts section in eMASS.
- All system documentation relevant to the security assessment is uploaded into the artifacts section and linked to appropriate controls within eMASS.
- Defense Information System Network (DISN) connected systems – System is registered in the PPSM registry. https://pnp.cert.smil.mil/pnp/
- Classified systems – Applicable Security Classification Guides (SCG) have been uploaded as artifacts or DISA SCGs are referenced.

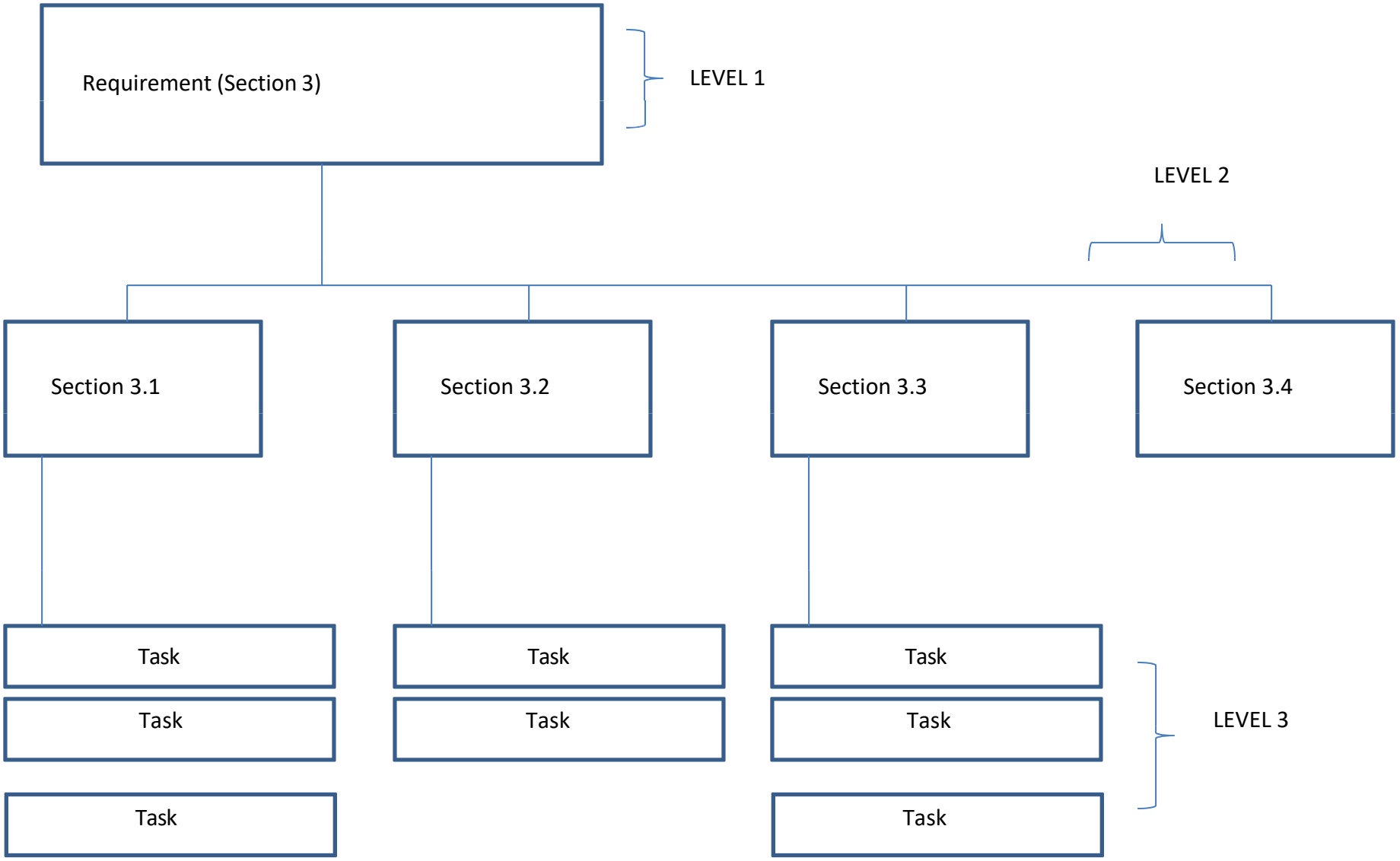
The SCAs include the following CDRLs:

- Pre Deployment Meeting Checklist, CDRL SE003 (ATT032)
- Test Readiness Review Questionnaire, CDRL SE004 (ATT033)
- In-Brief, CDRL SE005 (ATT034)
- Daily Project Report, CDRL SE006 (ATT035)
- Out-Brief, CDRL SE007 (ATT036)
- Post-Deployment Meeting Checklist, CDRL SE008 (ATT037)
- Data/Collection Archive Folder Structure (DCAFS), CDRL SE009 (ATT038)
- eMASS upload/download, CDRL SE011 (ATT039)

- Test Data, CDRL SE012 (ATT040)
- Data Analysis Work Products, CDRL SE013 (ATT041)
- Risk Calculator, CDRL SE021 (ATT048)
- Security Control Assessment Report (SCAR), CDRL SE022 (ATT049)
- SCA-V Recommendation Memorandum, CDRL SE023 (ATT050)

End of Sample Task #1

Work Breakdown Structure – This sample illustrates a notional 3-level work breakdown structure.



Work Breakdown Structure – This sample illustrates a notional 3-level work breakdown structure.