

**PERFORMANCE WORK STATEMENT (PWS)** **FOR**

**SPECIAL MISSIONS INFORMATION TECHNOLOGY SUPPORT**

**18 AUGUST 2021**

**AMENDED 29 SEPT 2021**

**AIR FORCE MATERIEL COMMAND (AFMC) OGDEN AIR LOGISTICS COMPLEX (OO-ALC) 75TH AIR BASE WING (75 ABW)**

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

**Table of Contents**

1. [DESCRIPTION OF SERVICES 1](#_bookmark0)
   1. [Scope of Work 1](#_bookmark1)
   2. [Program Management 2](#_bookmark2)
   3. [Special Requirements 4](#_bookmark3)
      1. [Controlled Area 4](#_bookmark4)
      2. [Meetings 4](#_bookmark5)
      3. [Travel 5](#_bookmark6)
      4. [Reports 5](#_bookmark7)
      5. [Transportation 6](#_bookmark10)
      6. [Data Call 6](#_bookmark11)
   4. [Personnel Qualifications 6](#_bookmark12)
   5. [Information Assurance and Protection 9](#_bookmark15)
      1. [Cybersecurity 9](#_bookmark16)
      2. [Risk Management Framework 9](#_bookmark17)
      3. [Data & Systems Protection 11](#_bookmark18)
   6. [Configuration & Change Management 13](#_bookmark19)
   7. [Enterprise Script Developer 13](#_bookmark20)
   8. [Oracle Database Administrator 15](#_bookmark21)
   9. [MS SQL Database Administrator 16](#_bookmark22)
   10. [System Administration / Server Support 18](#_bookmark23)
       1. [Hosting Services / System Analyst 19](#_bookmark24)
       2. [Administrative Services 21](#_bookmark25)
   11. [Software Development 23](#_bookmark26)
   12. [Depot Cost and Schedule Tool (DCAST) Design / Development and Sustainment 24](#_bookmark27)
   13. [DevSecOps Engineer 27](#_bookmark28)
   14. [Windows Software Testing Support 28](#_bookmark29)
   15. [BMC Remedy Subject Matter Expert 28](#_bookmark30)
   16. [Task Order Roles Summary 30](#_bookmark31)
2. [SERVICE SUMMARY (SS) 31](#_bookmark33)
   1. [Government Quality Assurance 31](#_bookmark34)
   2. [Performance Evaluation 31](#_bookmark35)
   3. [Service Summary Table 31](#_bookmark36)
   4. [Quality Control 32](#_bookmark38)
      1. [Quality Control Plan 32](#_bookmark39)
      2. [Quality Assurance 33](#_bookmark40)
      3. [Contracting Officer Representative (COR) 33](#_bookmark41)
3. [Use of GOVERNMENT Property, equipment, materials and software 33](#_bookmark42)
   1. [General 33](#_bookmark43)
   2. [Equipment Inventory 33](#_bookmark44)
   3. [Government Furnished Facilities 34](#_bookmark45)
   4. [Government Furnished Information 34](#_bookmark46)
   5. [Data rights 34](#_bookmark47)
   6. [Data rights and non-commercial computer software 34](#_bookmark48)
   7. [Utilities 35](#_bookmark49)
   8. [Contractor Representation and Presentation 35](#_bookmark50)
   9. [Telephone Service 35](#_bookmark51)
   10. [Custodial Service 35](#_bookmark52)
   11. [Refuse Collection 36](#_bookmark53)
   12. [Base Civil Engineering 36](#_bookmark54)
   13. [Security Forces 36](#_bookmark55)
   14. [Postal Service 36](#_bookmark56)
4. [GENERAL INFORMATION 36](#_bookmark57)
   1. [Common Access Card (CAC) 36](#_bookmark58)
   2. [Restricted Area Badges and Access to Controlled Areas 37](#_bookmark59)
   3. [Access to the Network 37](#_bookmark60)
   4. [Computer Connectivity 37](#_bookmark61)
   5. [Virtual Private Network (VPN) 37](#_bookmark62)
   6. [Foreign Object Damage (FOD) and Drop Object Prevention (DOP) 37](#_bookmark63)
   7. [General Contract Information 38](#_bookmark64)
   8. [Contractor Program Manager (CPM) 38](#_bookmark65)
   9. [Contractor Employees 38](#_bookmark66)
   10. [Security Requirements 39](#_bookmark67)
   11. [Security Clearance Investigations 39](#_bookmark68)
   12. [Non-Disclosure 39](#_bookmark69)
   13. [Telecommuting 40](#_bookmark70)
   14. [Freedom of Information Act (FOIA) / Privacy Act 40](#_bookmark71)
   15. [Physical Security 41](#_bookmark72)
   16. [Key Control Methods 41](#_bookmark73)
       1. [Key loss / Duplication 41](#_bookmark74)
       2. [Replacement 41](#_bookmark75)
       3. [Key Control 41](#_bookmark76)
   17. [Hours of Operation 42](#_bookmark77)
       1. [Normal Hours of Operation 42](#_bookmark78)
       2. [Recognized Holidays 42](#_bookmark79)
       3. [Emergency Situations 42](#_bookmark80)
       4. [Contingency Services 42](#_bookmark81)
   18. [Records 42](#_bookmark82)
   19. [Government Observations 43](#_bookmark83)
   20. [Training 43](#_bookmark84)
   21. [Information Assurance 43](#_bookmark85)
   22. [Continuing Education, Training, and certification 43](#_bookmark86)
   23. [Government Provided Training 43](#_bookmark87)
   24. [Fulfilling Mission Requirements 44](#_bookmark88)
   25. [Publications 44](#_bookmark89)
   26. [Internal Operating Procedures 44](#_bookmark90)
   27. [Conservation of Utilities 44](#_bookmark91)
   28. [Environmental Protection and Safety 45](#_bookmark92)
   29. [Environmental Controls 45](#_bookmark93)
       1. [Compliance with Laws and Regulations 45](#_bookmark94)
       2. [Notification of Environmental Spills 45](#_bookmark95)
       3. [Material Storage and Use 45](#_bookmark96)
       4. [Participation in Government Activities 45](#_bookmark97)
   30. [Transition Period 46](#_bookmark98)
   31. [Phase-out Period 46](#_bookmark99)
   32. [System for Award Management (SAM) Reporting Requirement 47](#_bookmark100)
   33. [Section 508 of the Rehabilitation Act 47](#_bookmark101)

[Appendix A. GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 1](#_bookmark102)

[Appendix B. GLOSSARY OF ACRONYMS 5](#_bookmark103)

[Appendix C. SAFETY REQUIREMENTS 13](#_bookmark104)

[Appendix D. REQUIRED FILES/DOCUMENTATION FOR SERVER ADMINISTRATION](#_bookmark105) [AND SOFTWARE/WEB DEVELOPMENT 16](#_bookmark105)

[Appendix E. GOVERNMENT FURNISHED EQUIPMENT (GFE) 17](#_bookmark106)

**Table of Figures**

[Figure 1-1 — DoD 8570.01-M Fig. C2.F1 Overview of Basic IA Workforce Structure 7](#_bookmark13)

**Table of Tables**

[Table 1-1 — Approved Baseline Certifications 8](#_bookmark14)

[Table 1-2 — Task Orders, Programs, & Baseline Certification Matrix 30](#_bookmark32)

[Table 2-1 — Service Summary Table 31](#_bookmark37)

# DESCRIPTION OF SERVICES

The Contractor shall provide all contract administration, contract management, personnel, tools, equipment, material, vehicles, transportation, consumable supplies, operation and maintenance necessary to perform Information Technology (IT) System Administration, Software Development, Web Based Application Development, Enterprise Script Writing, System Analyst, Database Administration, BMC Remedy products and Software testing for multiple Air Force (AF) IT systems in accordance with (IAW) this Performance Work Statement (PWS) and the Government regulations identified in [Appendix A.](#_bookmark102) The Contractor shall provide recommended solutions for technical issues associated with this PWS. The Contractor shall perform to the standards, workload estimates, and the degree of ability, knowledge, skills and timeliness required in the PWS. The Contractor shall be knowledgeable of developing technologies, including information security and Cloud services, and shall be expected to have the technical expertise to transition into new operating environments. The Contractor shall provide all Contractor personnel, supervision, and management necessary to perform the services as defined in this PWS. The Contractor shall have a physical office set up within 50 miles of Hill AFB, Utah.

## SCOPE OF WORK

Hill Air Force Base (AFB) is an Air Force Materiel Command (AFMC) base located in Northern Utah and is home to many operational and support missions, with the 75th Air Base Wing (75 ABW) serving as the host organization. The center provides worldwide engineering and logistics management for the F-35, F-16 Fighting Falcon, A-10 Thunderbolt II, Minuteman III intercontinental ballistic missile, and Space and C3I system program offices. The base performs depot maintenance on the F-16, A-10 and C-130 Hercules aircraft. Unless otherwise noted all services apply to "Team Hill" including but not limited to the OO-ALC, 75th Air Base Wing (75 ABW), and all their subordinate organizations, including associate units.

This requirement is to obtain System Administration, Desktop Engineering, Network and Server support, Contractor Program Management, Content and Configuration Management, Software Development, BMC Remedy Administration and Development, Oracle Architecture Database support, Structured Query Language (SQL) Database Administration/Development support, and IT software testing support.

Contractor personnel shall comply with Privacy Act of 1974, 5 U.S.C. § 552a, and all system requirements and Government Directives, Instructions and Regulations. The Contractor shall be required to perform activities including the collection, use and dissemination of records which contain personally identifiable information (PII) protected by the Privacy Act. Therefore, the Contractor shall ensure that all work is performed in strict compliance with the Privacy Act and all related laws and regulations. The Contractor shall provide, report, and obtain assistance for correction and/or resolution of IT system problems. The Contractor shall make equipment network-ready with the Federal Standard Desktop Configuration (FSDC) and all applicable application software packages required for the owning organization. The Contractor shall remain abreast and certified in new technologies. The Contractor shall train as specified in DoD 8570.01-M, per PWS para. [1.4](#_bookmark12) or its replacement. The Contractor shall report network intrusions, viruses, malicious logic, network attacks, and scheduled outages through the 75th Communications and Information Directorate (75 ABW/SC) Help Desk 24/7/365 at 586-8324 and the Task Order Program Manager (TOPM).

The Contractor will be required to work on the following systems (not all-inclusive):

* Execution and Prioritization of Repair Support System (EXPRESS)
* Depot Cost and Schedule Tool (DCAST) system
* BMC Remedy at Hill AFB, Tinker AFB, OK, and Robins AFB, GA
* Part Number Supply Support Request System (PNSSRS)
* Depot Maintenance Accounting and Production System (DMAPS)
* Process Order Development and Deployment System (PODDS)
* Emergency Management Command and Control (EMC2) System
* Industrial Product Support Vendor/Point of Use (IPV/POU)

The following applications (not all-inclusive) are in sustainment and may require upgrades/rewrite/maintenance:

* AMXG & CMXG Equipment database
* Form 957
* Request for Personnel Action (RPA)
* Post Office/Official Mail Center (OMC) database
* IHS Standards Database Services (IHS)
* ShoeTag
* TrueChem

Upon award of this requirement, the Contractor shall have 30 days, or such time as may otherwise be agreed upon in writing by the Government, to be fully prepared to perform the requirement.

## PROGRAM MANAGEMENT

Program Management is a mandatory element of the requirement. The objective of Contractor Program Management is to provide the project control and contract administration necessary to manage a high volume, multiple task processes for a large, diversified team so that the cost, schedule and quality requirements of each task order are tracked, communicated to the Government, and ultimately attained. The Contractor shall provide real-time monitoring of status/deliverables, tracking the quality of work products and gauging overall customer satisfaction by submitting a Program Management Plan (see CDRL A/B/C010).

This is a non-personal services contract. The Contractor is solely and exclusively responsible for all matters governing and relating to the employer-employee relationship between the Contractor and the person(s) the Contractor hires and assigns to perform the work described herein. The Contractor shall provide a written Personnel Management Plan used in the performance of the requirements as stated in this PWS (see CDRL A/B/C006).

The Personnel Management Plan shall describe the following:

* hiring and recruitment processes
* employee retention and turnover
* employee performance plan or policy
* the employee termination process
* employee replacement and operational continuity
* leave plans and policies relating to scheduled leave, unscheduled leave, employees leaving employment, or emergency coverage of employees experiencing long-term illness
* contingencies for natural disasters and public health conditions
* organizational structure
* employee cross-utilization or cross-training approach
* obtaining security clearances
* maintaining commercial certifications, including an education and training program for evolving technologies, information security, Cloud services, and best practices such as but not limited to Information Technology Infrastructure Library (ITIL), secure coding, test driven development (TDD), code quality, and agile software development

The Contractor shall address in detail their management of customer expectations, reporting metrics and lines of communications within the Contractor’s own team. The Contractor shall submit the plan at the post-award conference.

All changes to personnel and management assigned to the contract shall be reported in writing or via email to the Contracting Officer Representative (COR) and Government Task Order Program Manager (TOPM) within three (3) business days. The Contractor shall provide current and approved files for all hard copy and electronic files associated with the Server Administration and Software/Web Development (see CDRL A/B/C011). A list of such files, though not exhaustive, is included in [Appendix D.](#_bookmark105) The Contractor shall work with the Government TOPM to coordinate with the Records Manager for the task order to which they are assigned to make sure that this information is recorded and stored.

The Contractor shall ensure all employees possess required training, qualifications, certifications, proficiency, and security clearances and satisfy all other access requirements IAW DoD 8570.01-M prior to start of work (see CDRL A/B/C008). Proof of the 8570 certifications shall be presented to the COR at beginning of contract or when beginning employment (see CDRL A/B/C007). Contractor employees shall not begin work until 8570 certified and the COR is presented with a copy of the certificate. An 8570 Certification Plan will be submitted at time of contract proposal to address how the Contractor will manage Contractor personnel affected by DoD 8570 certification/training requirements (see CDRL A/B/C008). The plan shall describe how the Contractor intents to train and obtain certifications, track the certifications, track expiration of certifications/renewal and continuing education (CE). The 8570 training/certification will not be paid for by the Government. (CDRL A/B/C008). This training/certification requirement shall be completed in compliance with AF processes identified in [Appendix A](#_bookmark102): Glossary of References and Supporting Information.

As part of providing services under this contract:

* The Contractor Management Staff shall demonstrate a firm Business Plan to include an organizational management structure, and reasonable business approach.
* The Contractor Management Staff shall use metrics to ensure adequate internal controls and procedures are in place to measure the AF’s contract requirements are met with satisfaction. The process shall outline methods and frequency of customer interactions, reporting processes and problem resolution procedures.
* The Contractor Management Staff shall have in place a Human Resource Management Plan to ensure qualified candidates are identified, screened, placed, monitored, and trained/retained to fulfill service requirements of this PWS.
* The Contractor Management Staff shall provide a Quality Assurance and Productivity Measurements (QAPM) plan (see CDRL A/B/C009) that demonstrate techniques for compilation and application of internal controls for workload management as it relates to acceptable output standards, quality checks and efficiencies. These systems and controls for recording and monitoring workload shall be capable of providing historical and in-process workload data segregated by CLIN shall address the areas covered by the Service Summary. The QAPM is required to the Contracting Officer’s Technical Representative (COR) at the Post-Award Conference. (see CDRL A/B/C009)
* The Contractor Management Staff shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, experience, knowledge, training, certifications, abilities and skills, as well as physical capabilities.
* The Contractor Management Staff retains employee management and supervisory responsibility because of the employee-employer relationship. This includes but is not limited to providing guidance for employees during designated Government non-workdays or other times when Government offices may be closed; initial and refresher training as required by each labor category; and administrative support (i.e., time reporting, leave processing, pay). Clear organizational authority and responsibility to effectively manage and control the Contractor personnel will be established between the employees and their employing company. This shall be accomplished without requiring Government employees to engage in the Contractor’s operational or human resource management processes. The Government will provide input as needed through the CO and COR.
* Use of Government staff members to record arrival or departure times, report absenteeism, sign payroll timesheets, or to perform any other duties inherent in the employer–employee relationship is not authorized. The Contractor shall have a process in place internally to ensure times reported for contract personnel are accurately reflected on billing invoices.
* The Contractor shall provide the name of its designated PM and any alternate(s) who shall act for the Contractor when the PM is absent. The name of the Contractor PM and any alternate(s) shall be designated in writing to the CO within ten (10) business days after contract award. The Contractor shall provide telephone numbers and email addresses for its PM and any alternate(s) where these persons may be contacted at any time. The Contractor PM and any alternate(s) shall have full authority to act for the Contractor on all matters relating to Contractor personnel and or Contractor performance under this contract. The Contractor PM and any alternate(s) must be a United States (US) citizen. Contractor shall ensure that all employees performing under this contract read, write, speak, and understand English at a technical level and proficiency adequate to the nature of the tasks assigned. The Contractor PM and any alternate(s) may be required to attend meetings, as requested by the CO. The Contractor PM and any alternate(s) shall be available during core hours within two (2) business hours to meet with Government TOPM and/or COR to discuss task order status. The Contractor shall provide points of contact, the CPM and the alternate, who are available 24 hours per day, 7 days per week in the event of situations which will require on-call services.

## SPECIAL REQUIREMENTS

## CONTROLLED AREA

All requests for access to controlled areas shall be submitted in writing to the COR within five (5) business days of required access. Requests shall contain the justification for and duration of access, including the names of specific personnel who will need to access the controlled area.

## MEETINGS

The Contractor shall assist Government personnel and provide technical representation for the Government. The Contractor shall present briefings, participate in formal and informal discussions and provide opinions to Government personnel at base staff meetings and at other functions as required for task orders. The Contractor may be required to attend meetings/conferences to discuss and evaluate efforts and progress in the accomplishment of assigned tasks and resolution of technical issues as they arise. Such meetings include Software Review Board (SRB), Technical Review Board (TRB), Change Advisory Board (CAB), discussions with Information Assurance (IA) personnel regarding information

security processes and plans, Requirements Review, Customer Requirements Elicitation, and any other meetings where the technical expertise of the Contractor may be required. Meetings will be held at Government furnished facilities, via Teams, or via other virtual means. The Contractor shall ensure that all Contractor personnel attending meetings are visibly and/or audibly identified in all meetings. The Contractor should note, the Government has the right and authority to exclude any Contractor personnel from any meeting.

## TRAVEL

The Contractor shall travel if necessary and attend technical interchange, project review meetings and conferences, both locally and across the continental United States (CONUS) to provide technical expertise and representation. Each travel request will be reviewed by the COR and submitted to the CO. The Contractor shall obtain written approval from the CO prior to making travel arrangements. Travel shall be subject to the Joint Travel Regulations and negotiated on an as needed basis when requested outside the local area.

## REPORTS

The Contractor shall provide electronic monthly status reports, monthly metrics and status based on trouble tickets and performance via email to the Government COR. (see CDRL A/B/C001)

* + - 1. **MONTHLY ACTIVITY REPORTING**

The Contractor shall provide monthly status reports that include all current efforts, completion/expiration dates, and problems, if any. (see CDRL A/B/C001)

The monthly status report shall include the following information:

* Status of work in progress: (this shall be included for each task order or project being worked)
  + Program Name
  + Software Deployment Change Request (SDCR) (file name or number)
  + Development Process status
  + Expected Completion date
  + Brief description of any problems or issues encountered during the month
  + Brief description of:
    - any system changes,
    - software upgrades/changes,
    - security upgrades/changes at the Application level,
    - updates to technical software or database repository files
  + Brief description of current status or situation regarding static code analysis
  + Brief description of any changes or updates to:
    - Software Design Document
    - Software Requirements Document
    - Software Test Plan or Software Test Procedures
    - Test Results (if in Unit or Integration Test)
    - Software Release Document or Instructions
    - User Manual or User Guide
    - Any other pertinent documentation and Configuration Items not listed
  + Hindrances encountered that may impact the project now or in the future
  + Any additional information deemed by the Contractor to be necessary to relay to the TOPM in a monthly or one-time status update
* Assistance or support provided to the TOPM regarding:
  + Creation or update of Plan of Action & Milestone (POA&M)
  + Creation or update of Software Release Transmittal Letter (SRTL)
  + Participation or support for Software Review Board (SRB)
  + Participation or support for Change Advisory Board (CAB)
* Accomplishments in support of Configuration Management policies
* Accomplishments in support of Risk Management Framework (RMF)
* Accomplishments in support of and compliance with Cybersecurity
* Hindrances encountered that are impacting or may impact the compliance with Configuration Management policies, RMF, or Cybersecurity

The TOPM may request additional information that does not apply to a recurring monthly status report. The TOPM will relay this request to the COR to be included in the overall status report request. (see CDRL A/B/C001)

* + - 1. **WEEKLY ACTIVITY REPORTING**

The Contractor shall provide weekly status reports that include all current efforts, completion/expiration dates, problems, if any for each Task Order. (see CDRL A/B/C003)

The weekly activity report shall include:

* Name/date/branch
* Status on current projects:
* Roadblocks
* Milestones
* Concerns/Needs

## TRANSPORTATION

The Contractor shall provide Contractor-owned or personal transportation for Contractor employees in performance of this PWS. There may be times when the Contractor will need to attend meetings in another building. The Contractor shall comply with all federal regulations and policies while driving on base**,** IAW AFMAN 31-116\_HILLAFBSUP, *Air Force Motor Vehicle Traffic Supervision*.

## DATA CALL

The Contractor shall respond to Government ad hoc requests for data/information in the specified time per task order requirements. If a delay is encountered and the Contractor cannot respond in the specified time, the Contractor shall inform the Government of their inability to provide the information and propose a new projected date/time for CO approval.

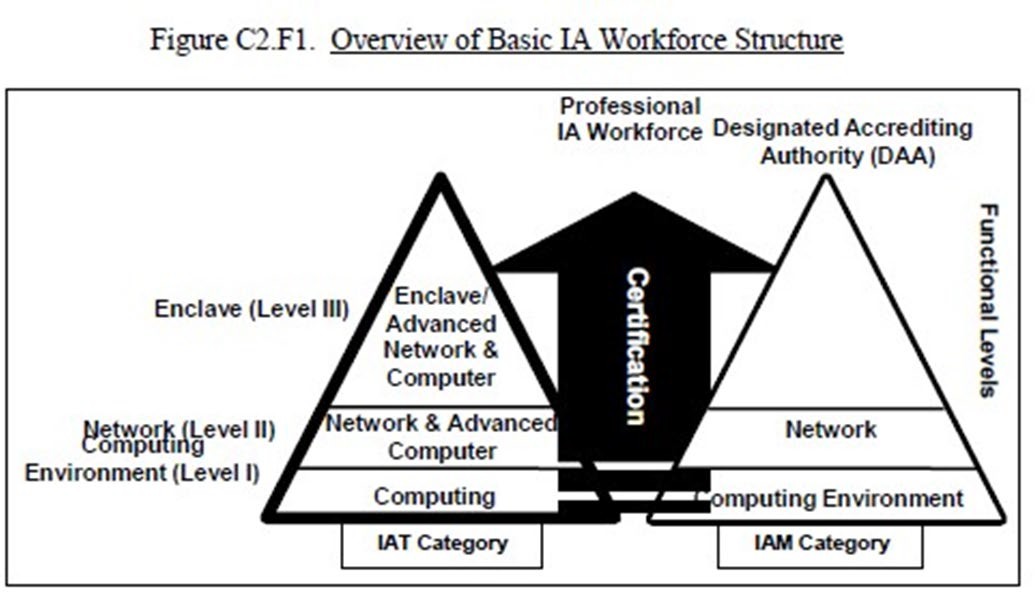
## PERSONNEL QUALIFICATIONS

The Contractor shall provide personnel who can understand, read, write and clearly speak the English language and communicate with and assist base personnel within the scope of the PWS. All Contractor personnel shall be courteous, observing military and business professional etiquette and present a neat, clean, and professional appearance. All Contractor personnel shall be knowledgeable and able to effectively communicate problem resolutions to and for customers. All Contractor personnel shall be qualified and maintain certifications as listed throughout this PWS and required per DoD 8570.01,

identified in PWS para. [1.1,](#_bookmark1) at time of contract award and throughout the duration of the contract (see CDRL A/B/C007 & A/B/C008). See DoD 8570.01-M, Chapter 2, Figure C2.F1 for the Overview of Basic Information Assurance (IA) Workforce Structure.

IA certification programs are intended to produce IA personnel with a baseline understanding of the fundamental IA principles and practices related to the functions of their assigned position. Each category, specialty, and skill level have specific training and certification requirements. Meeting these requirements will require a combination of formal training and experiential activities such as on-the-job training and continuing education. These training and certification requirements shall be provided to employees at no cost to the government.

Contractor personnel, both existing and future, providing service under the basic contract shall be required to currently have the DoD 8570.01-M certification requirements per AFMAN 17-1303 at time of contract award and throughout the duration of the contract. The Contractor’s workforce, including subcontractors, shall maintain compliance with the cybersecurity Contractor training and certification requirements in DoD Directive (DoDD) 8570.01 and DoD 8570.01-M and meet the investigative level requirements established in Enclosure 3 of DoDI 8500.01(See CDRL A/B/C007 & A/B/C008).



*Figure 1-1 — DoD 8570.01-M Fig. C2.F1 Overview of Basic IA Workforce Structure*

*Table 1-1 — Approved Baseline Certifications*

|  |  |  |
| --- | --- | --- |
| APPROVED BASELINE CERTIFICATIONS | | |
| **IAT Level 1** | **IAT Level II** | **IAT Level III** |
| A+ CE | CCNA Security | CASP+ CE |
| CCNA-Security | CySA+ | CCNP Security |
| CND | GICSP | CISA |
| Network+ CE | GSEC | CISSP (or Associate) |
| SSCP | Security+ CE | GCED |
|  | CND | GCIH |
|  | SSCP |  |
| **IAM Level 1** | **IAM Level II** | **IAM Level III** |
| CAP | CAP | CISM |
| CND | CASP+ CE | CISSP (or Associate) |
| Cloud+ | CISM | GSLC |
| GSLC | CISSP (or Associate) | CCISO |
| Security+ CE | GSLC |  |
|  | CCISO |  |
| **IASAE I** | **IASAE II** | **IASAE III** |
| CASP+ CE  CISSP (or Associate) CSSLP | CASP+ CE  CISSP (or Associate) CSSLP | CISSP-ISSAP CISSP-ISSEP |
| **CSSP Analyst** | **CSSP Infrastructure Support** | **CSSP Incident Responder** |
| CEH | CEH | CEH |
| CFR | CySA+ | CFR |
| CCNA Cyber Ops | GICSP | CCNA Cyber Ops |
| CCNA-Security | SSCP | CCNA-Security |
| CySA+ | CHFI | CHFI |
| GCIA | CFR | CySA+ |
| GCIH | Cloud+ | GCFA |
| GICSP | CND | GCIH |
| Cloud+ |  | SCYBER |
| SCYBER |  |  |
| **CSSP Auditor** | **CSSP Manager** |  |
| CEH | CISM |  |
| CySA+ | CISSP-ISSMP |
| CISA | CCISO |
| GSNA |  |
| CFR |  |
| <https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/> | | |
| **NOTE:**  An individual needs to obtain only one of the “approved certifications”; for his or her IA category or specialty and level to meet the minimum requirement. For example, an individual in an IAT Level II position could obtain any one of the four certifications listed in the IAT Level II cell.  Higher level IAT and IAM certifications satisfy lower-level requirements. Certifications listed in Level II or III cells can be used to qualify for Level I. However, Level I certifications cannot be used for Level II or III unless the certification is also listed in the Level II or III cell.  Higher level CSSP and IASAE certifications do not satisfy lower-level requirements | | |

## INFORMATION ASSURANCE AND PROTECTION

The Contractor shall provide Information Assurance (IA) and protection to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems (IS), and provide for restoration through incorporation of protection, detection, and reaction capabilities.

Information System security requirements are defined by regulation and policy in the most current versions of AFPD 17-1, AFI 17-101, and AFI 17-130 identified in [Appendix A.](#_bookmark102) The Contractor shall use Enterprise Systems Management (ESM), Systems Management Server (SMS) or other Government- specified software to manage the computing environment. Desktop systems shall be continually updated with the latest approved software and security patches, provided by the Government, to minimize security vulnerabilities. Information systems, desktops and supported peripherals shall be certified and accredited to comply with the DoD system security policies before they can be added to the network IAW DoDI 8510.01 identified in [Appendix A.](#_bookmark102) Protection shall be accomplished with time-sensitive procedural countermeasures and Government-issued technical advisories. Information systems and data shall be protected against tampering using Government-approved and provided anti-virus software. The Contractor shall ensure that the standard methodology for installation, operation, maintenance, update, and/or patching of software does not alter the secure configuration settings from the approved configuration.

## CYBERSECURITY

Per DoDI 8500.01, cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Cybersecurity applies to all DoD Information Technology (IT) that receives, processes, stores, displays, or transmits DoD information.

Cybersecurity measures must be taken to protect AF information and IT from criminal or unauthorized use. Suspected vulnerabilities and security incidents shall be reported IAW AFI 17-130 identified in [Appendix A.](#_bookmark102) Activity logs shall be audited, retained, and documented for review. These logs shall be protected by both Government and Contractor employees. Suspect activity shall be monitored, identified and reported immediately to the 75 Communications and Information Directorate (75 ABW/SC) Help Desk 24/7/365 at 586-8324, the Task Order Program Manager, and the 75 ABW/SC Cybersecurity office IAW OPR 75 ABW/SCXS, *Computer Incident Quick Response Guide* (May 2019). Access to information and resources will be strictly controlled IAW AFMAN 17-1301. The Contractor shall comply with DFARS Clause 252.204-7012 and ensure the sub-Contractor compliance.

The Contractor shall ensure all desktop hardware and software meets information systems security requirements as defined by regulation and policy in AFI 17-130, and identified in [Appendix A.](#_bookmark102) The Contractor shall protect system information and resources according to established security policies and procedures, maintain account with ESM, SMS or other Government-specified tracking system, and ensure desktop systems are updated with the latest approved software and security patches, provided by the Government, to minimize security vulnerabilities.

## RISK MANAGEMENT FRAMEWORK

The 75 ABW/SC organization, in accordance with the Air Force, is striving to make a more secure IT environment for our customers and the warfighter. We have a responsibility to secure diverse interconnected technologies, many new, and many legacy systems. In order to reach this goal, we require a broad knowledge of industry standards for securing and maintaining IT systems that are tracked and

inspected through Defense Information Systems Agency (DISA) STIGs (Security Technical Implementation Guides).

The Risk Management Framework (RMF) provides a disciplined and structured process that combines Information Systems (IS) security and risk management activities into the development lifecycle and authorizes their use within the DoD.

RMF describes the DoD process for identifying, implementing, assessing, and managing cybersecurity capabilities and services, expressed as security controls, and authorizing the operation of IS and Platform Information Technology (PIT) systems.

RMF brings a risk-based approach to the implementation of cybersecurity, supports cybersecurity integration early and throughout the system lifecycle, promotes reciprocity to the maximum extent possible, and stresses continuous monitoring. The Contractor shall ensure that the cybersecurity portions of the overall system design are included in systems engineering and design documents, test plans, procedures, and reports.

The Contractor shall be prepared to support all DoD/AF cybersecurity requirements, including but not limited to, assistance with the preparation of Assess and Authorize (A&A), Assess Only, software assessments and Authorized to Operate (ATO) packages, as well as all required documentation needed to support the RMF process, continuous monitoring, and the attainment and sustainment of the system ATO package, to include but not limited to, the System Security Plan (SSP), Security Assessment Report (SAR), Security Assessment Plan (SAP), Plan of Action and Milestones (POA&M), and Ports, Protocol and Services (PPS) (see CDRL A/B/C015 & A/B/C016). The Contractor shall ensure that information systems added to the network comply with the DoD system security policy and are properly certified and accredited in accordance with AF and DoD policy. The Contractor shall support any changes to current processes and future cybersecurity processes or practices mandated by policy or best practices. The Contractor shall implement procedural countermeasures and Government-issued technical advisories including Notices to Airmen (NOTAM), Time Compliance Network Orders (TCNO), Field Engineering Notices (FEN), System Advisory Notices, Heads Up Messages (HUM), Air Force Computer Emergency Response Team (AFCERT) notices, Time Compliance Technical Order (TCTO), Information Condition Changes (INFOCON), and service packs and security patches according to AFCERT or Automated System Security Incident Support Team (ASSIST) guidance, within the timeframe specified by the technical advisory. The notifications are distributed by the Communications Focal Point (CFP), 75 ABW/SCOSC, and 75 ABW/SCXP via email and communicated during meetings or other discussions.

The Contractor shall protect the information systems and data against tampering by loading Government- approved and provided anti-virus software to detect the presence of viruses and by maintaining current signature files. The Government will advise Contractor users on reporting and cleaning procedures if a virus is detected within the user’s system. The Contractor shall identify and report all suspect activity immediately to the Government COR and the TOPM. The Contractor shall limit access to privileged program files, utilities, and security relevant programs/data files to authorized personnel as designated by the appropriate security manager. Each user shall be provided with only those privileges needed for the user’s assigned tasks, as defined by the TOPM.

DISA is the authoritative agency that provides IT and communications support to both government and associated defense organizations. Organizations must attain and stay compliant with these guidelines, or the system risks being taken off of the DoD network.

A STIG is a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. STIGs also describe maintenance processes

such as software updates and vulnerability patching. The Contractor shall ensure there are no “Very High” or “High” levels of risk as defined by NIST SP 800-30 for Non-compliant (NC) security controls. The Contractor shall identify and resolve or mitigate all Moderate, Low, and Very Low levels of risk for NC security controls. Any level of risk which cannot be mitigated must be approved by the Government. The Contractor shall develop or assist the PM with the development of a POA&M to document residual levels of risk present in the system along with a plan to mitigate or eliminate those risks in the future, which must be approved by the Government. Any level of risk which cannot be mitigated must be approved by the Government.

STIGs are the configuration standards for DoD Cybersecurity and IA-enabled devices/systems. STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Contractors shall ensure that they follow STIG guidance to configure hardware and software properly, implement security protocols, and identify potential weaknesses in code.

Hill AFB uses tools, such as Fortify, for security scans to identify and analyze security vulnerabilities. The Contractor shall be required to run these scans and provide corrections to the vulnerabilities.

The Contractor shall provide engineering support to Government-conducted evaluation events in support of the Technical Order Validation and Verification process, the DISA Application Development STIGs, deployment validation, and RMF efforts. The Contractor shall implement the applicable cybersecurity controls through the systems engineering technical processes: stakeholder requirements definition, requirements analysis, architecture design, integration, verification and validation. The Contractor shall ensure that the cyber risk management activities are consistent with guidance provided in CNSSP No. 22 *Cybersecurity Risk Management (August 2016)* and other DoD or AF guidance.

## DATA & SYSTEMS PROTECTION

Anti-Tamper (AT) entails systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system. All Acquisition Category (ACAT) programs and weapon system developments must implement the DoD AT process to determine whether AT is required for their systems. AT must be considered for all upgrades, spiral/incremental developments, modifications, or technology insertion efforts. AT must also be considered in replacement of legacy systems, components and parts of those items containing Critical Program Information (CPI). Software Assurance (SwA) is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

The Contractor shall ensure compliance with AT and SwA per DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)* (1 Oct 2020), AFI 63-101\_20-101, *Integrated Life Cycle Management* (30 June 2020), and DoDI 4140.67, *DoD Counterfeit Prevention Policy* (6 Mar 20).

### Operations Security (OPSEC)

Reference: National Security Decision Directive (NSDD) 298 DOD 5205.02-M

DODD 5205.02E

AFI10-701AFGM\_2018-01

All Contractors, sub-Contractors, their employees, associates, and consultants who have access to Critical Information (CI) must comply with the DoD and AF-sponsored OPSEC program. The OPSEC Program is directed by NSDD 298, DoD Publications, and applicable AF guidance.

OPSEC is a systematic means of identifying and protecting information, which an adversary could use to their advantage or to our disadvantage. CI is generally unclassified but can become classified through compilation. This CI is sensitive and has been identified by the organization’s OPSEC program as requiring protection. OPSEC Measures (OM) are control standards with which all Contractor personnel must comply in order to protect CI against adversaries.

### Responsibilities:

The Security Office, 75 ABW/SC, OPSEC Program Coordinator will provide and approve OPSEC training curriculum for use by the Contractor. Critical Information and Indicator Listings (CIILs) will be protected by all Contractor personnel as “Controlled Unclassified Information (CUI). Approved organizational OPSEC measures will be used by all Contractor personnel to protect CI in their possession and protect against current foreign intelligence and industrial espionage threats. The OPSEC Program Coordinator and the Contractor must ensure all Contractor personnel working on the contract or having access to CI attend approved initial and annual recurring, refresher training. Training will be provided by the Government before Contract personnel are allowed access to or handling of CI. All Contractor personnel will comply with various AF the organizations OPSEC standards and practices as trained.

Additional training may be required based on updates to CI, OPSEC measures, intelligence threat/vulnerability, or other fundamental changes to the OPSEC program. Contractors with OPSEC requirements within a contract must ensure employees receive OPSEC training as specified within the contract. Accomplishment of OPSEC training must be completed within90 days from initial assignment to a contract with OPSEC requirements. OPSEC training will be accomplished annually via Computer Based Training (CBT). The Contractor personnel will not be given access to an organization’s CIIL until after training has been completed and documented by the Government OPSEC Coordinator.

The OPSEC Program Coordinator for the organization will track OPSEC training statistics for all Contractor and sub-Contractor personnel working on the contract, when each individual has received the required OPSEC training, and when refresher training is due. The OPSEC Program Coordinator will provide a copy of the 75 ABW OPSEC Plan to the Contractor upon request and the Contractor is subject to the requirements of that plan. The 75 ABW OPSEC Plan is “Controlled Unclassified Information (CUI)” and distribution outside the constraints of the contract in part or in its entirety is prohibited. Upon completion of the contract, the Contractor will destroy the OPSEC Plan by shredding the document so that it cannot be reconstructed and deleting any electronic copies.

Prior to seeking approval through Hill AFB Public Affairs, any information to be released outside of official U.S. Government channels, via any media, must be approved through an OPSEC review by the 75 ABW/SC Coordinator. All Contractor personnel must promptly report OPSEC related incidents, issues,

and concerns to the 75 ABW/SC Coordinator, (801) 586-0332 who will then report it to the 75 ABW Communications Focal Point (CFP), (801) 586-8008 and the TOPM.

## CONFIGURATION & CHANGE MANAGEMENT

The Contractor shall be responsible for following Configuration Management and Change Management policies instituted by 75 ABW/SC and prescribed by FIPS 200, NIST 800-53, and NIST SP 800-128.

Configuration Management ensures uniformity within the organization’s software technology and supports other Information Technology Service Management (ITSM) activities. The Contractor shall have at least an introductory understanding of ITIL practices for Configuration Management and Change Management and understanding of industry best practices on software configuration management. The Contractor shall follow the above-mentioned policies regarding source code management, Configuration Items (CIs) and other work products, and documentation and presentations in support of Requirements Review Board (RRB), Technical Review Board (TRB), Software Review Board (SRB), and Change Advisory Board (CAB). CIs include, but are not limited to, hardware and software lists, Configuration Control Directives (CCD), Software Test Description and Report (STDR), Software Release Transmittal Letter (SRTL), Test Plan and Test Procedures, Risk Management Plan, Schedules, Interface Control Document (ICD)/Interface Requirements Agreement (IRA), Release Review Checklist (RRC), Static Code Analysis (SCA) and Assured Compliance Assessment Solution (ACAS) results, system event logs, DISA Checklists, User Manuals, and Coding Standards. The Contractor shall use the prescribed Information Systems Management Tool (ISMT), currently Remedy, for tracking of work tasks, task status, and submission of Change Management and Configuration Management requests unless otherwise directed by TOPM, or 75 ABW/SC, Air Force and/or DOD policy. The Contractor shall comply with all procedures involved in system baselines, backups and restoration. The Contractor shall create or update data flow diagrams, perform data standardization, and perform enterprise modeling, functional economic analysis, simulation/modeling, activity-based costing and activity-based management support. The Contractor shall provide business process improvement support that includes all activities involved in helping improve customer data systems through business process redesign, including rethinking program design, and aligning IT infrastructures with business missions, goals, and objectives. The Contractor, with coordination with the TOPM, shall gather requirements information by developing and implementing data collection instruments. The Contractor, with coordination from the TOPM, shall conduct requirement surveys, document reviews, and interviews to gather requirements and feedback from customers. The Contractor shall provide organizational facilitation support including aiding and advising the Government in building cross-functional teams within organizations and components of organizations. The Contractor shall perform manual and automated modeling efforts, including requirements, processes, activities, and data. The Contractor shall provide prospective and potential functional analysis using statistical methods, comparative analysis, timeline analysis, cross-functional analysis, and cause and effect diagrams. The Contractor shall evaluate suitability of business process improvement tools and methodologies.

## ENTERPRISE SCRIPT DEVELOPER

The Contractor shall provide administration, testing, maintenance, and support of Enterprise Management tools software that may include Commercially Off-the-Shelf (COTS) software The Contractor shall provide expertise in Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), Extensible Markup Language (XML), JavaScript Object Notation (JSON), advanced PowerShell scripting, Asynchronous Java Script, XML (AJAX), Java Script and other COTS scripting technologies. The Contractor shall provide expertise in using various scripting languages for dynamic content generation using applicable web technologies incorporating content from external data files and databases.

The Contractor shall develop, test and integrate enterprise scripts, process automation tools and Web front-ends utilizing best industry practices. The Contractor shall perform in accordance with DoD, Air Force, and AFMC architectures, policies and standards, including the Global Combat Support Systems (GCSS) architecture. The Contractor shall use industry-standard programming and scripting languages including Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), and Structured Query Language (SQL) for creating reports.

The Contractor shall possess a strong understanding of MS Active Directory (AD) and related technologies including Group Policy Objects (GPO), Lightweight Directory Access Protocol (LDAP), managing tools rights and assigning permissions, accepted AD management and structuring techniques, and industry-standard principles of Information Assurance (IA).

The Contractor shall have a strong foundation in the Microsoft Windows operating systems including MS Windows 8 and 10, MS Server 2012 R2, 2016 and 2019 and virtual machine environments. The Contractor shall be able to develop scripts to automate and control the various IT infrastructure components across the Hill AFB enterprise.

The Contractor shall perform requirements management to include gathering and maintaining requirements traceability. The Contractor shall provide business process-improvement support that includes all activities involved in helping improve customer data systems through business processes including rethinking program design and aligning information technology infrastructures with business missions, goals, and objectives. The Contractor shall use tools and methodologies in conducting business process-improvement tasks.

The Contractor shall perform the validation and testing of scripts and interfaces to verify the system satisfies functional and operational requirements. The Contractor shall coordinate with the customer throughout the project to ensure thorough testing before any scripts/tools are migrated to the production environment. Testing is required before each product release and shall be conducted at Hill AFB. The Contractor shall coordinate preparation of test cases, test scripts and test reports with SC management and the customer. The Contractor shall execute test cases, evaluate results, prepare a Software Test Report, generate and resolve Software Problem Reports in conjunction with the customer. The Contractor shall adhere to organizational test requirements and test group coordination. The Contractor shall obtain customer acceptance before each software release. The Contractor shall maintain proper documentation of and version control over developed scripts.

The Contractor shall perform planning, design, development, test and implementation of various front-end interface scripts to gather static and dynamic content from various sources. The Contractor shall maintain expertise in computer information systems to provide linkage between all elements of the work forces, control work processes, and manage, store, retrieve, manipulate, and process key web data elements.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

**Minimum Qualifications**

Senior Level Position. The Contractor shall have either a Bachelor of Science - Computer Science, or 3 years of experience in the areas of scripting using Powershell, HTML, VB Scripting, Shell scripting, command line utilities, administration and maintenancne, troubleshooting and problem solving of Enterprise Management Toolset.

**Certification and Security Clearance/Background Check Qualifications**

This position is certified as an IAT Level II position.

### Minimum Background Check:

Secret Clearance Required

## ORACLE DATABASE ADMINISTRATOR

The Contractor shall be able to perform Oracle Data Base Administration tasks. These include but are not limited to:

* Plan, design, install, configure, tune, troubleshoot, upgrade, and integrate high-end Oracle Database 11g /12c and future versions environments. Manage, maintain and administer database systems including troubleshooting and performance tuning.
* Provide Development and/or Production support. This includes creating primary database storage structures, designing and creating primary objects, modifying database structure as necessary for enhancements or performance, creating documentation, designing interfaces, database objects, and creating lifecycle plans.
* Strong Oracle Real Application Clusters (RAC) database skill with Oracle 11g/12c and future versions
* Strong Oracle performance tuning skills
* Advanced experience using Recovery Manager (RMAN) and Data Guard on 12c and future versions
* Experience with Red Hat Linux 7 and future versions
* Strong knowledge of Unix shell or Perl scripting languages
* Building High Availability Oracle Database RAC Architectures including clustering, load balancing, disaster recovery, backup and recovery, data guard implementation
* Monitor, report, and optimize performance of the database, plan for backup and recovery of the database, and allocate system storage and plan future storage needs.
* Create database-related scripts and programs to support development and production environments
* Establish and maintain sound backup and recovery policies and procedures
* Research, evaluate, design, test, recommend, and plan implementation of new or improved Oracle database, Online Analytical Processing (OLAP), Data Warehousing, Engineering Technical Letter (ETL) and database tools
* Provide technology blueprints, roadmaps, optimization and migration strategies
* Exposure and practice at using the Oracle Database Management System (DBMS) to optimize performance of large databases for enterprise use is preferred.
* Experience with Oracle Identity Management Single Sign-On/Oracle Internet Directory (SSO/OID)
* The Contractor shall be responsible for creating and maintaining configuration and system documentation.

The Contractor shall upload all system changes, software upgrades/changes, security upgrades/changes if at the application level, and any updates to any technical software or database repository files to a test environment as specified by the 75 ABW/SC for testing before official release to the production

environment. The Contractor shall demonstrate via testing that all critical components used in cryptographic systems are free of intentional defects and malicious design alterations.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform duties at Database Administrator (DBA) level, equal to someone with 5+ years of experience supporting relational databases as a DBA, with multiple distributed relational Oracle DBMS and related tools.

The Contractor shall be proficient working in a primarily Linux Server environment.

The Contractor shall be able to assist Government and other Contractor applications developers with such things as developing application programming interfaces between the data base and the user programs, designing and implementing new data base tables and instances to support new applications or new systems and requirements from the customers.

The Contractor shall be able to provide database upgrades and minor development to include On-Line Transaction Processing (OLTP) applications IAW IT standards from Headquarter AF.

### Certification Qualifications:

This position is certified as an IAT Level II position IAW AFMAN 17-1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required

## MS SQL DATABASE ADMINISTRATOR

The Contractor SQL Database Administrator shall perform tasks on databases residing on Windows Servers. The Contractor shall possess demonstrable skills in a multi-platform environment including the following:

* Extensive experience with SQL Server 2014, SQL Server 2016 and future versions. Overall experience shall be 5+ years IAW the Minimum Qualifications of this section.
* Strong experience in developing, maintaining and deploying complex SQL Server Integration Services (SSIS) packages.
* Experience with Storage Area Network (SAN) based architecture and understanding of Windows Server OS 2012, Windows Server OS 2016, and any future versions, Active Directory, VMWare and container environments, and network infrastructure.
* Experience in working with applications that have a very high accessibility need
* Deep understanding of all types of SQL Server replication, clustering, partitioning and mirroring.
* Implement and maintain a schedule for maintenance jobs in order to maintain the health, performance and integrity of the database systems.
* Experience with adhering to and implementing best practices within an enterprise environment that includes using source control for all database related artifacts (including jobs, SSIS packages and replication configuration) and following a change request/notification policy.
* Experience with upgrading prior versions of SQL Server to latest Release to Manufacturing (RTM) version or Community Technology Preview (CTP) version in a quick and efficient manner that minimizes downtime.
* Manage database security and control access permissions and privileges.
* Windows Server – a high level knowledge of Windows Operating environments including system administration, performance tuning, backup and restoration solutions, raid implementation using fiber channel storage mediums and knowledge of SAN. Previous experience in setup and administration of enterprise scale Windows Networks. Experience optimizing Windows applications.
* Continuity of Operations (COOP) – Experience working in and supporting a disaster recovery solution such as geo-clustering, data recovery and failover solutions.
* Networking Infrastructure – A broad general knowledge of networking principles and practices. Knowledge of multiple commercial hardware platforms including Cisco.
* Web Technologies – Experience supporting business applications on Internet Information Services (IIS), .NET, and Java 2 Platform Enterprise Edition (J2EE).
* Hardware – Experience with multiple hardware architectures. Experience troubleshooting hardware failures and system incompatibilities on these platforms. Experience with HP, Compaq, and Dell server platforms and network attached storage (NAS) storage systems.
* Perform System Administrative functions including migration of applications from development through testing and production, troubleshooting and diagnostics of applications, system and vendor software monitoring, tuning client and web applications, software and hardware upgrade installations and maintenance.
* Experience Government IT systems, policies and procedures and Government workflow processes, with system administration on a cross platform network.
* Project Management – significant experience in project management including work with Defense Information Systems, knowledge of project timelines, budgets, and Government reporting.
* Monitor products within the environment using such system monitors as Windows Event logs, Report, Web log files, etc.
* Provide technical consulting services to the Hill Enterprise Data Center (HEDC) customer on questions and issues relating to the software maintained on the HEDC systems for applications. Provide consulting and technical advice and problem resolution for development of application programs and system interfaces.
* Perform trend analysis on system performance, recommend configuration changes to the Government PM, and participate in the planning activities to schedule system upgrades.
* Continuously document/share and make generally available system information with stakeholders (both Government and other Contractors) as configuration, program or technical changes are made or occur. May provide, as-needed, hands-on, informal training and knowledge transfer to stakeholders each week as determined by the TOPM.
* At a minimum, all IT provided under, or in support of, this acquisition requires testing of at least a representative sampling of the IT that is delivered, and the results documented in writing. Use generally accepted commercial standards/practices for testing and documentation. Upon request, a copy of the test results shall be provided to the Government.
* Experience with reading, comprehending, and implementing STIGs pertaining to the supported systems.
* The Contractor shall be responsible for creating and maintaining configuration and system documentation.

The Contractor shall upload all system changes, software upgrades/changes, security upgrades/changes if at the application level, and any updates to any technical software or database repository files to a test environment as specified by the 75 ABW/SC for testing before official release to the production environment. The Contractor shall demonstrate via testing that all critical components used in cryptographic systems are free of intentional defects and malicious design alterations.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform Database Administrator level duties, equal to someone with 5+ years of experience.

### Certification Qualifications:

This position is certified as an IAT Level II position IAW AFMAN 17-1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required

## SYSTEM ADMINISTRATION / SERVER SUPPORT

The Contractor shall be responsible to provide server support, as well as operational support (hosting services) for servers, hosted application Commercial Off-the-Shelf (COTS) and Government Off-the- Shelf (GOTS), clusters, Domains, File Services, and Enterprise Backup Systems. The current supported environment includes Windows Server (2012, 2016, 2019, and approved future versions), Linux servers, and COTS and GOTS hosted applications. In addition to support for file services, server support shall include management of application servers, web servers, and database servers. Services are proactively monitored using a variety of tools for collecting information and issuing alerts. Routine maintenance and upgrades that may affect customer availability are normally performed outside of normal business operational hours; duties performed outside of normal business hours are coordinated and scheduled in advance. Server support shall also include disaster recovery planning and implementation services. The Contractor shall configure COTS operating system, middleware, and application software in accordance with DoDI 5200.44. The Contractor shall upload all system changes, software upgrades/changes, security upgrades/changes if at the application level, and any updates to any technical software or database repository files to a test environment as specified by the 75 ABW/SC for testing before official release to the production environment. The Contractor shall demonstrate via testing that all critical components used in supported servers, software, and cryptographic systems are free of intentional defects and malicious design alterations.

All source code/project files shall be uploaded to the 75 ABW/SC source code repository. (see CDRL A/B/C014)

Contractor personnel shall be knowledgeable of and proficient in the use of:

* Windows and Linux servers including but not limited to:
* Current AF approved versions of: Web servers (Apache, Tomcat, IIS), database servers (MS SQL Server, Oracle), application servers
* Application Development Environment
* Application Production Environment
* Isolated testing environment
* Disaster Recovery/COOP site servers (backup, Web)
* Virtual servers (i.e., VMWare, etc.)
* Containers
* Networks, VLANs, subnets, Internet
* Web sites that have very high accessibility needs
* Supporting web development environments
* Supporting MS SQL Server 2014/2016 server environments
* Supporting Oracle 11g/12c and future versions of server environments
* Oracle Enterprise Manager
* Familiarity with INET and IPV network and node requirements
* Disaster recovery planning, testing and preparedness
* Reading, comprehending, and implementing STIGs pertaining to the supported systems
* Creating and maintaining configuration and system documentation
* Maintaining permissions, security groups, confidentiality and general security of servers

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform the duties of System Administration and Server Support at a level equal to someone with at least 5+ years of experience.

### Certification Qualifications:

These positions are certified as IAT Level II positions IAW AFMAN 17-1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required

## HOSTING SERVICES / SYSTEM ANALYST

The Contractor shall be responsible for hosting services to include websites, applications, and database server services supported under this contract. Linux and Windows Server platforms are currently supported. Hill AFB Systems support both custom-developed applications and customized COTS applications.

The Contractor shall perform vulnerability testing and security analysis for software in an isolated test environment before approval on production networks. Testing shall include setting up various environments for desktop and server applications, patching environments, setup monitoring tools, and analyze results. The Contractor shall possess knowledge of common security threats and attack vectors, common ports and protocols, and STIGs.

Operational hours for all managed systems are 24/7/365. All scheduled maintenance, system backups and support services that affect customers are normally performed outside of core business hours. Application maintenance or other system downtime may be scheduled at the direction of the Government. Servers will not be available when scheduled server maintenance is performed. The Contractor shall be available to perform this scheduled maintenance as required outside of core business hours. Specific hours outside of core work hours, individual workload estimates, and a description of work shall be coordinated in advance with Government POC. The Contractor shall ensure that availability of the services will be measured end- to-end from the user’s desktop to the server providing the service. The goal is to provide availability from end-to-end 99.9% of the time outside of the scheduled maintenance window. The Contractor shall generate monthly server status reports on an as-required basis. The Contractor shall perform nightly backups to ensure that in case of a massive failure, restored data shall never be greater than 24 hours in arrears. This will minimize the amount of time required to bring the data integrity levels back to within operational specifications. If specified in an individual workload estimate, the Contractor shall be capable of longer archival, disaster planning, and off-site recovery services. Servers are monitored by the Communications Focal Point (CFP) on a 24/7/365 basis.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

The Contractor shall perform all infrastructure services, including proposed updates/patches/STIGs, needed to support the applications:

* tuned hardware
* system software
* database software
* utilities
* software interfaces to external systems
* user administration
* general logical and physical management
* configuration
* performance management
* fault management (OS patching and updates and STIG implementation)
* troubleshooting of any issues or problems encountered by patches, updates, STIG, and TCNO/TCTO implementations

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform Analyst/Administrator duties equal to someone with 5+ years of experience.

### Certification Qualifications:

The DMAPS Sr. Systems Analyst/Administrator does not require an IAT or IASAE certification.

All other Systems Analyst/Administrator positions require IAT Level II certification IAW AFMAN 17- 1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required

## ADMINISTRATIVE SERVICES

The Contractor shall be responsible to provide administrative services to include individual and group access to applications, domains and systems through user registration and profile management; server configuration, disk space and directory management; resource management; and establishing and managing directory services.

The Contractor shall provide individual and group access to applications, domains and systems through user registration and profile management; server configuration, disk space and directory management; shared resource management; and establishing and managing directory services. The Contractor shall oversee the creation of user accounts IAW AF policy and guidance, specifying the user’s identification data, group memberships, security-policy information and defining the user’s rights on the system. The Contractor shall create and maintain volumes and directory structures; assign account, workgroup and print managers; administer directory distribution and replication; define and manage resources, domains and server passwords; support standard security mechanisms and trusted third-party security servers; and synchronize security structures across servers. The Contractor shall, IAW AF policy and guidance, configure, set up servers with both OS and network OS software; acquire and upgrade hardware and software and associated addresses; and develop installation documentation and server images. The Contractor shall follow AF configuration management policies, including use of Remedy tools. The Contractor shall create and maintain technical documentation. The Contractor shall configure the OS and network OS; include protocol details, user and group definitions, address schemes, backup and restore processes, and disk space mappings. The Contractor shall monitor and report on service level delivery, hardware configurations, and access rights. The Contractor shall manage Windows Server domains and Active Directory, Internet Protocol (IP) addresses, and firewall parameters. The Contractor shall monitor, report and analyze server performance statistics, install management agents, and tune servers. The Contractor shall resolve problems using escalation and alert processes in coordination with the TOPM; and shall also maintain a log of all activity in Remedy for fault management. The Contractor shall develop server capacity plans, monitor current server workloads and project future workloads. The Contractor shall provide problem diagnosis and resolution. The Contractor shall perform hardware maintenance and repair IAW manufacturer warranty. The Contractor shall perform change management in accordance with established policy. The Contractor shall coordinate with the TOPM to mitigate vulnerabilities reported by IT security scans and industry reports, continually assess requirements, evaluate risks, and implement procedures to log, alarm and report security violations. The Contractor shall ensure that anti-virus software agents and definitions are current on all servers. The Contractor shall monitor events related to system security to identify any security breaches and to determine the extent and location of any damage, perform corrective actions to repair systems, and notify the proper authorities if warranted. The Contractor shall implement all TCNOs and AF Time Compliance Technical Orders (TCTO) within the specified timeframes identified by TO PMs as well as the guidance given by the communication of the TCTO and TCNO. The Contractor shall provide patch management via MS SMS, and Windows Server Update Services (WSUS). OS patches/updates and STIG compliance that cannot be automatically applied shall be manually implemented and shall include testing of the above changes, to include a test report. The Contractor shall perform automated server monitoring which includes network connectivity, central processing unit (CPU), memory, disk space thresholds, uptime, response time, and web server availability, and shall provide reporting via Remedy work order/incident ticket. The Contractor shall maintain and review server logs using AF-provided log consolidation tools; log warnings and alerts should be reviewed daily in a proactive manner. The Contractor shall maintain server inventory and provisioning documents.

The Contractor shall maintain software inventory, warranty information, licensing and vendor contact information. The Contractor shall notify the AF in the event of expiring support of hardware and software. The Contractor shall maintain a clean server and surrounding area environment. The Contractor shall maintain currency of existing service offerings through research, development, deployment, and training. The Contractor shall provide updates to user manuals and support materials. The Contractor shall perform Backup, Restoration and Disaster Recovery including maintenance, administration, and documentation of backup infrastructure as described above; perform and monitor all server backups; restore files and directories in response to user help desk requests; perform tape rotation IAW Hill AFB policies and procedures; interface with Hill AFB offsite tape storage facility; and support tape backup and restore activities associated with the DR/COOP process and ensure data backup and transfer to the DR/COOP facility.

In addition to the Administrative Services requirements listed in paragraph 1.10.2, the Contractor shall have an in depth understanding of the intricacies of the Depot Maintenance Accounting and Production System (DMAPS) and the Execution & Prioritization of Repairs Support System (EXPRESS).

DMAPS is a suite of systems established to ensure AFMCs compliance with various legislative financial requirements. The DMAPS suite includes Air Force and other DoD systems that support financial, material ordering, labor, overhead, pricing and user access functionality. These systems are highly integrated and require rigorous monitoring and precise timely processing. The Contractor supporting DMAPS shall have an in-depth understanding of the applicable DMAPS interfaces, system architectures, data processing schedules & functions (daily, monthly and annual), reporting functions, AFMC change & configuration management processes and system testing & approval processes. The Contractor shall communicate closely with the various system Program Management Offices (PMOs) and shall provide support with system enhancements, testing, troubleshooting, user access management and facilitate collaboration between the various DMAPS system PMOs & user communities.

EXPRESS is a component of the Weapon System Management suite of systems and is the standard command system for the Repair-on-Demand environment. EXPRESS is integrated with several legacy systems and is utilized to facilitate repair prioritization, support & funding availability and product distribution. The Contractor supporting EXPRESS shall have an in-depth understanding of the applicable interfaces, data handling, user access and account management processes related to that system. The Contractor shall facilitate and oversee all EXPRESS batch processing (daily, monthly and annual) and ensure that they are completed accurately and as scheduled. The Contractor shall have the ability to manually run the batch processes and manage the automated processes. The Contractor shall have experience with SharePoint and the ability to manage the EXPRESS documentation and reporting within the SharePoint site. The Contractor shall communicate closely with the EXPRESS Program Management Office (PMO) and shall provide support with system enhancements, testing, troubleshooting, user access management and facilitate collaboration between the EXPRESS system PMO and the user communities.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform duties at a Senior Analyst/Administrator level, equal to someone with 5+ years of experience at a senior level.

### Certification Qualifications:

The DMAPS Sr. Systems Analyst/Administrator does not require an IAT or IASAE certification.

All other Sr. Systems Analyst/Administrator positions require IAT Level II certification IAW AFMAN 17-1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required

## SOFTWARE DEVELOPMENT

The Contractor shall provide database administration, system administration, software maintenance, software development support and technical expertise in support of 75 ABW/SC managed systems.

Database upgrades, application sustainment, and new development, to include OLTP applications, shall be required. The Contractor shall be responsible for creating program specifications and unit test criteria, coding and testing program units, and produce technical program documentation. The Contractor shall use applicable structured development and object-oriented principles and tool suites. Responsibilities include coding, developing, testing and maintaining new and existing client, client-server, and web applications. The Contractor shall upload all system changes, software upgrades/changes, security upgrades/changes if at the application level, and any updates to any technical software or database repository files to a test environment as specified by the 75 ABW/SC for testing before official release to the production environment. The Contractor shall demonstrate via testing that all critical components used in cryptographic systems are free of intentional defects and malicious design alterations. The Contractor shall be required to develop interactive solutions with web optimization that integrate with back-end legacy systems and databases

The Contractor shall be responsible for following applicable Configuration Management policies (SharePoint access to the policies will be provided to Contractor after award) including source code management, documentation, and operating procedures. The Contractor shall demonstrate expertise in DoD, AF, and AFMC architectures, policies and standards, including the GCSS architecture. The Contractor shall have experience applying systems engineering concepts and factors, such as structured design, supportability, reliability, scalability, and maintainability, sufficient to ensure that applications are optimized for technology and functionality. The Contractor shall apply these concepts utilizing various programming languages and tools to include SQL, T-SQL, PL/SQL, C#, Java, .NET Core, .NET Framework, Visual Basic and ASP. NET. Experience using the Model View Controller design pattern is preferred. The Contractor shall have knowledge of common web programming languages and tools, including but not limited to, HTML, CSS, and JavaScript, JSON, AJAX, jQuery, Bootstrap, Razor, XML, and experience with Git based source control tools. Contractor experience developing and maintaining software using DevOps, secure coding practices, Test Driven Development and other software development technologies is preferred.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform duties as a Software Developer equal to someone with 5+ years of experience.

### Certification Qualifications:

These positions are certified as an Information Assurance System Architect and Engineer (IASAE) Level I or Level II IAW AFMAN 17-1303.

### Minimum Background Check:

Secret Clearance Required

## DEPOT COST AND SCHEDULE TOOL (DCAST) DESIGN / DEVELOPMENT AND SUSTAINMENT

DCAST provides an analytical look at Maintenance, Repair, and Overhaul (MRO) activities including labor productivity, asset repair cost and revenue, Profit and Loss, budgets, partnering financials, earned value management, leave and wellness indicators and organizational and personal labor performance metrics across the Air Logistics Center (ALC). DCAST is installed at all three ALCs (Ogden Air Logistics Center at Hill AFB, Warner-Robins Air Logistics Center at Warner-Robins AFB, and Oklahoma City Air Logistics Center at Tinker AFB). To complete this analysis, the DCAST system performs a daily update which includes pulling data from multiple data sources, processing this data through the several DCAST business rules modules, aggregating, collating and generating all the data necessary for the for- system functions. This update process entails the import, analysis and manipulation of over 75 million database records.

DCAST is a Java web-based multi-level management reporting tool that tracks cost, revenue and transactional data covering the production and/or repair of all assets at the ALC as well as an extensive set of labor productivity metrics. DCAST satisfies all levels of management purview by providing organizationally based reports at the Employee, Supervisor, Resource Cost Center (RCC), Squadron, Group and Wing level while also providing product cost and revenue reports at the Operation, Job Order Number (JON), End Item, Weapon System and ALC level. Earned Value Management (EVM) metrics are available for all serialized workloads.

DCAST is designed, by consolidating and analyzing data from multiple systems, to be a “one stop, top to bottom” reporting tool to assist in the daily management of MRO activities. DCAST provides functional as well as financial reporting metrics and analysis across the breadth and depth of the ALC.

Support for DCAST shall include upgrading the software to maintain compliance with government computer systems and regulations. Architecting, coding, testing and adding new reports and requirements requested by the three ALC’s (OO-ALC, OC-ALC and WR-ALC). This includes approximately three new releases deployed yearly with all technical support for the deployment, training of system Office of Primary Responsibility (OPRs), in depth training to users, bug fixes and troubleshooting of hardware and software. Help desk support for DCAST users shall also be required as a part of this position. Contractor shall update and maintain the DCAST User Manual and System Administration Guide and all other system documentation. The Contractor shall have an extensive knowledge of DCAST source data locations, data formulation and processes and inter system communications. The Contractor shall have development skills and required expertise in Java, SQL, HTML, JSP and J2EE.

There is currently an effort to incorporate the DCAST system within Depot Maintenance Accounting and Production System (DMAPS). The Contractor supporting this effort shall have an in-depth working knowledge of AFMC financial, planning, data warehousing and legacy systems and processes. The Contractor shall have extensive knowledge of the application of performance yield rates, Earned Value Management, incremental Earned Hours, labor productivity, Defense Industrial Finance Management System (DIFMS) partner financials, bulk (indirect as direct) processing and leave and wellness indicators. The Contractor shall have expert knowledge of the DCAST update engine is required to assure the optimization of the update process and the integrity of the generated DCAST data.

The Contractor shall provide software design, development, and sustainment support and technical expertise for the DCAST. The Contractor shall be responsible for creating program specifications and unit test criteria, code and test program units, and produce program documentation; use applicable structured development and object-oriented principles and tool suites; be responsible for following applicable Configuration Management policies including source code management; demonstrate expertise in DoD, AF, and AFMC architectures, policies and standards, including the GCSS architecture; and be proficient using Oracle and J2EE. The Contractor shall provide consolidation from several data sources. Among these data sources will be various legacy data stored in either proprietary DBMSs or Oracle. The Contractor shall be required to work with various system points of contact (POCs) to determine the best data sources. The Contractor shall provide on-site support for the implementation, sustainment and deployment of DCAST systems and their associated enhancements.

The Contractor shall work with 75 ABW/SC to maintain the functionality of the overall DCAST. The Contractor shall provide business process improvement support that includes all activities involved in helping improve customer data systems through business process redesign, including rethinking program design, and aligning IT infrastructures with business missions, goals, and objectives. The Contractor shall gather information by developing and implementing data collection instruments. The Contractor shall perform manual and automated modeling activities, including requirements, processes, activities, and data. The Contractor shall perform business process reengineering.

The Contractor shall provide expertise in the technical areas of system administration for the maintenance and day-to-day operation of DCAST. The Contractor shall provide system training and user indoctrination upon request by 75 ABW/SC. The Contractor shall work with 75 ABW/SC to sustain the technical and functional capabilities of all DCAST programs including operations, maintenance, and modernization activities. The Contractor shall provide updates as required to any technical software and database repository files. The Contractor shall validate upgraded software and track system functional discrepancies and other functional issues to improve the system’s integrity. The system software maintenance/updates shall include Customer change requests as directed by the TOPM. The Contractor shall upload all system changes, software upgrades/changes, security upgrades/changes if at the application level, and any updates to any technical software or database repository files to a test environment as specified by the 75 ABW/SC for testing before official release to the production environment. The Contractor shall demonstrate via testing that all critical components used in cryptographic systems are free of intentional defects and malicious design alterations.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

The Senior Lead Developer position shall have 10+ years of experience with DCAST and/or DMAPS. The Senior Lead Developer shall have an understanding of the DCAST business rules pertaining to AFMC finance, production and MRO activities, including extensive understanding of how DCAST business rules align with the Depot Maintenance Accounting and Production System (DMAPS) systems and processes. The Contractor shall have a working knowledge of AFMC financial metrics including, plan cost, plan revenue, the application of applied rates, budgeting processes, performance yield rates, actual costs, and how these are derived from the legacy system databases.

The Senior Lead Developer position on DCAST shall have a minimum of 10+ years of experience with J2EE 3-tier applications in multithreaded environments, Oracle SQL, Java server pages (JSP) and Java Database Connectivity (JDBC) components applicable to data warehousing and be expert in the application of Java language object-oriented programming techniques and application in multi-tier and web environments. The Contractor shall have minimum of 5 years of experience with Earned Value Management concepts, development and application in a government setting and have experience training or be able to train diverse audiences, from Command Level Leaders down to shop floor technicians, on the DCAST application of financial disciplines to production activities. The Contractor shall have a thorough understanding of how the DMAPS system data is aggregated in the DMAPS Data Storage System (DDSS). The Senior Lead Developer shall have excellent trouble-shooting techniques including comprehensive knowledge of networking, Oracle databases, application server environments, and desktop configurations including Internet Explorer and Java implementations.

The Contractor shall be compliant of these requirements IAW AFMAN 17-1303 paragraph 3.2.12.2.1, AFMAN 17-1303 Attachment 2, and AFMAN 17-1303 Table A2.5.

### Certification Qualifications:

This position is certified as an IASAE Level II position.

### Minimum Background Check:

Secret Clearance Required

### Minimum Qualifications:

The Junior Developer position on DCAST shall have a minimum of 5+ years of experience with J2EE 3- tier applications, SQL, JSP, and JDBC components applicable to data warehousing. The Junior Developer position shall have experience in the application of Java language object-oriented programming techniques and web environments. The Junior Contractor position on DCAST shall have a basic understanding of the DCAST business rules pertaining to AFMC finance, production and MRO activities and a basic understanding of how DCAST business rules align with the DMAPS systems and processes.

### Certification Qualifications:

This position is certified as an IAT Level II position.

### Minimum Background Check:

Secret Clearance required

## DEVSECOPS ENGINEER

The Contractor shall provide DevSecOps Engineering expertise. The DevSecOps Engineer shall be accountable for overseeing the continuous integration and delivery (CI/CD) of the working product, and shall perform the following responsibilities:

* Implementing DevSecOps Strategy to include: recommending a migration and consolidation strategy for DevSecOps tools; implementing secure development process; implementing a version control strategy; integrating source control; managing build infrastructure; implementing code flow; implementing a mobile DevOps strategy; managing application configuration and secrets.
* Implementing Continuous Feedback to include: recommending and designing system feedback mechanisms; implementing a process for routing system feedback to development teams; optimizing feedback mechanisms; establishing monitoring metrics and notifications to rapidly respond to system issues; guiding and/or participating with Development and Engineering teams in establishing key performance benchmarks and monitoring for applications; implementing and maintaining application monitoring tools.
* Working with the Development and Engineering teams to define the set of tools and processes for the continuous delivery pipeline
* Working with the Information Assurance team to ensure that the tools are compliant with security requirements
* Working with the Information Assurance team to streamline the ATO process from a tools and technical process perspective
* Working with the Development and Engineering team to automate software testing where possible
* Working with the Development and Engineering team to ensure that the CI/CD processes align with operational requirements.

The DevSecOps Engineer shall also have hands-on experience working with tools and technologies in, at a minimum, two of the following areas: software development, configuration control, testing, security, automation, containerization, orchestration, cloud services, open-source technologies.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform the duties at a level equal to someone with at least 3+ years of experience.

### Certification Qualifications:

These positions are certified as IASAE Level I IAW AFMAN 17-1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required

## WINDOWS SOFTWARE TESTING SUPPORT

The Software Tester shall oversee installing and configuring testing environments from scratch using virtualization technologies, such as VMware, and shall perform standardized security testing and analysis results. The Contractor shall have a knowledge of ports, protocols, permissions, file systems, common attacks and threat vectors. The Contractor shall have knowledge of Air Force standard desktop and server operating system configurations; DISA STIGs, especially for operating systems; patching; external devices; drivers; and maintaining virtualized environments.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, critical or mandatory update/upgrades/migrations, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

Senior Level Position. The Contractor shall be able to perform the duties of a Software Tester with 5+ years of experience as a Windows system admin, performing testing for both desktop and server operating systems.

### Certification Qualifications:

These positions are certified as IAT Level II positions IAW AFMAN 17-1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required

## BMC REMEDY SUBJECT MATTER EXPERT

The BMC Remedy Subject Matter Expert shall have knowledge of techniques, procedures and processes such as operating system, computer system architecture, software engineering and computer communications and networking. The Contractor shall have the ability to formulate programming specifications and write code for multiple software platforms, including but not limited to, Oracle, WebLogic, Apache Tomcat, Java, SQL, and Scripting Languages. The Contractor shall have the ability to provide application production support for several BMC Remedy applications deployed in the Hill Enterprise Data Center (HEDC). The Contractor shall provide technology blueprints, roadmaps, and optimization and migration strategies for several technology vendors such as Oracle, BMC, etc., which are deployed at Hill AFB, Utah. The Contractor shall have the ability to test and evaluate tools and techniques to enhance the development and operation of computer software and computer systems. The Contractor shall have the ability to research, analyze, interpret and apply rules, regulations and procedures in a variety of situations and recommend timely and economical solutions. The job duties are varied and complex, and the Contractor shall utilize independent judgment.

The Contractor shall implement an after-hours call escalation process to ensure system availability should there be a problem outside of normal working hours. In general, the Contractor shall be available after normal duty hours to fix issues for servers and systems requiring this service. The Contractor staff shall be available for on-call and/or off-hours support on a pre-arranged, agreed upon basis.

During after-hours services, Contractor personnel shall shift normal duty hours to hours that will cover support for the outage or downtime.

### Minimum Qualifications:

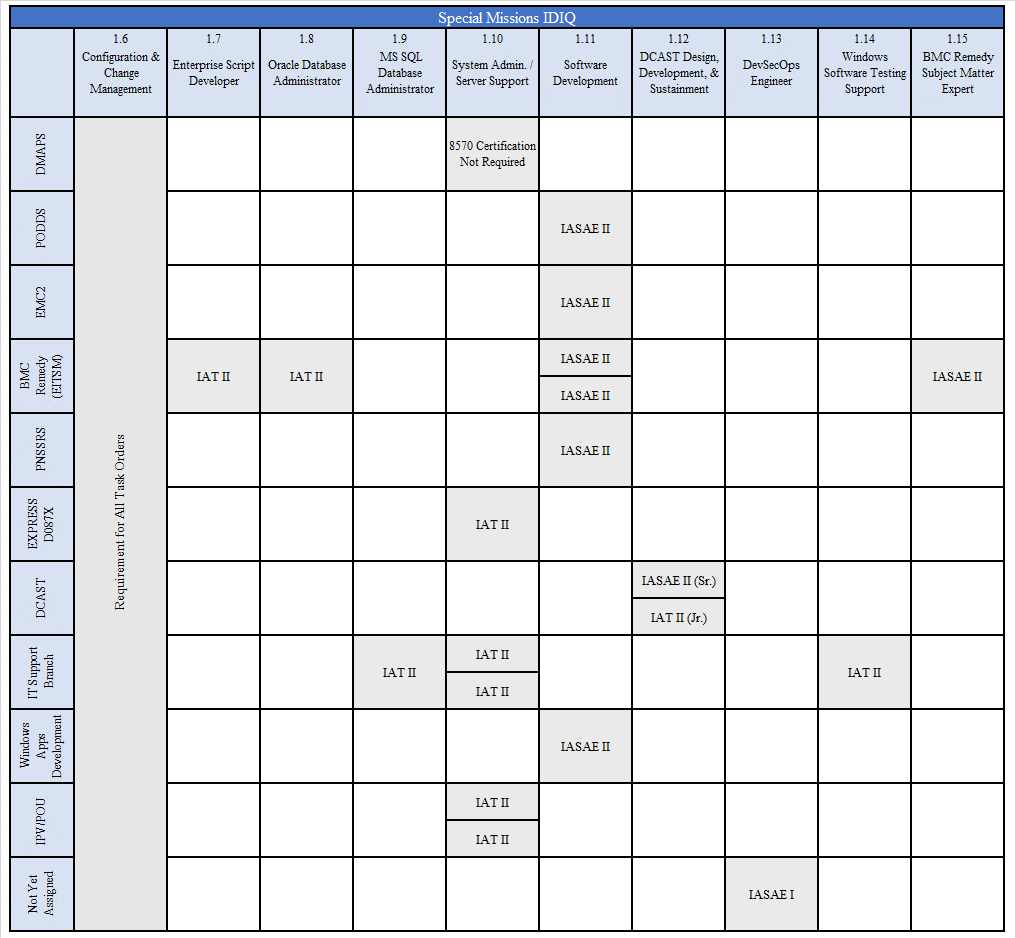
Senior Level Position. The Contractor shall have 8+ years of hands on and in-depth working experience in Unix/Linux (Redhat)/Windows/Virtual environment specifically VMWare architecting, engineering and implementation for large data center operations. This also includes knowledge of networking and communications related tools, and experience with DoD/DISA/Air Force organizations with a key 24 X 7 reliance on Oracle database.

### Certification Qualifications:

These positions are certified as IASAE Level II IAW AFMAN 17-1303.

### Minimum Security Clearance/Background Check:

Secret Clearance Required



## TASK ORDER ROLES SUMMARY

The following image shows the task order roles required in relationship to the requirements defined above.

*Table 1-2 — Task Orders, Programs, & Baseline Certification Matrix*

# SERVICE SUMMARY (SS)

The purpose of the SS is to define performance evaluation. The SS chart that follows ([Table 2-1](#_bookmark37)) lists the PWS Performance objective requirements (column 2) that the COR(s) will surveil. The absence of any PWS requirement from the SS does not detract from its enforceability nor limit the rights or remedies of the Government and sets forth the maximum allowable deviation from the standard of performance for that service.

The Contractor shall address and respond to special requirements identified by the tasking organization within task order requirements. These requirements may consist of items or tasks that are related to, but not specified in, the basic services identified in this PWS. The Contractor will be performing at their own risk and expense if work is performed before contract and/or Task Order award.

## GOVERNMENT QUALITY ASSURANCE

Contractor performance will be compared to the performance objectives and performance threshold. The Government may use a variety of surveillance methods to evaluate the Contractor’s performance to determine if it meets the performance objectives and performance threshold. (see [Table 1-2](#_bookmark32))

## PERFORMANCE EVALUATION

The Contractor’s performance will be evaluated to determine whether it meets the performance objectives and performance thresholds defined below. The Government will evaluate the Contractor’s performance under this contract using Inspection of Services Fixed Price FAR § 52.246-4. All surveillance observations will be recorded by the COR or TOPM.

## SERVICE SUMMARY TABLE

The Service Summary Table identifies Objectives, Performance Thresholds, and the referenced paragraphs in this PWS where the Objectives are described.

*Table 2-1 — Service Summary Table*

|  |  |  |
| --- | --- | --- |
| **PERFORMANCE OBJECTIVE** | **PWS PARAGRAPH** | **PERFORMANCE THRESHOLD** |
| The Contractor shall provide Monthly Status Reports to be delivered by 10 working days after the beginning of the month. (see CDRL A/B/C001) | [1.2](#_bookmark2), [1.3.4](#_bookmark7),  [1.3.4.1](#_bookmark8) | 100% within 10 working days after 1st of the month. |
| The Contractor shall report deficiencies and issues to TO PMs and in the Remedy trouble ticket reporting system. | [1.6](#_bookmark19), [1.7](#_bookmark20), [1.8](#_bookmark21), [1.9](#_bookmark22),  [1.10](#_bookmark23), [1.11](#_bookmark26), 1.12,  [1.13](#_bookmark27), [1.14](#_bookmark29), [1.15](#_bookmark30) | 90% within 1 business days.  Remaining 10% within  2 business days. |
| The Contractor shall document and report their System Administration Tools (SAT) findings and results to both the appointed Government test lead and to the software supplier(s) through Remedy. | [1.5](#_bookmark15), [1.6](#_bookmark19), [1.7](#_bookmark20), [1.8](#_bookmark21),  [1.9](#_bookmark22), [1.10](#_bookmark23), [1.11](#_bookmark26),  1.12, [1.13](#_bookmark27), [1.14](#_bookmark29),  [1.15](#_bookmark30) | 90% within 24 hours.  Remaining 10% within  7 days. |

|  |  |  |
| --- | --- | --- |
| The Contractor shall provide systems and process training to designated Government personnel (as requested). The Contractor shall indicate the percentage of hours for which training was provided in the Monthly Status Reports. (see CDRL A/B/C001) | [1.7](#_bookmark20), [1.8](#_bookmark21), [1.9](#_bookmark22),  [1.10](#_bookmark23), [1.11](#_bookmark26), 1.12,  [1.13](#_bookmark27), [1.14](#_bookmark29), [1.15](#_bookmark30) | 90% within 2 days of request  Remaining 10% within 7 days of request |
| The Contractor shall be responsible for following applicable Configuration Management policies including source code management, documentation, and operating procedures – Provide monthly status report of documentation progress (see CDRL A/B/C011). This includes Software Deployment Change Requests (SDCRs), Test Process documentation for the current change set, and assistance with the creation of the Software Release Transmittal Letter (SRTL), including Test Process/Procedures and Change Description. | [1.6](#_bookmark19), [1.7](#_bookmark20), [1.8](#_bookmark21), [1.9](#_bookmark22),  [1.10](#_bookmark23), [1.11](#_bookmark26), 1.12,  [1.13](#_bookmark27)*,* [1.14](#_bookmark29), [1.15](#_bookmark30) | 100% of the time. |
| Contractor-developed scripts, programs, and other utilities and tools will meet customer’s functional requirements.  Development, testing, and rework will not exceed allocated time and projects will be delivered on schedule and ready for production unless an extension has been approved by the Government. Projects will have comprehensive requirements definition, thorough unit and integration testing, and adherence to AF quality standards. | [1.6](#_bookmark19), [1.7](#_bookmark20), [1.8](#_bookmark21), [1.9](#_bookmark22),  [1.10](#_bookmark23), [1.11](#_bookmark26), 1.12,  [1.13](#_bookmark27), [1.14](#_bookmark29), [1.15](#_bookmark30) | 100% of the time. |
| Weekly Activities Report (WAR) (see CDRL A/B/C003) | [1.3.4.2](#_bookmark9) | 100% of the time. |
| The Contractor shall provide reports, plans, invoices, documentation and other correspondence at the time, frequency and in the number of copies specified in the PWS and CDRLs. | [1.2](#_bookmark2), [1.3](#_bookmark3), [1.5.2](#_bookmark17),  [1.6](#_bookmark19), [1.7](#_bookmark20), [1.8](#_bookmark21), [1.9](#_bookmark22),  [1.10](#_bookmark23), [1.11](#_bookmark26), [1.12](#_bookmark27),  [1.13](#_bookmark28), [1.14](#_bookmark29), [1.15](#_bookmark30),  [2.3](#_bookmark36), [4.30](#_bookmark98) | 100% of the time |

## QUALITY CONTROL

## QUALITY CONTROL PLAN

In compliance with FAR § 52.246, *Inspection of Services – Fixed-Price*, the Contractor shall establish a complete Quality Control Program to ensure the requirements of this contract are provided as specified. The Quality Control Plan shall be documented and provided to the Government for acceptance upon Request for Proposal (RFP) (see CDRL A/B/C009). The Quality Control Plan has specific areas of concern regarding quality control. Task Orders may include additional Quality Control Objectives that will define performance evaluation specific to the Task Order requirements. The CO will notify the Contractor of acceptance or required modifications to the Quality Control Plan before the contract start date. The Contractor shall make appropriate modifications (at no additional costs to the Government) and obtain acceptance of the plan by the CO before the start of the contract.

## QUALITY ASSURANCE

The COR may inspect each task as completed or increase the number of quality control inspections if deemed appropriate because of repeated failures discovered during quality control inspections or because of repeated customer complaints. Likewise, the COR may decrease the number of quality control inspections if merited by performance. The COR will also investigate complaints received from various customers located on the installation. The Contractor shall be responsible for initially validating customer complaints. However, the COR shall make final determination of the validity of customer complaint(s) in cases of disagreement with customer(s).

## CONTRACTING OFFICER REPRESENTATIVE (COR)

The COR is the authorized Government representative(s) who will perform assessments of the Contractor’s performance. Prior to contract award, the identity of the COR(s), with a letter defining their duties and authority will be promptly furnished to the Contractor. The COR(s) or alternate(s) will inform the CPM when discrepancies occur and will request corrective action. Any matter concerning a change to the requirement, scope, prices, terms or conditions of this contract shall be referred to the CO and not to the COR(s). All services to be performed by the Contractor during the period of this contract are subject to review by the CO or authorized representative(s) (i.e. Contract Specialist, COR, etc.).

# USE OF GOVERNMENT PROPERTY, EQUIPMENT, MATERIALS AND SOFTWARE

## GENERAL

The Government will provide the facilities, equipment, and/or services listed in this section. The Contractor shall be responsible for safeguarding Government equipment provided for Contractor use.

Each Contractor employee will be provided a computer and monitor(s) to facilitate network connectivity and remote access to servers and equipment. The Government will furnish a computer with the Air Force Standard Desktop Configuration (SDC) software and a connection to a printer on the local area network (LAN).

The Government will also furnish laptop computers to the Contractor with wireless capability and cellular air cards for remote access and virtual private network (VPN) access to the base network and servers in Building 849, 1211, 1236 and/or 891.

All products developed under this contract shall be considered Government work and shall have no license encumbrances. All Government Furnished Equipment (GFE), Government Furnished Software (GFS), and Government Furnished Material (GFM) shall be returned to the Government upon completion of this contract. In accordance with FAR 45.000b (5) all equipment is incidental to performance.

## EQUIPMENT INVENTORY

The Contractor and a Government Representative (COR/Equipment Custodian) shall conduct a joint inventory of GFE listed in this section not later than five (5) calendar days prior to start of the first operational performance period and not later than ten (10) calendar days before completion of the contract period including any option periods. The Contractor shall sign a receipt for equipment provided by the Government. The Contractor and a Government Representative shall jointly determine the working order and condition of equipment. Items of equipment missing or not in working order shall be recorded and the CO notified in writing. Except for those items identified in this section as being furnished “as is”, the

Government will replace missing items and repair items not in working order or the CO will direct the Contractor to replace the missing item(s) or accomplish the repair and the Contractor will be compensated by negotiated modification to this contract. The Government Representative will give disposition instructions for items beyond economical repair. The Contractor and the Government Representative shall certify their agreement as to the working order of the equipment. If the Contractor does not participate in the inventory, the Contractor shall accept as accurate the listing and stated condition of equipment provided by the Government. If the Contractor participates in the inventory but does not agree with the Government Representative's determination as to the working order of the equipment, this failure of the Contractor to agree on working order and defectives shall be treated as a dispute pursuant to the Federal Acquisition Regulation (FAR) § 52.233-1, Disputes.

At the end of each task order performance period, a joint inventory of property shall be conducted by the Contractor and a Government Representative (TOPM or Equipment Custodian). The Contractor shall be liable for loss, damage or destruction to Government Furnished Property beyond fair wear and tear according to the applicable property clause of the contract.

## GOVERNMENT FURNISHED FACILITIES

The Government will furnish and/or make available Facilities, as identified in this paragraph, to the Contractor to perform the requirements as defined in this contract. HILLAFBI 32-103 *Space Management* (Certified Current 07 Feb 2020) sets the standard for administrative space at 40 ft.2 per person. This standard is an organizational average per personal equivalent. This includes employees, supervision, conference rooms and administrative work and storage areas.

## GOVERNMENT FURNISHED INFORMATION

Where required by workload data, the Government may furnish the Contractor reasonable access to data required for support of the work effort. Any data, code, and/or work product created in the performance of this contract and its Task Orders gives the Government unlimited rights to the created products.

## DATA RIGHTS

The Government shall have unlimited licensing rights to all documents/material produced under this contract. The Contractor(s) will be required to sign a Non-Disclosure Agreement for each task order to protect unclassified or CUI data that the Contractor is given exposure to prior to beginning work on any task order. (See CDRL A/B/C013)

## DATA RIGHTS AND NON-COMMERCIAL COMPUTER SOFTWARE

In order to implement the provisions at DFARS 252.227-7013 and DFARS 252.227-7017, the Contractor shall disclose to the CO and ordering office in any proposal for a TO, or after award of a TO if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the TO. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. This disclosure requirement also applies to segregable routines of non-commercial software developed at Government expense to integrate Commercial Software components or applications provided under a commercial software license or developed to enable Commercial Software to meet requirements of this PWS. Performance of this disclosure requirement shall be considered a material performance requirement of any TO under which such technical data or non-commercial computer software is developed at Government expense.

All new source code development, code changes, code improvements, code fixes shall be placed in the 75 ABW/SC source code repository on a daily basis or as frequently as new development, changes, improvements, or fixes to source code are completed. (see CDRL A/B/C014)

## UTILITIES

The Government will furnish utilities-related services which are required for the operation of defined functions. These utilities include electricity, water, sewage, heating for facility and compressed air. Any non-emergency utility issues encountered by Contractor employees shall be reported to the building facility manager for the building they occupy. For any emergency utility issues encountered by Contractor employees shall be reported to the CO and COR.

## CONTRACTOR REPRESENTATION AND PRESENTATION

When using Government furnished communication devices or processes (e.g., the Voice over Internet Protocol (VOIP) network, telephones, e-mail, etc.) the Contractor and its employees shall take all reasonable precautions to ensure that the persons or entities with whom the Contractor or its employees are communicating are placed on notice that they (the persons or entities with whom the Contractor or its employees is communicating) are communicating with the Contractor, not the Government. These precautions are necessary to preserve the arms-length relationship that must always exist between the Government and the Contractor, and to eliminate or minimize the risk that the persons or entities with whom the Contractor is communicating will mistakenly believe they are communicating with the Government and inadvertently disclose information that the Contractor is not authorized to receive. Such precautions will include, at a minimum, 1) an express oral statement by the Contractor and its employees at the beginning of each telephonic or VOIP or similar audio communication that clearly informs the other party that they are communicating with the Contractor or one of its employees, and 2) a conspicuous written notice, including contact information on all email and other written communications sent by the Contractor and its employees, that clearly and immediately informs the other party that the sender is a Contractor or Contractor employee.

## TELEPHONE SERVICE

The Government will provide telephone service to include Defense Switched Network (DSN) service. Telephone service classes are defined in AFMAN 33-145. The Contractor shall ensure that usage of Government provided telephones is limited to only “Official” Government business related to the performance of this contract. DSN capability will be provided for small systems contract management, mid-tier application support and small systems software development. Government Furnished telephones and services will be used IAW AFMAN 33-145, *Voice Systems Management* (06 Sept 2012) and not for personal business. The Government will not provide cell phones, Blackberry devices, smart phone devices, or other mobile communication devices for the Contractor, except as deemed necessary by the Government.

## CUSTODIAL SERVICE

The Government will provide limited custodial service to the extent provided in the Base Custodial Contract(s) for the facilities provided. The Contractor shall abide by posted signs regarding Custodial requirements.

## REFUSE COLLECTION

The Government will provide for refuse services to the extent provided in the Base Refuse Contract(s). Contractors will be responsible for:

* Collecting and disposing of their refuse by depositing in base-provided dumpsters
* Emptying their desk garbage weekly
* Properly disposing of batteries and any other hazardous material

## BASE CIVIL ENGINEERING

The Government will provide fire prevention and protection, inspection and maintenance of Government Furnished fire extinguishers and/or systems, pest control and grounds maintenance. The Contractor shall make all assigned facilities, areas and equipment available for inspection, surveys and accomplishment of fire protection services, maintenance and repair by authorized Government or Contract personnel. Fire Department telephone extension is 911 for emergency calls and 586-0821 for routine calls.

## SECURITY FORCES

The Government will provide general on-base Security Forces service. Security Forces emergency phone extension is 911 and 777-3056 for routine calls.

## POSTAL SERVICE

The Government will provide the required postal service in support of this contract. Postal Services will be limited to official Government mail matter required under terms of this PWS.

# GENERAL INFORMATION

Prior to beginning work, the Contractor employees must complete the 75 ABW/SC In-Processing Checklist provided by 75 ABW/SC. The Out-Processing Checklist, also provided by the 75 ABW/SC, must be completed upon Contractor employee exit from the job or at termination of the contract. The In- Processing Checklist or Out-Processing Checklist can be obtained by the TOPM for the appropriate task order.

## COMMON ACCESS CARD (CAC)

Contractor shall complete the organization's In-Processing Checklist Contractor shall present document(s) that establish identity; acceptable document(s) include valid driver's license with photograph, name, date of birth, gender, height, eye color and address; ID card issued by federal, state, or local Government agencies with photograph, name, date of birth, gender, height, eye color and address; U.S. military card; military dependent ID card. A Common Access Card (CAC) is required for all on-site Contractor personnel. The organization's security manager(s) will start Form 496 process if JPAS shows favorable result of background investigation. The Government will provide appropriate identification cards which shall be issued, displayed and surrendered as directed in HAFBI 31-101, Installation Security Program.

The Contractor Program Manager shall ensure that all employees have the proper identification credentials prior to entering Hill AFB. CACs are used for identification and network access. CACs are not to be worn off base, photographed or be reproduced in any other manner. The Contractor shall return all credentials to the organization's security managers or Government COR and out-process via the organization's Out-Processing Checklist (if applicable), upon termination from the contract or contract completion.

## RESTRICTED AREA BADGES AND ACCESS TO CONTROLLED AREAS

The Contract Manager or alternate shall complete an AF Form 2586, Unescorted Entry Authorization Certificate, for each employee requiring unescorted entry into controlled areas IAW HAFBI 31-101. The request shall be coordinated through the Government organization's security manager. If approved, employee shall present the AF 2586 to 75 SFS Pass and Identification, building 430 for processing.

Employee will receive AF Form 1199C (commonly known as line badge). Employee must return AF 2586 to the organization’s security manager. The form will be needed when changes to the card are requested and are only issued for one year or shorter based off of expiration of the contract. When the badge is no longer needed, employee shall pick up the AF 2586 from the organization's security manager and take to 75 SFS to turn in. Employee shall return the AF 2586 to the organization's security managers. The controlled area badges shall be surrendered as required in HAFBI 31-101.

## ACCESS TO THE NETWORK

Non-privileged network access may be extended to Contractor employees for email and other network resources. Information System (IS) access will be granted only after all criteria have been met as defined in AFI 17-130. If at any time conduct is deemed inconsistent with IA policies as outlined in AFI 17-130, network access will be denied. Network professional certification requirements are covered by AFMAN 17-1303, Cybersecurity Workforce Improvement Program. Non privileged (IT-III) network access may be extended to Contractor employees for email and other network resources. This access will be granted only after all training criteria (PWS para. [4.19](#_bookmark84)) and systems access requests have been met and may be suspended for cause. All Contractor personnel will complete and sign a formal statement of assigned cybersecurity responsibilities (CDRL A/B/C004).

## COMPUTER CONNECTIVITY

The Government will provide connectivity to the base systems for Government official business in the number of connections required to perform services for this contract. The Contractor shall confine Desktop/Laptop system configurations to the current Government FSDC. Any requests for variations will be submitted to the TOPM and approved by the Government prior to implementation. Contractor equipment shall not be permitted connectivity to the base network before it has been scanned and approved for connection by the 75 ABW/SC.

## VIRTUAL PRIVATE NETWORK (VPN)

The Contractor shall not use Contractor owned equipment for VPN access. IAW AFGM2018-17-02, only Government owned equipment may be used for VPN access.

## FOREIGN OBJECT DAMAGE (FOD) AND DROP OBJECT PREVENTION (DOP)

Contractor personnel who, in the performance of their assigned duties on this contract, work in or travel through areas near operational and production aircraft, engines, munitions, missiles, drones, space systems, support equipment, Aerospace Ground Equipment (AGE), trainers and components, and Contractor personnel operating vehicles and equipment on flight lines, runways, taxiways, parking ramps and in aircraft hangars and maintenance areas are required by Air Force Material Command Instruction (AFMCI) 21-122 to receive FOD/DOP training and to comply with AFMCI 21-122. Contractor personnel shall obtain FOD/DOP awareness and prevention training which is available on the Hill intranet. In the Contractor is unable to access the Hill intranet or that the training is not available, the COR will provide the training video to the Contractor upon written request (e-mail is acceptable) by the Contractor. The

Contractor shall provide completion certificates as proof of training. Certificates shall have the title of the training, name of person who received the training, and date of the training. Contractor shall provide the COR with a copy of the certificate within 10 days of completed training. The Contractor shall maintain copies of the certificates. Training shall be accomplished after contract award. Contractor personnel starting work after task order award shall receive the training within 30 days of commencement of duties IAW task order requirements. Contractor personnel shall receive refresher training by reviewing the initial FOD/DOP awareness and prevention training annually (if applicable).

## GENERAL CONTRACT INFORMATION

The Contractor shall be responsible for work requirements and work in progress at the start of the performance period. All Work Breakdown Structures (WBS) and/or backlogs will be provided by the TOPM to the Contractor after Basic IDIQ award. Although it is the responsibility of the Contractor to recruit, retain, and retrain its employees, the Contractor shall ensure that all employees performing under this contract read, write, speak and understand English at a technical level and proficiency adequate to the nature of the tasks assigned.

## CONTRACTOR PROGRAM MANAGER (CPM)

The Contractor shall provide the CPM who shall be responsible for the overall performance of the work. The CPM shall not be provided any workspace on base. The name of this person and any alternate(s) who shall act for the Contractor when the manager is absent shall be designated in writing to the CO within fifteen (15) days prior to start of contract and any subsequent changes shall be identified within two (2) business days of appointment. The Contractor shall provide telephone numbers of the CPM and alternate(s) where these persons may be contacted at any time. The CPM or alternate shall have full authority to act for the Contractor on matters relating to operation of this contract at Hill AFB via telephone and/or wireless device. The CPM or alternate shall be available to meet on the installation with Government personnel designated by the CO to discuss problem areas or any other contract items.

## CONTRACTOR EMPLOYEES

The Contractor shall employ and maintain a technically trained and experienced work force. The Contractor shall become familiar with and employ new technology in their functional area at no additional cost to Government and without reducing support during the performance period. The Contractor shall maximize the use of cross-utilization of personnel and provide the Government initial and updated lists of Contractor employees’ names, cross-utilization metrics, security clearance status, and position titles. The Contractor shall provide the initial list no later than ten (10) working days prior to contract start date. The Contractor shall provide updated lists as personnel changes occur within two (2) business days. The Government will not be obliged to accept performance by any Contractor employee that the CO has identified to the Contractor as a threat to the health, safety, or general well-being of any other person on the installation. Moreover, the Government will not be obliged to accept performance from any Contractor employee that the CO has identified to the Contractor as a threat to good order and discipline, to Government property, or to any Government operation or mission. The Contractor shall ensure personnel have obtained a favorable local file check or favorable NACI or NACL prior to applying for network access. The Contractor shall not employ any person who is an employee of the United States Government if the employment of that person would create a conflict of interest, unless such person seeks and receives approval according to the DoD 5500.07-R, *Joint Ethics Regulations (JER)*, (17 Nov 2011).

The Contractor is cautioned that off-duty active military personnel hired under this contract may be

subject to permanent change of station, change in duty hours, or deployment. Military Reservists and National Guard members may be subject to recall to active duty. The abrupt absence of these personnel could adversely affect the Contractor's ability to perform. Their absence at any time shall not constitute an excuse for nonperformance under this contract. The Contractor shall not perform this contract in a manner that creates a conflict of interest or the appearance of a conflict of interest vis-à-vis Government employees, e.g., by hiring Government quality assurance evaluators (QAE) to surveil Government contracts, subcontracts, or task orders during their off-duty hours. The Contractor shall ensure that its employees conduct themselves in a professional and courteous manner and that they present a neat and professional image appropriate to their duties to include wearing suitable attire and protective clothing as appropriate. The selection, assignment, reassignment, transfer, supervision, management, and control of Contractor employees in performance of this PWS shall be the responsibility and prerogative of the Contractor; however, the Contractor shall comply with the requirements set forth in this PWS and Hill AFB regulations concerning conduct of employees as referenced herein. Contractor personnel shall comply with directives pertaining to operation of privately owned vehicles on Hill AFB per AFMAN 31- 116\_HILLAFBSUP, *Air Force Motor Vehicle Traffic Supervision*, (17 Dec 2019).

## SECURITY REQUIREMENTS

The Contractor shall provide the CO a comprehensive security plan to cover aspects of the requirements identified in this section. The highest classification for this requirement is Secret. The Contractor shall comply with all security and threat related requirements as specified in DOD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, (18 May 2016); AFI 16-1404 AFMCSUP, *Air Force Information Security Program*, (4 Aug 2020); AFI31-101\_HILLAFBSUP-O, and subsequent instructions, and as directed by the 75 ABW/SC.

## SECURITY CLEARANCE INVESTIGATIONS

Contractor personnel shall be required to obtain and maintain a Secret Security Clearance at contract award and through the duration of the contract. All Contractor personnel must meet the terms of this PWS and must be United States citizens. Applicable directives include DoDM 5200.02\_AFMAN 16-1405 *Personnel Security Program Management* (1 Aug 2018). Per DoDM 5200.02\_AFMAN 16-1405, persons accessing the base network shall, at a minimum, have a completed favorable Local Files Check (not by 75 SFS) or a favorable National Agency Check (NAC, ENTNAC, or NACI) if required by Homeland Security Presidential Directive 12 (HSPD-12), verified through the Joint Personnel Adjudication System (JPAS). IAW AFI 16-1406\_AFMCSUPP, *Air Force Industrial Security Program* (19 Dec 2017) when Contractors require unescorted entry to restricted areas, access to sensitive unclassified information, access to Government automated information systems (AIS) and/or sensitive equipment, not involving access to classified information, the Contractor's personnel security questionnaire is processed by the sponsoring AF activity per DoDM 5200.02\_AFMAN 16-1405. Every user with administrative rights to core network services must possess a completed and favorable National Agency Check (NACIC) and will require National Agency Check with Law and Credit (NACLC). Any costs associated with obtaining the Secret Security Clearance or Single Scope Background Investigation (SSBI) shall be the responsibility of the Contractor.

## NON-DISCLOSURE

The Contractor shall not divulge any information about files, data, processing activities or functions, user ID’s, passwords, or other knowledge that may be gained, to anyone who is not authorized to have access

to such information. The Contractor personnel shall abide by all agency rules, procedures, and standards of conduct. The Contractor personnel shall be in compliance with the Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Contractor Employees. The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement HSPD-12, Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201-2. The Contractor shall insert HSPD-12, Office of Management and Budget (OMB) guidance M-05-24, and FIPS PUB Number 201-2 in all subcontracts when the sub-Contractor is required to have physical access to a federally controlled facility or access to a Federal information system. If the CO determines that a non-disclosure agreement is required from the Contractor or any of its employees, the Contractor agrees to cooperate fully and without delay to execute the disclosure agreement. The Government is not obliged to accept performance from the Contractor or any of its employees who decline to sign or otherwise fail to execute a non-disclosure agreement as requested by the COR or TOPM. (see CDRL A/B/C013)

## TELECOMMUTING

The Government may allow provisions for Contractor employees to telecommute no more than four times per week, during the time periods defined as normal duty hours, outlined in PWS para. [4.17](#_bookmark77).

Telecommuting can be used to increase employee productivity and quality of life, serve as an effective recruitment and retention strategy, accommodate persons with disabilities, and enhance emergency preparedness. The Government reserves the right to assess each position and determine whether telecommuting is appropriate for that position. The Government reserves the right to deny or terminate the use of telecommuting based on eligibility, business needs, or performance. The Government may terminate this agreement within one (1) day written notice to the Contractor. The Contractor employee must complete the approved Office of Personnel Management (OPM) telecommuting training provided at [https://www.telework.gov/training-resources/telework-training/virtual-telework-fundamentals-training-](https://www.telework.gov/training-resources/telework-training/virtual-telework-fundamentals-training-courses/employee-course/index.htm) [courses/employee-course/index.htm](https://www.telework.gov/training-resources/telework-training/virtual-telework-fundamentals-training-courses/employee-course/index.htm) before becoming eligible. The Contractor shall provide a written plan to the Government outlining the necessary steps to ensure security of Government property and information. The Contractor employees are not authorized to work with classified information away from the traditional worksite unless specifically authorized by the Government. The Contractor shall provide the Government expectations and performance evaluation factors prior to telecommuting being authorized. Telecommuting must be performed using GFE only. If approved, the Government will provide the appropriate GFE. It is the responsibility of the Contractor to ensure the GFE is patched and remains compliant to Government standards monthly. Upon termination of the Contractor employee or contract, it is the responsibility of the Contractor to return all GFE as outline in [Appendix E](#_bookmark107). The Contract employee may not start exercising telecommuting until all steps necessary to establish network connectivity have been established at the place where work will be performed. Any requests for variations to this section will be submitted to the COR and approved by the Government prior to implementation.

## FREEDOM OF INFORMATION ACT (FOIA) / PRIVACY ACT

All official Government records affected by this contract are subject to the provisions of the FOIA and Privacy Act. Any request received by the Contractor for access/release of information from these records to the public (including Government/Contractor employees acting as private citizens), whether oral or in writing, shall be immediately brought to the attention of the CO for forwarding to the Base FOIA Manager to ensure proper processing and compliance with the Act.

## PHYSICAL SECURITY

The Contractor shall be responsible for safeguarding all Government property provided for Contractor use. At the close of each work period, Government facilities, property, and materials shall be secured. It will be the Contractors responsibility to safeguard facilities in which they are working.

The Contractor shall protect government facilities and property to prevent damage during the period of time they are on site. The Contractor shall report promptly to the CO all available facts relating to each instance of damage to Government facilities or property.

The Contractor understands that any Contractor employee may be summarily and immediately removed from or denied access to any Government property, facility, and installation at the sole discretion of competent Government authority if that authority determines such action is necessary to protect or preserve Government property, safety and security, or to maintain good order and discipline. With approval from the CO, the COR will verbally report such actions to the Contractor within 2 hours of the situation and provide a written statement notification to the Contractor within 24 hours including reasons for the action. It is the responsibility of the Contractor to replace any of its employees that are removed pursuant to the section where replacement is necessary to ensure full, timely, and complete contract performance.

## KEY CONTROL METHODS

The Contractor shall establish and implement methods of ensuring that all keys or vindicator cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. Keys issued to the Contractor by the Government will not be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan (PWS para. [2.4.1](#_bookmark39)).

Such procedures shall include turn-in of any issued keys by personnel that no longer require access to locked areas.

## KEY LOSS / DUPLICATION

The Contractor shall immediately report the occurrences of a lost or duplicate key/vindicator card to the CO.

## REPLACEMENT

In the event that keys, other than master keys, are lost or duplicated, the Contractor shall, upon written direction of the CO, re-key or replace the affected lock or locks at Contractor’s expense; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

## KEY CONTROL

The Contractor shall prohibit the use of Government-issued keys or vindicator cards by any persons other than the Contractor’s employees to whom the keys or vindicator cards were assigned. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor’s employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the CO and/or TOPM.

## HOURS OF OPERATION

## NORMAL HOURS OF OPERATION

The Contractor shall perform the services required under this contract during Core Business Hours, Monday through Friday, except Federal holidays, during the core duty hours of 0600-1800, except as noted in individual workload data. Hours of support may vary over the course of the contract. The Contractor shall optimize personnel staffing and manning to match the individual workload requirements and performance criteria between these hours.

## RECOGNIZED HOLIDAYS

The Contractor is not required to provide service on the following days:

* New Year’s Day
* Martin Luther King Day
* Presidents Day
* Memorial Day
* Juneteenth National Independence Day
* Independence Day
* Labor Day
* Columbus Day
* Veterans Day
* Thanksgiving Day
* Christmas Day

If the holiday falls on Saturday, it is observed on Friday. If the holiday falls on a Sunday, it is observed on Monday. The Contractor may be required to observe all energy days and/or other down days as directed by AFMC, Base, and/or OO-ALC Commander at no cost to the Government.

## EMERGENCY SITUATIONS

The CO/COR shall notify the Contractor when emergency situations exist (e.g., natural disasters, weather- related situations, base closures), which may cause changes to installation operations tempo. The Contractor PM shall communicate to the Contractor employees the conditions and expectations of the Contractor during emergency situations.

## CONTINGENCY SERVICES

On occasion, services may be required to support an activation or exercise of contingency plans outside the normal duty hours described above. The Contractor’s responsibilities for emergency support will be defined in the workload data. This is an unplanned event that would require staff that would need to be able to communicate and perform services for Base infrastructure. Refer to PWS para [1.2](#_bookmark2).

## RECORDS

The Contractor shall be responsible for creating, maintaining, and disposing of only those Government required records that are specifically cited in this PWS or required by the provisions of a mandatory directive listed in [Appendix A.](#_bookmark102) If requested by the Government, the Contractor shall provide the original record or a reproducible copy of any such record within five (5) working days of receipt of the request.

All official records (regardless of media) as defined in 44 U.S.C. Part 3301/AFI 33-322 are the property of the U.S. Government and shall remain so upon termination or completion of this contract.

## GOVERNMENT OBSERVATIONS

Government personnel, other than the CO and CORs, may from time to time, with CO coordination, observe Contractor operations. However, these personnel may not interfere with Contractor performance or make any changes to the contract. Any observations should be reported to the COR.

## TRAINING

The Contractor is responsible for maintaining currency of all licenses, certifications and qualifications associated with the applicable labor categories. All training records for personnel must be maintained by the Contractor and be made available for Government inspection upon request. The Government’s intent with this requirement is to ensure that personnel providing service are qualified by continually attaining required training, and currently licensed and certified for their assigned tasks. The minimum continuous learning requirement for certifications included in DoD 8570.01-M is 40 hours annually or 120 hours over a three-year period. A training plan shall be submitted addressing an education and training program for 8570 certification, continuous learning, evolving technologies, information security, Cloud services, and best practices such as but not limited to Information Technology Infrastructure Library (ITIL), secure coding, test driven development (TDD), code quality, and agile software development (see CDRL A/B/C002)

## INFORMATION ASSURANCE

Before becoming an AF network user, an individual must be trained and obtain certification of completion of training. This process of training ensures that every AF network user is trained and aware of the basic principles of network security and their role in Information Assurance (IA) and Operational Security (OPSEC). Contractor personnel will be required to complete the IA and OPSEC training outlined in PWS para. [4.23](#_bookmark87). Also refer to PWS para. [1.5](#_bookmark15) for additional OPSEC guidance.

## CONTINUING EDUCATION, TRAINING, AND CERTIFICATION

Specific access requirements may require utilization of Computer Based Trainings (CBT). Irrespective of whether the Government makes training available to the Contractor and its employees, the Contractor retains full responsibility for ensuring that its employees are always adequately and appropriately trained to carry out their duties as assigned by the Contractor under this contract. Evolving technologies may necessitate the continuing education of the Contractor’s employees. Such education will be funded by the Contractor and will be performed outside of contract hours IAW AFMAN 17-1303 paragraph 3.4.4. The Contractor shall also fund any subscription service necessary for the continuing education of its employees. The Contractor shall ensure compliance with AFMAN 17-1303 paragraph 3.2.12.2.2.1.

## GOVERNMENT PROVIDED TRAINING

The Government may provide training as required and as approved by the COR or Functional Director, including but not limited to the topics listed below. All training must be approved by the Functional Director or COR prior to attendance. Most, but not all, of the training is provided via CBT.

* Cyber Awareness Challenge
* Anti-Terrorism, Suicide Prevention, and Safety
* SECDEF OPSEC Campaign
* AFMC Fire Safety and Prevention Training/Refresher
* Initial Fire Safety and Prevention
* 75ABW/SC Unit Emergency Management
* 75ABW/SC Operational Risk Management
* Air Force Facility Energy Awareness Training
* Environmental Awareness
* AFSO21 Awareness
* Commanders Safe Site Challenge
* Introduction to the Voluntary Protection Program (VPP)
* 75 ABW/SC Annual Security
* Force Protection
* Human Relations
* Notification and Federal Employee Anti-discrimination and Retaliation (No FEAR)
* Religious Freedom Training
* Suicide Prevention Training
* Air Force Inspection System (AFIS)

## FULFILLING MISSION REQUIREMENTS

The Contractor shall plan for and respond to mission requirements in the event of mobilization, terrorism, natural disaster, labor disputes, etc. Upon notification by the CO of the requirement to support these operations the Contractor shall provide documentation for all hours worked.

## PUBLICATIONS

Compliance with all publications, regulations and operating instructions provided by the Government is required when they pertain to the procedures for materials expediting herein and where the Contractor is authorized by this PWS to accomplish the work specified in the publication, regulation or operating instructions. The publications prescribe USAF policies, use of materials, procedures and processes applicable to the work requirements. The Contractor is required to acquire and work according to the latest version of the publication. See [Appendix A](#_bookmark102) for a listing of all applicable guidance and directives.

## INTERNAL OPERATING PROCEDURES

The Contractor shall follow all established local operating procedures listed herein for internal circulation control, protection of resources and regulation of entry into AF controlled/restricted areas during normal, simulated and actual emergency operations and any additional direction by the 75 ABW/SC leadership.

## CONSERVATION OF UTILITIES

The Contractor shall instruct employees in utilities conservation practices. The Contractor shall be responsible for operating under conditions which prevent the waste of utilities, which include the following:

* Lights shall be used only in areas where and when work is actually being performed.
* Mechanical equipment controls for heating, ventilation and air conditioning systems shall not be adjusted by the Contractor or by the Contractor employees unless authorized.
* Water faucets or valves shall be turned off after the required use has been accomplished.
* Government telephones shall be used only for official Government business.

## ENVIRONMENTAL PROTECTION AND SAFETY

The Contractor shall be knowledgeable of and comply with all applicable federal, state, and local laws, regulations, and requirements regarding environmental protection. In the event environmental laws or regulations change during the term of this contract, the Contractor is required to comply as such laws come into effect.

Hill AFB has adopted the Voluntary Protection Program (VPP) as recognized by Occupation Safety Health Association (OSHA) and IAW AFI 91-202 *The US Air Force Mishap Prevention Program* (12 Mar 2020) and AFI91-202\_AFMCSUP *Air Force Instruction 91-202 Air Force Materiel Command Supplement to The US Air Force Mishap Prevention Program* (17 May 2017). Consequently, VPP impacts all “applicable Contractors” operating on Air Force Installations. It is the Contractor’s responsibility to ensure its employees and managers have a comprehensive understanding of VPP as well as full compliance with OSHA requirements. Detailed information on VPP is available on the OSHA website (<http://www.osha.gov/dcsp/vpp/index.html>). Contractors, whether regularly involved in routine site operations or engaged in temporary projects such as construction or repair, must follow the safety and health rules of the installation or VPP site.

VPP requirements apply to Contractors whose employees work more than 1,000 hours per quarter. The Contractor shall flow down these requirements to all Sub-Contractors who qualify as applicable Contractors under this contract.

Contractors are required to provide from their OSHA 300 information the Total Case Incident Rate/Days Away Restricted or Transferred (TCIR/DART) rate by 15 January of each year to the COR for submission as part of the installation’s annual OSHA VPP self-evaluation report described in Appendix A of OHSA CSP 03-01-005. Reference [Appendix A](#_bookmark102) for the guidance listed above.

## ENVIRONMENTAL CONTROLS

## COMPLIANCE WITH LAWS AND REGULATIONS

The Contractor shall be knowledgeable of and comply with all applicable Federal, State, and Local laws, regulations, and requirements regarding environmental protection. In the event environmental laws/regulations change during the term of this contract, the Contractor is required to comply as such laws come into effect.

## NOTIFICATION OF ENVIRONMENTAL SPILLS

If the Contractor spills or releases any substance contained in 40 CFR 302 into the environment, the Contractor or its agent shall immediately report the incident to Hill AFB Fire Dept. at 777-1911. The liability for the spill or release of such substance's rests solely with the Contractor and its agent.

## MATERIAL STORAGE AND USE

The Contractor shall follow manufacturer’s guidelines and professional recommendations for control of humidity, temperature, cleanliness, and materials handling. This includes hazardous materials.

## PARTICIPATION IN GOVERNMENT ACTIVITIES

Contractor shall participate in various Government initiated activities such as Continuous Process Improvement initiatives, process identification and management, various meetings, safety programs related to work center hazards/Voluntary Protection Program (VPP), and similar activities as requested by the Government.

## TRANSITION PERIOD

**Estimated to be 30 days**. The Contractor shall ensure a seamless transition. The Contractor’s Transition Plan shall demonstrate how personnel, materials and equipment will be utilized through the transition period and a method to ensure seamless performance issues to include phase-in timelines. The plan shall also include the number, position titles, and qualifications of personnel to be on site for the transition period. The Contractor shall begin the transition and provide a written Transition Plan as required by CDRL. (see CDRL A/B/C005)

The purpose of the transition plan is to demonstrate how the Contractor shall meet the intent of the following:

* Observe work accomplished by current employees and become thoroughly familiar with work requirements
* Complete personnel requirements (work force), including the hiring of personnel to assure satisfactory performance. Soliciting Government or Contractor personnel for employment during their duty hours is prohibited.
* Complete Security requirements as identified by the PWS para. [4.10](#_bookmark67) and para. [4.11](#_bookmark68)
* Complete documentation and requests during the orientation period for all applicable security clearances (NACIs and NACLC), or acceptable local files checks
* Complete the development of necessary work plans and procedures based on PWS requirements
* Conduct and Complete GFE inventory IAW PWS para. 3.5
* The Contractor will be allowed access to the facilities to familiarize supervisors, key personnel and staff with equipment, reporting, work scheduling and procedures. However, such access will not interfere with the production efforts of current work force. To preclude such interference, arrangements for access to the Government facilities will be made with the COR and/or TOPM.

## PHASE-OUT PERIOD

If there is a change in Contractor, the incumbent Contractor shall provide familiarization and allow the follow-on Contractor to observe monthly operations, facilities, work, equipment locations and reporting procedures on a non-interference basis. The Contractor’s Phase-Out Period Plan shall demonstrate how personnel, materials, equipment, programs and projects will be phased out and turned over to the incumbent Contractor. The plan shall also include the number, position titles, and qualifications of personnel to be on site for the transition period (see CDRL A/B/C012).

Copies of all new data and software, developed data and software, changed data and software, data and software improvements or data and software fixes shall be given to each TOPM prior to end of task order or contract. (see CDRL A/B/C005, A/B/C012)

The Government reserves the right to conduct site visits in Contractor operated facilities in conjunction with the solicitation of offers for the follow-on contract. In the event the follow-on contract is awarded to other than the incumbent, the incumbent Contractor shall cooperate to the extent required to permit an orderly change over to the successful Contractor.

The incumbent Contractor and TOPM shall ensure network access is removed for those employees who do not intend to work for the new Contractor and process a Contractor Out-Processing Checklist.

## SYSTEM FOR AWARD MANAGEMENT (SAM) REPORTING REQUIREMENT

The Contractor shall report ALL Contractor labor hours (including Sub-Contractor labor hours) required for performance of services provided under this contract for the United States AF via a secure data collection site. The Contractor is required to completely fill in all required data fields using the following web address: [https://sam.gov.](https://sam.gov/) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30.

While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2020.

The Contractor may direct questions to the help desk at: [https://fsd.gov/.](https://fsd.gov/)

U.S. calls: 866-606-8220 / International calls: +1 334-206-7828 / DSN: 94-866-606-8220. In preparation of FSD assistance:

* Be sure to provide as much detail as you can.
* Ensure you promptly respond to any follow-up questions from the agent.
* Tickets are closed in 3 days if the requestor does not respond.

## SECTION 508 OF THE REHABILITATION ACT

The Contractor shall meet the requirements of the Access Board’s regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use IT to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use IT to access the information on an equal footing with people who do not have disabilities.

# APPENDICES

**APPENDIX A. GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

|  |
| --- |
| **REFERENCES AND SUPPORTING INFORMATION** |
| 29 CFR § 1910.1200 Occupational Health and Safety Administration (OSHA) Part 1910 Standard 1200 Hazard Communication (25 May 2012) |
| 36 CFR § 1194 Electronic and Information Technology Accessibility Standards (01 July 2011) |
| 36 CFR § 1194.22 Web-Based Intranet and Internet Information and Applications (01 July 2011) |
| 40 CFR § 302 Designation, Reportable Quantities, and Notification (01 July 2019) |
| 44 U.S.C. § 3301 Title 44-Public Printing and Documents §3301. Definition of records (05 Oct 2020) |
| 48 CFR – Federal Acquisition Regulation (FAR) VOL. 1 Federal Acquisition Regulation, Volume 1, Parts 1 to 51 (01 Oct 2020) |
| 48 CFR § 45.5 Federal Acquisition Regulation, Part 45, Subpart 45.5 - Support Government Property Administration (02 Oct 2020) |
| 48 CFR § 52.233-1 FAR Part 52, Section 233-1, Disputes (May 2014) |
| 48 CFR § 52.246-4 FAR Part 52, Section 246-4, Inspection of Services-Fixed-Price (Aug 1996) |
| 48 CFR § 252.245-7002 FAR Part 252, Section 245-7002- Reporting Loss of Government Property (Dec 2017) |
| 48 CFR § 252.245-7003 FAR Part 252, Section 245-7003 - Contractor Property Management System Administration (Apr 2012) |
| 48 CFR § 252.245-7004 FAR Part 252, Section 245-7004 - Reporting, Reutilization, And Disposal (Dec 2017) |
| 5 U.S.C. § 552 Freedom of Information Act (FOIA), (4 July 1966, Amended 2016) |
| 5 U.S.C. § 552a Privacy Act of 1974, Records maintained on individuals (05 Oct 2020) |
| 29 U.S.C. § 794d; SEC. 508 Public Law 105-220, Section 508, Federal Electronic and Information Technology (Updated 06 August 2015) |
| AFGM 2018-17-02 Air Force Guidance Memorandum Establishing Enterprise Information Technology Management (31 May 2018) |
| AFI 17-201 Command and Control (C2) for Cyberspace Operations (04 Mar 2014) |
| AFI 16-1404\_AFMCSUPP Air Force Material Command Information Security Program (04 Aug 2020) |
| AFI 17-101 Risk Management Framework (RMF) for Air Force Information Technology (IT) (05 Feb 2020) |
| AFI 17-130 Cybersecurity Program Management (12 Feb 2020) |

|  |
| --- |
| AFI 17-140 Architecting (28 June 2018) |
| DoDI 4140.67 DoD Counterfeit Prevention Policy (Incorporating Change 3, March 6, 2020) |
| DoDI 4140.66 Registration and End-Use Monitoring of Defense Articles and/or Defense Services ( Incorporating Change 1, May 24, 2017) |
| AFI 33-322 Records Management and Information Governance Program (22 Mar 2020) |
| AFI 35-107 Public Web and Social Communication (15 Mar 2017) |
| AFI 64-106 Contract Labor Relations Activities (03 Oct 2019) |
| AFI 91-202 The US Air Force Mishap Prevention Program (11 Mar 2020) |
| AFI 91-202\_AFMCSUP The US Air Force Mishap Prevention Program (16 May 2017) |
| AFI 10-701 Operations Security (OPSEC) (Incorporating Change 1, 09 June 2020) |
| DODM 5220.22 Vol 2 National Industrial Security Program: Industrial Security Procedures for Government Activities *(18 Aug 2018)* |
| AFMAN 17-1203 Information Technology (IT) Asset Management (ITAM) (18 May 2018) |
| AFMAN 17-1301 Computer Security (COMPUSEC) (12 Feb 2020) |
| AFMAN 17-1303 Air Force Cybersecurity Workforce Improvement Program (12 May 2020) |
| AFI 63-101\_20-101 Integrated Life Cycle Management (30 June 2020) |
| AFMAN 31-116\_HILLAFBSUP Air Force Motor Vehicle Traffic Supervision (17 Dec 2019) |
| DoDI 5200.39 Critical Program Information (CPI) Identification and Protection Within Research,  Development, Test, and Evaluation (RDT&E) (Incorporating Change 3, Effective October 1, 2020) |
| CNSSP 22 Cybersecurity Risk Management (August 2016) |
| AFI21-101\_HILLAFBSUP-HILAFBGM21-04 Foreign Object Damage (FOD) and Dropped Object Awareness and Prevention Program *(20 Jul 2009*) |
| AFPD 10-7 Information Operations (04 Aug 2014) |
| AFPD 17-1 Information Dominance Governance and Management (11 Apr 2016) |
| DAFPD 17-2 Cyber Warfare Operations (26 Oct 2020) |
| CNSSI 1253 Security Categorization and Control Selection for National Security Systems (27 Mar 2014) |
| CNSSI 1253F, Attachment 6 CNSS Security Categorization and Control Selection for National Security Systems Attachment 6 to Appendix F (23 April 2015) |
| CSP 03-01-005 Occupational Safety and Health Administration Voluntary Protection Programs Policies and Procedures Manual (30 Jan 2020) |
| DoDM 5205.02-M DoD Operations Security (OPSEC) Program Manual (Incorporating Change 1, 26 Apr 2018) |

|  |
| --- |
| DOD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) (Incorporating Change 2, 18 May 2016) |
| DOD 5500.07-R Joint Ethics Regulations (JER) (Change 7, 17 Nov 2011) |
| DoD 8570.01-M Information Assurance Workforce Improvement Program (07 Mar 2019) |
| DODD 5205.02E DoD Operations Security (OPSEC) Program (Incorporating Change 2, 20 Aug 2020) |
| DoDD 8000.01 Management of the Department of Defense Information Enterprise (DoD IE) (Incorporating Change 1, 27 July 2017) |
| DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) (Certified Current 23 Apr 2007) |
| DoDD 8140.01 Cyberspace Workforce Management (5 Oct 2020) |
| DoDI 1100.22 Policy and Procedures for Determining Workforce Mix (Change 1, 01 Dec 2017) |
| DoDI 4161.02 Accountability and Management of Government Contract Property (Incorporating Change 2, 31 Aug 2018) |
| DoDI 5200.02 DoD Personnel Security Program (PSP) (Incorporating Change 3, Effective 24 Sept 2020) |
| DoDI 8410.02 NetOps for the Global Information Grid (GIG) (19 Dec 2008) |
| DoDI 8500.01 Cybersecurity (Incorporating Change 1, 7 Oct 2019) |
| DoDI 8500.01 Enclosure 3 Cybersecurity – Risk Management (14 March 2014) |
| DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) (Incorporating Change 3, 29 Dec 2020) |
| DoDI 8520.03 Identity Authentication for Information Systems (Incorporating Change 1, 27 July 2017) |
| DoDI 8530.01 Cybersecurity Activities Support to DoD Information Network Operations (Incorporating Change 1, 25 July 2017) |
| DoDI 8580.02 Security of Individually Identifiable Health Information in DoD Health Care Programs (12 Aug 2015) |
| DoDM 5200.02 Procedures for the DoD Personnel Security Program (PSP) (Change 01, 29 Oct 2020) |
| DoDM 5200.02\_AFMAN 16-1405 Air Force Personnel Security Program (01 Aug 2018) |
| DoDM5200.08V3\_AFMAN31-101V3 Physical Security Program: Access to DoD Installations (18 Sep 2020) |
| AFI 33-393 Electronic and Information Technology Accessible to Individuals with Disabilities, Section 508 (3 Jul 2019) |

|  |
| --- |
| FIPS PUB 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors (Aug 2013) |
| FIPS 199 Standards for Security Categorization of Federal Information and Information Systems (Feb 2004) |
| AFI31-101\_AFMCSUP\_HILLAFBSUP-0 Integrated Defense (01 Dec 2020) (CUI) |
| HAFBI 13-213\_HILLAFBSUP Airfield Driving (Certified Current 21 Mar 2021) |
| HILLAFBI 32-103 Space Management (Certified Current 07 Feb 2020) |
| HSPD-12 Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (03 Apr 2020) |
| NIST 800-30 Guide for Conducting Risk Assessments Revision 1 (16 Jan 2020) |
| NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach **(**Dec 2018) |
| NIST SP 800-53 Revision 5 Security and Privacy Controls for Federal Information Systems and Organizations (Sep 2020) |
| NIST SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans Revision 4 (16 Jan 2020) |
| NSDD298 National Operations Security Program (22 Jan 1988) |
| OMB M-05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors Incorporating Change 5  (8 Oct 2013) |

|  |
| --- |
| **FORMS:** |
| DD Form 1172-2 Application for Identification Card/DEERS Enrollment (Apr 2020) |
| AF IMT 2586 Unescorted Entry Authorization Certificate (13 July 2020) |
| AF Forms 1199D USAF Restricted Area Badge (Blue) |
| DD Form 1423-2 Contract Data Requirements List (Aug 1996) |
| DD Form 254 Department of Defense Contract Security Classification Specification (Apr 2018) |
| DD Form 254 Instructions for Department of Defense Form 254 (Apr 2018) |
| DD Form 2875 System Authorization Access Request (SAAR) (Aug 2009) |
| AFMC Form 496 Application for AFMC Identification Card (14 Mar 2003) |

**APPENDIX B. GLOSSARY OF ACRONYMS**

|  |  |
| --- | --- |
| **ACRONYM** | **DEFINITION** |
| A&A | Assess & Authorize |
| ABW | Air Base Wing |
| ACAS | Assured Compliance Assessment Solution |
| ACAT | Acquisition Category |
| AD | Active Directory |
| ADPE | Automatic Data Processing Equipment |
| AF | Air Force |
| AFB | Air Force Base |
| AFCERT | Air Force Computer Emergency Response Team |
| AFI | Air Force Instruction |
| AFIS | Air Force Inspection System |
| AFMAN | Air Force Manual |
| AFMC | Air Force Materiel Command |
| AFMCI | Air Force Materiel Command Instruction |
| AFMCSUP | Air Force Material Command Supplement |
| AFPD | Air Force Policy Directive |
| AFSPC | Air Force Space Command |
| AGE | Aerospace Ground Equipment |
| AIS | Automated Information Systems |
| AIT | Automated Information Technology |
| AJAX | Asynchronous Java Script Extensible Markup Language |
| ALC | Air Logistics Center |
| AMXG | Aircraft Maintenance Group |
| AO | Authorizing Official |
| APCP | (Non-Destructive Inspection) Automated Process Control Program |
| ASSIST | Automated System Security Incident Support Team |
| AT | Anti-Tamper |
| ATO | Authorized to Operate |

|  |  |
| --- | --- |
| C&A | Certification and Accreditation |
| CAB | Change Advisory Board |
| CAC | Common Access Card |
| CBT | Computer Based Training |
| CCSP | Cisco Certified Security Professional |
| CFP | Communications Focal Point |
| CFR | Code of Federal Regulations |
| CI | Critical Information |
| CIIL(s) | Critical Information and Indicator Listing(s) |
| CIO | Chief Information Officer |
| CLIN | Contract Line-Item Number |
| CMXG | Commodities Maintenance Group |
| CNSSP | Committee on National Security Systems Policy |
| CO | Contracting Officer |
| COMPUSEC | Computer Security |
| CONUS | Continental United States |
| COOP | Continuity of Operations |
| COR | Contracting Officer’s Representative |
| COTS | Commercial Off-the-Shelf |
| CPI | Critical Program Information |
| CPM | Contractor Program Manager |
| CPU | Central Processing Unit |
| CSS | Cascading Style Sheets |
| CTP | Community Technology Preview |
| CUI | Controlled Unclassified Information |
| DAA | Designated Accrediting Authority |
| DART | Days Away, Restricted, or Transferred |
| DBA | Database Administrator |
| DBMS | Database Management System |
| DCAST | Depot Cost and Schedule Tool |

|  |  |
| --- | --- |
| DCMA | Defense Contract Management Agency |
| DD Form | Department of Defense Form |
| DDSS | DMAPS Data Storage System |
| DIFMS | Defense Industrial Finance Management System |
| DISA | Defense Information Systems Agency |
| DIMAPS | Digital Instructional Materials Acquisition Policies for States |
| DMAPS | Depot Maintenance Accounting and Production System |
| DoD | Department of Defense |
| DoDD | Department of Defense Directive |
| DoDI | Department of Defense Instruction |
| DOP | Drop / Dropped Object Prevention |
| DR | Disaster Recovery |
| DSN | Defense Switched Network |
| eMASS | Enterprise Mission Assurance Support Service |
| EMC2 | Emergency Management Command and Control |
| ENTNAC | ENTrance National Agency Check |
| ESM | Enterprise Systems Management |
| ETL | Engineering Technical Letter |
| EVM | Earned Value Metrics; Earned Value Management |
| EXPRESS | Execution and Prioritization of Repair Support System |
| FAR | Federal Acquisition Regulation |
| FEN | Field Engineering Notices |
| FIPS | Federal Information Processing Standards |
| FIPS PUB | Federal Information Processing Standards Publication |
| FOD | Foreign Object Damage |
| FOIA | Freedom of Information Act |
| FOUO | For Official Use Only |
| FSD | Federal Service Desk |
| FSDC | Federal Standard Desktop Configuration |
| FY | Fiscal Year |

|  |  |
| --- | --- |
| GCSS | Global Combat Support Systems |
| GFE | Government Furnished Equipment |
| GFP | Government Furnished Property |
| GIF | Graphics Interchange Markup |
| GOTS | Government Off-the-Shelf |
| GPO | Group Policy Objects |
| HEDC | Hill Enterprise Data Center |
| HILLAFBSUP | Hill Air Force Base Supplement |
| HSPD | Homeland Security Presidential Directive |
| HTML | Hypertext Markup Language |
| HUM | Heads Up Messages |
| IA | Information Assurance |
| IAA | Information Assurance Awareness |
| IAM | Information Assurance Management |
| IASAE | Information Assurance System Architect and Engineer |
| IAT | Information Assurance Technical |
| IAW | In Accordance With |
| IDIQ | Indefinite Delivery Indefinite Quantity |
| IHS | Information Handling Services |
| IIS | Internet Information Services |
| INFOCON | Information Condition |
| IP | Internet Protocol; Information Protection |
| IPV/POU | Industrial Product Support Vendor/Point of Use |
| IIS | Internet Information Services |
| IS | Information System |
| IT | Information Technology |
| ITIL | (formerly known as) Information Technology Infrastructure Library; ITIL v.4 is now only knowns as ITIL |
| J2EE | Java 2 Platform Enterprise Edition |
| JDBC | Java Database Connectivity |
| JER | Joint Ethics Regulation |

|  |  |
| --- | --- |
| JON | Job Order Number |
| JPAS | Joint Personnel Adjudication System |
| JPEG | Joint Photographic Experts Group |
| JSON | JavaScript Object Notation |
| JSP | Java Server Pages |
| LDAP | Lightweight Directory Access Protocol |
| LDD | Loss, Damage, or Destruction |
| MRO | Maintenance, Repair, and Overhaul |
| MS | Microsoft |
| MS-DOS | Microsoft Disk Operation System |
| MSS | Mission Support Squadron |
| MVC | Model View Controller |
| NAC | National Agency Check |
| NACI | National Agency Check with Inquiries |
| NACLC | National Agency Check with Law and Credit |
| NAS | Network Attached Storage |
| NC | Non-compliant |
| NDA | Non-Disclosure Agreement |
| NISPOM | National Industrial Security Program Operating Manual |
| No FEAR | Notification and Federal Employee Anti-Discrimination and Retaliation |
| NOTAM | Notices to Airmen |
| NSDD | National Security Decision Directive |
| OC | Oklahoma City Air Logistics Center (Tinker AFB) |
| OC-ALC | Oklahoma City Air Logistics Center |
| OID | Oracle Internet Directory |
| OLAP | Online Analytical Processing |
| OLTP | Online Transaction Processing |
| OM | OPSEC Measures |
| OMB | Office of Management and Budget |
| OMC | Post Office / Official Mail Center |

|  |  |
| --- | --- |
| OO | Ogden Air Logistics Complex (Hill AFB) |
| OO-ALC | Ogden Air Logistics Complex |
| OPM | Office of Personnel Management |
| OPR | Office of Primary Responsibility |
| OPSEC | Operations Security; Operational Security |
| OS | Operating System(s) |
| OSHA | Occupational Safety and Health Administration; Occupational Safety and Health Act |
| PERL | General Purpose Program Language |
| PHP | Hypertext Preprocessor |
| PII | Personally Identifiable Information (PII) |
| PIT | Platform Information Technology |
| PIV | Personal Identity Verification |
| PM | Program Manager |
| PNG | Portable Network Graphics |
| PNSSRS | Part Number Supply Support Request System |
| POA&M | Plan of Action and Milestones |
| POC | Point(s) of Contact |
| PODDS | Process Order Development and Deployment System |
| PPS | Ports, Protocols and Services |
| PUB | Publication |
| PWS | Performance Work Statement |
| QAE | Quality Assurance Evaluators |
| QAPM | Quality Assurance and Productivity Measurements |
| RAC | Real Application Clusters |
| RCC | Resource Cost Center |
| RFP | Request for Proposal |
| RMAN | Recovery Manager |
| RMF | Risk Management Framework |
| RPA | Request for Personnel Action |
| RTM | Release to Manufacturing |

|  |  |
| --- | --- |
| SAN | Storage Area Network |
| SAP | Security Assessment Plan |
| SAR | Security Assessment Report |
| SDCR | Software Deployment Change Requirements |
| SDD | System Design Document |
| SFS | Security Forces Squadron |
| SLIN | Sub CLIN |
| SMS | Systems Management Server |
| SQL | Structured Query Language |
| SRB | Software Review Board |
| SRD | System Requirements Document |
| SS | Service Summary |
| SSAA | System Security Accreditation Agreement |
| SSBI | Single Scope Background Investigation |
| SSIS | Structured Query Language Server Integration Services |
| SSO | Single Sign-On |
| SSP | System Security Plan |
| STIGs | Security Technical Implementation Guides |
| STP | Software Test Procedures |
| SVG | Scalable Vector Graphics |
| SwA | Software Assurance |
| TCIR | Total Case Incident Rate |
| TCNO | Time Compliance Network Orders |
| TCTO | Time Compliance Technical Order |
| TRB | Technical Review Board |
| UNIX | Uniplexed Information and Computing Service |
| US | United States |
| USAF | United States Air Force |
| VB | Visual Basic |
| VBA | Visual Basic for Applications |

|  |  |
| --- | --- |
| VBS | Visual Basic Script |
| VM | Virtual Machine |
| VOIP | Voice Over Internet Protocol |
| VPN | Virtual Private Network |
| VPP | Voluntary Protection Program |
| WAR | Weekly Activity Report |
| WBS | Work Breakdown Structure(s) |
| WR | Warner-Robins Air Force Base |
| WR-ALC | Warner-Robins Air Logistics Center |
| WSUS | Windows Server Update Services |
| XML | Extensible Markup Language |

**APPENDIX C. SAFETY REQUIREMENTS**

### Safety, Health and Fire Protection Requirements

* The Contractor shall comply with all applicable State and/or Federal Occupational Safety and Health (OSHA) Standards, Fire Protection Standards and Environmental Protection Agency Requirements. Also, the Contractor shall comply with the stated or referenced Air Force safety requirements/clauses of the contract, safety provisions of technical publications listed within the PWS and take any additional immediate precautions as the Contracting Officer may reasonably require for safety and mishap prevention purposes.
* The Contractor shall initiate and maintain a safety, health and fire program for the protection of DOD property and personnel, which will comply, with the Safety, Health and Fire Protection requirements of this contract.
* The Contractor shall provide each employee an initial indoctrination and such continued training to enable performance of work in a safe manner.
* The Contractor shall include a clause in all subcontracts requiring subcontractors to comply with the safety provisions of this contract, as applicable.
* Work referred to under this contract shall in no way require persons to work in surroundings or working conditions that are unsafe or dangerous to their health.
* The Contractor shall be subject to the physical demands consisting of standing, walking, and lifting light loads (up to 50 pounds), walking to and visiting various buildings, including production areas.
* The Contractor shall provide and enforce the use of personal protective equipment in those tasks and areas so designated.
* The Contractor is responsible for maintaining copies of Material Safety Data Sheets (MSDS), IAW OSHA Standard, 29 CFR 1910.1200, for chemicals/materials connected with this contract. The Contractor shall comply with Federal, State, and local standards concerning waste minimization, hazardous waste handling and correct documentation for the disposition of accumulated wastes.

### Mishap Reporting and Investigation

* The Contractor shall report within one hour to the 75/ABW Safety Office and a designated Government Representative (GR) all available facts relating to mishaps.
* In the event of a mishap the Contractor shall take reasonable and prudent action to establish control of the mishap scene, prevent further damage to property/injuries and preserve evidence until released by the 75/ABW Safety Office. Such release may be accomplished through the designated GR.
* If the government elects to investigate the mishap, the Contractor shall cooperate fully and assist the government personnel until the investigation is completed.
* The Contractor shall include a clause in each applicable subcontract requiring the Sub- Contractor’s cooperation and help in mishap reporting and investigation.

### Vehicle Operations

* Contractor is responsible to ensure the safe operating condition of all vehicles operated by Contractor personnel on Hill Air Force Base. Vehicle operators will obey all Base and State traffic laws/regulations.
* Contractor vehicles operators shall possess a valid state driver’s license and if applicable a government vehicle operator’s license. All vehicle operators shall be trained and certified as operators for each type of vehicle they operate and complete applicable traffic safety training courses prior to operating a vehicle on the flight line. Vehicle operator training is the responsibility of the Contractor.
* All vehicles and equipment shall be inspected and maintained in good operating condition and kept in a clean and neat appearance.

### Housekeeping

* Power cables and cords shall not be strung carelessly across floors. Serious injuries may result by tripping over power cords and cables.
* Trash and litter shall not be allowed to accumulate on the floor. Hazardous waste shall be placed in metal containers with self-closing lids, appropriately labeled.

### Lifting Devices

* The Contractor shall inspect, maintain and operate hoists, cranes, slings and other lifting equipment in a safe manner to prevent damage to government property or injury to personnel.
* All lifting devices and equipment shall be of sufficient capacity for the loads lifted.
* Visually inspect all lifting devices and equipment before each use or daily.
* Slings shall not be used when tied in knots or when damaged.

### Fire Prevention/Protection

* Contractor personnel shall follow all local fire regulations and standards to ensure that damage does not occur to government property or personnel.
* Contractor personnel shall be knowledgeable of the work site/facility emergency evacuation procedures.
* All Contractor personnel shall be trained in the use of all types of fire extinguishers. All fire extinguishers shall be of sufficient capacity and type to adequately control the types of fires most likely to occur in the areas where they are to be located. All fire extinguishers shall be maintained in a readily visible and accessible location.
* All Contractor personnel shall be familiar with the placement and operation of available fire prevention and protection equipment located at all work sites. This should include how to report a fire and location and operation of fire alarms and fire extinguishers.
* Smoking is prohibited except in officially designated smoking areas.
* All electrical installations shall comply with the provisions of the current National Electric Code.
* Fire aisles/lanes and exits shall be kept clear of material, debris, vehicles, and etc.

### Government Property

* The Contractor shall handle, store, load and transport government property in such a way as to prevent damage to the property.
* All mechanical material handling equipment, including trucks, forklifts and conveyors shall be maintained in good operating condition.
* All materiel handling equipment operators shall be trained and certified as operators for each type of material handling equipment they operate. This training shall be the responsibility of the Contractor.
* Loaded vehicles shall not be put into motion until the load is properly stacked and secured.
* Side stakes, straps, or lashing materiel shall be used in high, unbalanced or odd shaped loads.
* All government property shall be protected from damage during storage. Property shall not be stacked directly on the floor. Property shall not be stored in direct contract with each other. All government property shall be palletized or separated by aluminum, wood, cardboard, or other suitable material. Broken or damaged pallets shall not be used for storage of government property.

### Storage/Handling of Flammable Liquids

* Precaution shall be taken to prevent the ignition of flammable vapors.
* No smoking, spark producing equipment or open flames shall be permitted in any flammable liquid storage area.
* Flammable storage cabinets and flammable storage areas shall be clearly marked “FLAMMABLE – KEEP FIRE AWAY”. Materials used in cleaning operations shall be limited to those having a flashpoint above 100-degree F whenever possible.

**APPENDIX D. REQUIRED FILES/DOCUMENTATION FOR SERVER ADMINISTRATION AND SOFTWARE/WEB DEVELOPMENT**

Any data, code, and/or work product created in the performance of this contract and its Task Orders gives the Government unlimited rights to all data, code, and/or work product.

Create or update the following:

* System Design Document (SDD)
* System Requirements Document (SRD)
* Software Deployment Change Requirements (SDCR)
* Software Test Procedures (STP)
* User’s Manual or User’s Guidance documents

Assist with the creation or maintenance of the following:

* Hardware and Software Inventory Lists
* System Security Plan (SSP)
* Information System Continuous Monitoring Strategy
* Plan of Action and Milestones (POAM)
* Access Control Process Plan
* Contingency Plan
* Ports, Protocols and Services (PPS)
* Security Control Assessments
* Software Release Transmittal Request (SRTL)
* Categorization and Selection Checklist
* Authorizing Official (AO)-Compliant System Boundary Topology
* Any other artifacts developed through RMF activity in the future (see CDRL A/B/C015 & A/B/C016)

**APPENDIX E. GOVERNMENT FURNISHED EQUIPMENT (G****FE)**

The government will provide to the Contractor the equipment listed below:

* Desktop or Laptop Computers
* Monitors
* Work Desks (at Hill AFB)
* Chairs (for use at Hill AFB)
* VoIP Telephones (for use at Hill AFB)