PERFORMANCE WORK STATEMENT (PWS)

for

480th Intelligence, Surveillance and Reconnaissance Wing

(480 ISRW)

Distributed Common Ground System (DCGS)

Mission Systems Information Technology Services

x

Date: 9 September 2024

1.0 INTRODUCTION

The 480 ISRW is the Air Force leader in globally networked intelligence, surveillance and reconnaissance (ISR) operations. The 480 ISRW has the Lead Wing designation for the Air Force Distributed Common Ground System (AF DCGS), as well as national cryptologic, information technology, cyber ISR, tactical analysis, Combined Forces Air Component Command (CFACC) support, and national-to-tactical signals intelligence (SIGINT) integration.

The 480 ISRW global 24/7/365 mission is executed from the DCGS Operations Center (DOC) with command and control execution delegated 480 ISRW/A6 performing enterprise technical operations and Command, Control, Communications, Computers and Intelligence (C4I) management across several core sites and remote locations worldwide.

2.0 BACKGROUND

2.1 MISSION. The AF DCGS weapon system is the Air Force's primary Intelligence, Surveillance, and Reconnaissance (ISR) problem centric analysis system. AF DCGS provides actionable, multi-discipline intelligence derived from multiple ISR platforms to Combatant Commands (COCOMs), Component Numbered Air Forces (C-NAF), and national command authorities across the globe 24/7/365.

Through distributed (reach back and deployed) and collaborative operations, Active Duty (AD), Air National Guard, Air Force Reserve Center, joint, and coalition units work as an integrated combat capability, enabling the Air Force to engage in multiple, simultaneous military operations across the globe.

2.2 SCOPE. This PWS describes the technical tasks along with the information assurance (IA) and information technology (IT) capabilities. 480 ISRW requires support for these various AF ISR missions. Primary locations are at Joint Base Langley-Eustis (JBLE), Virginia, and Beale Air Force Base (AFB), California. The Level of Effort provided by this task order is to augment the current military and Government civilian workforce in a blended effort.

3.0 REQUIREMENTS

3.1 480 ISRW DISTRIBUTED COMMON GROUND SYSTEM (DCGS) DCGS MISSION SYSTEMS INFORMATION TECHNOLOGY SERVICES.

3.1.1 Configuration Management and Life Cycle Management

Support 10 ISS/SCX, JBLE, VA and 548 ISRG, Beale AFB, CA.

The contractor, in coordination with Government, will ensure daily systems integration, support, management, and control of all software, hardware, system, and network configurations associated with the enterprise. The contractor shall:

- Provide systems integration management capabilities, planning, and implementation support to the 480 ISR WG and its subordinate active components in accordance with government directives.
- Submit a site-specific Configuration Management Plan that develops and maintains updated database documentation to identify, map, account, and record all network and information processing system components, devices, serial numbers, and hardware configurations in accordance with government directives, and monitors and ensures system drawings and floorplans, consisting of the unclassified and classified computers, accurately

depict approved connections and configuration as requested by the Government. **(CDRL 001)**

- Provide support to the Data Center Infrastructure Management (DCIM) process and the Data Center Manager (DCM) in accordance with processes outlined in the 480 ISR Wing instruction 17-101 Mission System Data Center Management plan, and additional 10 ISS and 548 ISRG local guidance documentation.
- Distribute, manage, track, and account for all software applications in accordance with licensing and maintenance agreements, provide quarterly inventory. **(CDRL 002)**
- Coordinate, collaborate, and accomplish activities with 480 ISRW and associated DCGS personnel, as requested by the government, to facilitate the receipt and recording of inventory and maintenance data to further refine the accuracy of the inventory tracking system.
- Organize and support all configuration management activities, including but not limited to the following activities: configuration identification, mission system equipment management, release management, change control, and configuration audits. Prior to modification, validate all changes are approved and processed.
- Ensure systems comply with established DoD and AF policies and directives.
- Draft, edit, provide input and maintain configuration management policies for hardware and software; support Government entities with developing requirements and project scope. **(CDRL 003)**
- Participate in the Configuration Control Board (CCB) to include coordinating, scheduling, and facilitating meetings; provide draft agendas, inputs or meeting minutes when requested by the government. **(CDRL 004)**
- Participate in the DCIM Local Data Center Change Advisory Board (LCAB), when requested.
- Participate in operations assessment of existing and future facility requirements relating to impacts on mission system network infrastructure and communications-computer systems.
- Complete, as requested by the government and as allowed by local security regulations, to be trained and responsible for accomplishing local SCIF procedures and tasks.
- Attend meetings, on-site conferences, teleconferences and briefings as requested by Government. Provide meeting minutes or reports. **(CDRL 005)**
- Contractor shall provide process acclimation to selected government/military personnel, as requested by the COR.
- Provide weekly status report to government task lead and COR. **(CDRL 006)**
- Possess ITIL (Foundation level) and Information Assurance Technical (IAT) Level II certifications
- Workload:

  3600+ CPUs (Class/Unclass)
  5000+ Monitors (Support all
  CPUs) 1500+ KVMs
  1400+ VOIP (Class/Unclass)
  80+ printers (Class/Unclass)

3.1.2 **C4I Systems Management for 480 ISRW/A6, JBLE, VA.** The contractor shall, in coordination with the Government, provide operations, maintenance, administration, and technical services for controlling and managing all servers, workstations, peripherals, and associated operating systems and software applications per organizational guidance.

3.1.2.1 Systems Server Administration and Support. The contractor shall maintain systems

and servers associated with 480 ISRW/A6 System Server architecture to include: Microsoft Windows Server and SQL Server, Oracle/Solaris, Red Hat Linux, Trusted Solaris, VMware/VxRail ESXi, Dell EMC Isilon NAS, Dell EMC IDPA; supporting the associated ISR applications including but not limited to Unified Collections Operations Reporting Network (UNICORN), Trusted Manager (TMAN), Oracle ZFS Storage Appliances, and Data as a Service (DaaS).
In addition, the contractor shall:

- Provide Tier 2 support based on industry standards to devices and servers for all system problems, performance deficiencies and anomalies on 480 ISRW/A6 supported networks. This includes, but not limited to Non- classified Internet Protocol (IP) Router Network (NIPRnet), Secret Internet Protocol Router Network (SIPRnet), and Langley campus-wide Joint Worldwide Intelligence Communications System (JWICS) network at both local and remote locations.
- Track, assign, troubleshoot, fix and/or close trouble tickets and new requirements in appropriate electronic system. Timelines depicted in PWS paragraph 4.5.
- Prepare systems (Windows and/or UNIX mission servers) for security accreditation.
- Install, configure, and maintain Windows, Red Hat Linux, Solaris, VMware operating systems, to include Operating System (OS), application software patches, and service packs.
- Review security, network, and system audits; and remedy identified anomalies IAW the timeline identified in the ticket or the maintenance response time chart identified in PWS section 4.5. Provide report capturing detected anomalies and resolution status. **(CDRL 007)**
- Draft, edit, maintain, and provide input to local Standard Operating Procedures (SOP). **(CDRL 008)**
- Analyze and resolve problems associated with A6 System Server architecture server hardware, operating systems, and applications software while adhering to mandated security requirements and guidelines.
- Prepare, test, and implement scripts to simplify system tasks for local use IAW security policies.
- Perform system backup and recovery utilizing network backup software.
- Support 480 ISRW ISSM and/or 480 ISRW ISSO to identify and resolve security related server and application issues.
- Provide test and evaluation support for new technology. Prepare and provide reports detailing the results of the test and evaluation including specific recommendations. (CDRL 009)
- Perform assigned CSRDs (new requirements) to complete installation requirements for new technologies and provide results in appropriate electronic record system.
- Perform assigned Problem Reports, troubleshoot systems/services, and provide results in appropriate electronic record system. Response times as depicted in PWS paragraph 4.5.
- Attend meetings, on-site conferences, teleconferences and briefings as requested by Government. Provide meeting minutes or reports. **(CDRL 005)**
- Contractor shall provide system software and hardware architecture acclimation to selected government/military personnel, as requested by the COR.
- Provide weekly status report to government task lead and COR. **(CDRL 006)**
- Ensure certification requirements are met IAW DoD 8570.01-M Information Assurance Technical (IAT) II
- Must have skillsets in:
  Administration of Microsoft Windows Server 2019 and/or up to the most current version;

Administration and maintenance of VMware versions 6.x/7.x or most current version;
Microsoft IIS 7.x/8.x or most current version;
Microsoft SQL Server 2019 or most current version

- Workload:

  64 Windows Servers (Windows Server 2019)
  6 UNIX Servers (Solaris / Red Hat)
  118 VMware/VxRail ESXi Hosts / vCenter Appliances
  2 TMAN Servers (Cross Domain Solution)
  4 Oracle ZFS NAS/SAN Storage Appliances
  1 Dell Isilon NAS
  1 Dell IDPA Storage Appliance

3.1.2.2 System Application Administration and Support 480 ISRW/A6, JBLE, VA. The contractor shall, in coordination with the Government will provide Tier 2 support, based on industry standards, to maintain the 480 ISRW ISR mission applications including but not limited to: Unified Collections Operations Reporting Network (UNICORN), Trusted Manager (TMAN), Oracle ZFS Storage Appliances, and Data as a Service (DaaS) applications.
In addition, the Contractor shall:

- Test, implement, administer, troubleshoot, upgrade, and maintain operation of the 480 ISRW ISR virtualization software, Microsoft SQL Server, Microsoft Windows Server, and DaaS application system software as installed on the following: the Non- classified Internet Protocol (IP) Router Network (NIPRnet), Secret Internet Protocol Router Network (SIPRnet), and the Langley campus-wide Joint Worldwide Intelligence Communications System (JWICS) network at both local and remote locations.
- Maintain applications and Virtual Machines (VMs) in a Cloud Computing Services (C2S) Dev/Ops, Amazon Web Services (AWS) or like cloud environment.
- Test, implement, administer, troubleshoot, upgrade and maintain operation of web-based applications to include but not limited to UNICORN, DaaS, and other systems, on all networks at both local and remote locations.
- Complete daily status checks on all services/systems; provide results and anomaly reports in appropriate electronic record systems, and validate required backups are completed IAW established policies.
- Ensure system application security posture is maintained IAW 480 ISRW ISSM and/or 480 ISRW ISSO security policies.
- Perform all security related server and application periodic procedures IAW 480 ISRW ISSM and/or 480 ISRW ISSO security policies.
- Identify and resolve all security related server and application issues IAW 480 ISRW ISSM and/or 480 ISRW ISSO security policies.
- Perform user account, group, and directory maintenance for clients in coordination with Client Systems Administration personnel, 480 ISRW Information System Security Manager (ISSM), and/or 480 ISR Wing Information System Security Officers (ISSO). Manage user and group policies and rights; conduct auditing for same.
- Perform assigned Problem Reports, troubleshoot and resolve systems/services issues, generate After Action Reports and provide results in appropriate electronic record system. Response times depicted in PWS paragraph 4.5.
- Draft, edit, maintain and provide input to local Standard Operating Procedures (SOP). **(CDRL 008)**

- Provide support to 480 ISRW integration activities to identify procedural changes and processes that would enhance the overall environment. Generate and provide ad-hoc systems/services utilization reports as requested by Government.
- Coordinate with Program Management Offices (PMOs) for ongoing updates and maintenance of the ISR web sites.
- Provide test and evaluation support for new technology. Prepare and provide reports detailing the results of the test and evaluation including specific recommendations. (**CDRL 009**)
- Perform assigned CSRDs (new requirements) to complete installation requirements for new technologies and provide results in appropriate electronic record system.
- Attend meetings, on-site conferences, teleconferences and briefings as requested by Government. Provide meeting minutes or reports. **(CDRL 005)**
- Contractor shall provide system software and hardware architecture acclimation to selected government/military personnel, as requested by the COR.
- Provide weekly status report to government task lead and COR. **(CDRL 006)**
- Ensure certification requirements are met IAW DoD 8570.01-M Information Assurance Technical (IAT) II.
- Skillset requirements:
  Administration and maintenance of VMware/ versions 6.x/7.x or most current version;
  Administration of:
  Microsoft Windows Server 2019 and/or up to the most current version
  Microsoft IIS 7.x/8.x or most current version
  Microsoft SQL Server 2019 or most current version
  480 ISRW Data as a Service (DaaS) applications
- Workload:

  # of Server/Application environments to support:
  64 Windows Servers (Server 2019)
  6 UNIX Servers (Solaris / Red Hat)
  118 VMware/VxRail ESXi Hosts / vCenter Appliances
  2 TMAN Servers (Cross Domain Solution)
  4 Oracle ZFS NAS/SAN Storage Appliances
  1 Dell Isilon NAS
  1 Dell IDPA Storage Appliance

3.1.2.3 Client Systems Administration (CSA) The contractor shall, in coordination with the Government, maintain workstations and applications associated with 480 ISRW Network and Communication architectures to include Windows Workstations. CSA support shall be provided to facility-wide NIPRnet, SIPRnet, and Langley campus-wide JWICS and NSAnet infrastructures. In addition, the contractor shall:

- Provide Tier 1 and Tier 2 support based on industry standards to support clients for all system problems and anomalies.
- Submit, track, troubleshoot, fix and/or close trouble tickets and new requirements submitted via applicable electronic requirements and problem reports systems. Timelines depicted in paragraph 4.4.
- Prepare workstations for security accreditation and security compliance inspections.
- Install, configure, test, and maintain Windows operating systems, to include System (OS), and application software patches and service packs on workstations and laptops.

- Perform Tier 1 and Tier 2 user account, group, and home directory creation and maintenance for users, workstations, laptops, and member servers, in coordination with 480 ISR Wing ISSO.
- Issue new user accounts and certificates on SIPRnet and JWICS as a Trusted Agent (TA). Perform user account troubleshooting to include user Common Access Cards SIPRnet, and JWICS Tokens.
- Perform printer software configuration and maintenance.
- Analyze and resolve problems associated with workstation and member server hardware, operating systems, applications software, and 480 ISR Wing ISSO identified security related issues while adhering to requirements and guidelines.
- Prepare, test, and implement local scripts to simplify system tasks.
- Perform local back-up and recovery procedures utilizing and managing media backup storage devices.
- Secure and manage storage, destruction, tracking, and organization of media.
- Provide test and evaluation support for new technology as directed by local or higher command guidance. Prepare reports detailing the results of the test and evaluation including specific recommendations. **(CDRL 009)**
- Evaluate and recommend improvements to the security configuration of member workstation computer systems by electronic and manual review methods.
- Draft, edit, maintain and provide input to local Standard Operating Procedures (SOP). **(CDRL 008)**
- Attend meetings, on-site conferences, teleconferences and briefings as requested by Government. Provide meeting minutes or reports. **(CDRL 005)**
- Contractor shall provide system software and hardware architecture acclimation to selected government/military personnel, as requested by the COR.
- Provide weekly status report to government task lead and COR. **(CDRL 006)**
- Ensure certification requirements are met IAW DoD 8570.01-M Information Assurance Technical (IAT) II.
- Must have skillsets in:
    - Computer/hardware/software troubleshooting and help desk support
    - Hands-on experience with Microsoft Windows operating platforms
    - IT security policies and best practices
    - Experience in imaging workstations and laptops to the current standard desktop configurations (SDC)
    - Vulnerability management practices to include, but not limited to, remediation of system vulnerabilities and patch management.
- Workload:

    1600+ CPUs (Class/Unclass – Bldg. 23 and across JBLE)
    2600+ Monitors
    450+ KVMs
    120+ Printers (Class/Unclass)
    1000+ Phones (Class/Unclass – Bldg. 23 and across JBLE)
    200+ software suites (Not including OS – Bldg. 23 and across JBLE)

3.1.3 Network Infrastructure Management for 480 ISRW/A6P, JBLE, VA. The contractor shall, in coordination with the Government, provide operations, maintenance,

administration, and technical services for controlling and managing all network infrastructure services to include troubleshooting and testing networks, routers, switches, hubs, systems, and other related hardware components. In addition, the contractor shall:

- Track, assign, troubleshoot, fix and/or close trouble tickets and new requirements in appropriate electronic system. Timelines depicted in paragraph 4.4.
- Provide fault isolation and incident resolution support for networks, Infrastructure Architecture (IA) Suites using Government-provided network analysis tools and applications (e.g. SolarWinds).
- Provide technical support in the configuration, optimization, troubleshooting, and software maintenance of IA Suites (firewalls, IDS), routers, switches, servers, High Assurance Internet Protocol Encryptor (HAIPE) devices, workstations, overall network, and long haul communication circuit support.
- Provide detailed documentation on all tasked actions that affect the operation of the system environment, to include but not limited to: system trouble calls handled, configuration changes, and new products or solutions.
- Draft, edit, maintain and provide input to local Standard Operating Procedures (SOP). **(CDRL 008)**
- Provide test and evaluation support for new technology. Prepare reports detailing the results of the test and evaluation including specific recommendations. **(CDRL 009)**
- Engineer network solutions in an Internet Protocol (IP) and Gigabyte Ethernet (GIG-E) Local Area Network (LAN)/Wide Area Network (WAN) environment.
- Design, document, and provide technical solutions to customers for classified networks. **(CDRL 010)**
- Work with vendors and other military organizations to design possible solutions for classified networks.
- Provide timelines and cost estimates for the new installation of local and remote networks to accommodate voice, video, and data.
- Configure, troubleshoot, and maintain Voice over Internet Protocol (VoIP) phones and Video Teleconferencing (VTC) equipment. Create Virtual Local Area Networks (VLANs), configure Quality of Service (QoS), and port-security in a voice network infrastructure. Video traffic shall be separated from other types of data to ensure high QoS to video customers.
- Create network infrastructure to support real-time (RT) and near real-time (NRT) high bandwidth video feeds.
- Administer and manage Microsoft Windows Server Dynamic Host Configuration Protocol (DHCP) scopes, General Dynamics Encryption Manager (GEMOne), SolarWinds, Cisco Access Control Server (ACS) Identity Services Engine (ISE) and similar technologies.
- Provide classified courier duties within the local area and follow base and unit Operations Security guidance (SOPs, OIs, etc.). A copy of the local guidance will be provided to the contractor. **(CDRL 005)**
- Attend meetings, on-site conferences, teleconferences, and briefings and provide meeting minutes or reports as requested by Government. **(CDRL 005)**
- Contractor shall provide system software and hardware architecture acclimation to selected government/military personnel, as requested by the COR.
- Provide weekly status report to government task lead and COR. **(CDRL 006)**
- Ensure certification requirements are met IAW DoD 8570.01-M Information Assurance Technical (IAT) II and maintain skillsets in the following:

- Configuration and management of Cisco Routers and Switches
- Tactical Local Area Network Encryption (TACLANE) devices
- Administering internet protocol networks to include VoIP, VTC, and fiber optic technologies

- Workload:

  31 Bldgs (bldg. 23 and across Joint Base Langley-Eustis)
  3 Geographically Separated Units
  250+ network switches
  90+ crypto devices
  JWICS and DISA Regional Nodes (suite of equipment as service provider)
  All patch cables connecting switches and end devices (CPUs/Phones/Printers, etc)

4.0 GENERAL INFORMATION

This is a non-personal services contract. The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. The contractor shall manage its employees and guard against any actions that are of the nature of personal services, or give the perception of personal services. The contractor shall notify the Contracting Officer (CO) immediately if they perceive any actions constitute personal services.

These services shall not be used to perform any inherently governmental functions. The services described support the Air Force (AF) Distributed Common Ground System (DCGS) Program and 480 ISRW Mission Systems.

4.1 SURGE OPERATIONS.

The Government may require the contractor to provide surge capabilities as reflected in PWS Section 3.0. Surge capabilities may be required within 10 days of notification as directed by the CO. During surge operations, the contractor can expect that one operating location has been rendered partially or completely inoperable and all operational mission requirements must be accomplished at the remaining operational location. Performance that will be required during surge operations may include all or some of the capabilities reflected in PWS Section 3.0 and will be further specified by the Government prior to the onset of surge operations. These surge operations are considered above and beyond normal operations as specified in this PWS. The Government estimate for surge utilization is not expected to exceed one month in duration and can be exercised by the Government in a daily increment. If the contractor's solution is for personnel to travel from one location to the other, the cost of travel will be reimbursed under the Government Directed Travel CLIN. The contractor shall provide support for surge operations at a level-of-effort that is no more than what is included in the most current contract.

4.2 PROGRAM MANAGEMENT.

4.2.1 General Requirements. The contractor shall identify a Program Manager. This PM shall be the primary representative responsible for the successful completion of all work awarded under this contract. The PM shall participate in all Program Management Reviews.

4.2.1.1 The contractor shall provide qualified and fully trained personnel to perform the required services from task order (TO) start until completion.

4.2.1.2 The contractor shall notify the Contracting Officer (CO) of all direction received from Government personnel they consider to be outside the scope of PWS requirements prior to performing the work.

4.2.1.3 Unless specifically called in this PWS, all days refer to calendar days, not business days

4.2.2 Program Management Review (PMR). The contractor shall schedule and attend PMRs at times mutually agreed upon with the Government. The CO, Contracting Officer's Representative (COR), and other Government personnel, as appropriate, shall meet periodically with the contractor to review performance. PMRs shall be held at least quarterly; however, the Government reserves the right to conduct PMRs more frequently as needed. The assigned COR and the contractor site lead shall meet five (5) business days in advance of the PMR to review the agenda which shall include, at a minimum, hiring status, and feedback on performance standards, overall contract performance, and all other significant events. The contractor shall document the meeting and provide the minutes to the CO and COR. **(CDRL 011)**

4.3 CONTRACT MANPOWER REPORTING

4.3.1 The Contractor shall report ALL labor hours required for performance of services provided under this task order via the Government's contractor manpower reporting data collection system. The Contractor is required to completely fill in all required data fields. Reporting inputs shall be for the labor executed during the PoP for each Government fiscal year (FY), which is 1 October through 30 September. While inputs may be reported anytime during the FY, all data shall be reported no later than 31 October of each calendar year; unless otherwise stated by either the CO or the reporting management system. The prime Contractor shall be responsible to ensure all subcontractor data is reported. Data shall be reported to SAM.gov at beta.sam.gov (or future changes/ updates of the identified data collection system/ new data collection system).

4.3.2 Uses and Safeguarding of Information: Information from the secure data collection system/ web site is considered to be proprietary in nature when the contract number and the Contractor identity are associated with the direct labor hours and direct labor dollars. The data collection system houses the responsibility to ensure data is not released to the public that includes the Contractor name, contract number, and associated reported data.

4.3.3 Help Desk: The Contractor may direct questions to the help desk of the identified system.

4.4 PERIOD OF PERFORMANCE.

The period of performance for the basic contract will be one (1) base year plus four (4) option years and a transition in and transition out timeframe. The transition period is ten (10) business days to transitioning in and ten (10) business days to transition out.

4.5 HOURS OF WORK.

The Government will designate normal core hours, but in general, the hours are between 7 A.M. to 5 P.M. (0700-1700) Monday through Friday. When directed by the Government, the contractor shall respond to emergencies and recalls (excluding practice telephone recalls). For sections **3.1.2. C4I Systems Management** and **3.1.3. Network Infrastructure Management**, a rotating on-call duty with other contractor, military, and Government personnel is required. If an urgent after hours problem is identified, the contractor shall telephonically respond to the on-call notification within 15 minutes and shall respond to duty location within 45 minutes, and follow the response time chart, when directed by the Government.

The level of participation, for the rotating on-call duty roster is projected to occur between six

(6) to eight (8) times a year; lasting two weeks in duration per event, which could include a federal holiday.

For all assigned trouble tickets, the following timelines will be utilized to maintain a smooth operational tempo.

Response Time Chart

Priority	Response Time To User From Initial Call	Required Update To User Until Issue Is Resolved
LOW	within 8 hours	weekly
MEDIUM	within 4 hours	every 8 hours
HIGH	within 1 hour	every 2 hours
URGENT	within 15 minutes	every hour

In the event of inclement weather, heightened security concerns, or other unique events, the contractor shall adhere to direction of their government task leads. Deviations from the Government-designated core hours shall be coordinated with the Government COR and CO.

4.6 FEDERAL HOLIDAYS.

Federal holidays, as determined by Executive Order, shall be observed by the contractor and are listed below, however, mission may dictate work on any of the below holidays. If the holiday falls on a Sunday, it is observed on the following Monday. If it falls on a Saturday, it is observed on the preceding Friday. Government oversight will not be present on these days.

New Year's Day	Dr. Martin Luther King's Birthday	Presidents' Day
Memorial Day	Independence Day	Labor Day
Columbus Day	Veterans Day	Thanksgiving Day
Christmas Day		

In support of Family, Energy Conservation, and Early Release Days. There will be days when the Government, Major Command (MAJCOM), and/or Base Commander will direct Family Days, Energy Conservation Days, and/or early release days. When these days are identified, the Contractor is expected to work when the facilities are available for them to do so. Furthermore, the COR/PM may not direct the Contractor regarding whether or not to compensate employees if not required to work that day. The Contractor may elect to grant employees the day off with pay, but there is no additional Government contract costs (wages for these hours are already in the contract cost). This contract specifies that in order for contractors to remain in place, they must have Government oversight in place.

In support of Alternate Work Locations (AWL). Alternate Work Locations shall be permitted for this task order on a case-by-case basis with COR/CO approval. In the event the primary duty location is unavailable to the contractor (i.e the installation/facility is closed) then the contractor may be directed to telecommute or work from an alternate, approved location. Working from an alternate location shall not involve working with or transporting classified information. The contractor shall provide an AWL status IAW PWS paragraph 4.9, Deliverables (**CDRL 06**). Telework, as set forth in all wing contracts (e.g. Performance Work Statements) requires approval of an 'Alternate Work Location (AWL)'. Telework and an approved AWL is interpreted as ONLY being authorized when it is advantageous to the government and/or when directed by the Government. **Telework is not authorized** for the time period associated with ROM when a contractor employee takes personal travel outside of the local area and upon return are required to ROM.

In support of the Continuation of Essential Contractor Services Clause. There may be days when the Government, MAJCOM, and/or Base Commander will direct closure of the installation and/or facilities. The contractor shall provide a Mission Essential Contractor Services Plan to the government within 60 calendar days of contract award, and shall maintain and update the plan as necessary to provide the identified essential contractor services at PWS paragraph 8.0 and 8.1 (when exercised) (**CDRL 015**).

4.7 KICK-OFF MEETING

The contractor shall schedule and attend an initial kick-off meeting within seven (7) business days of contract start date. Meeting shall consist of the contractor representatives, Government COR, and Contracting Officer (CO). The contractor shall provide a transition management plan three (3) business days prior to the kickoff meeting. The transition management plan will include Project Management Plan, Risk Management Plan, Staffing Plan, Company Organizational Chart and a Conflict of Interest Mitigation Plan.

The transition management plan will be presented and discussed at the kick off meeting with feedback being incorporated and a final management plan being delivered to the government ten (10) business days after the kickoff meeting (**CDRL 012**). The contractor shall submit Kickoff meeting minutes to the Government CO within three (3) business days after this meeting (**CDRL 013**).

4.8 TRAVEL

Travel shall be required. All travel will be approved by the COR prior to making travel reservations. All travel performed by the contractor shall comply with the provisions of the Joint Travel Regulations (JTR). Wherever possible, contractor shall have identical travel and lodging arrangements as Government travelers. When Government and contractor travel is coincident (same dates, same destinations, same travel objective), Government personnel will obtain rental car and miscellaneous supplies, when arrangements are the same. Costs for travel shall be billed on a strictly cost reimbursable basis IAW the terms and conditions of this contract. Trip reports will be submitted to the COR and CO within five (5) business days of the completion of all trips. **(CDRL 014)**

4.9 DELIVERABLES. The contractor shall provide deliverables as specified in Contract Data Requirement List (CDRL). A list of CDRLs are as follows:

CDRL	Data Item Number	Data Item Description	PWS Paragraph	Delivery Schedule
001		Submit a site specific Configuration Management Plan as requested by the Government	3.1.1	45 days after contract award; reviewed/updated every 60 days thereafter; updates when identified shall occur within 5 business days.
002		Distribute, manage, track, and account for all software applications in accordance with licensing and maintenance agreements, provide quarterly inventory	3.1.1	Quarterly Inventory
003		Draft, edit, provide input and maintain configuration management policies for	3.1.1	3 months after contract award, reviewed/updated monthly.

CDRL	Data Item Number	Data Item Description	PWS Paragraph	Delivery Schedule
		hardware and software; support Government entities with developing requirements and project scope.		
004		Participate in the Configuration Control Board (CCB) to include coordinating, scheduling, and facilitating meetings; provide draft agendas, inputs or meeting minutes when requested by the government.	3.1.1	2 days after meeting concludes.
005		Attend meetings, on-site conferences, teleconferences and briefings as requested by Government. Provide meeting minutes or reports.	3.1.1 3.1.2.1 3.1.2.2	2 days after meeting concludes, the on-site conference, the teleconference and/or briefing.
006		Provide weekly performance status report to government lead; summary to COR	3.1.1 3.1.2.1 3.1.2.2 3.1.2.3 3.1.3 4.6 AWL	End of the duty day Friday, unless PWS section 4.5 applies, then report is due on next business day.
007		Review security, network, and system auditing and remedy identified anomalies. Provide report capturing detected anomalies.	3.1.2.1	Report submitted within 2 days; report captures anomalies and actions taken.
008		Draft, edit, maintain and provide input to local Standard Operating Procedures (SOP).	3.1.2.1 3.1.2.2 3.1.2.3 3.1.3	Within 10 days upon request.
009		Provide test and evaluation support for new technology. Prepare reports detailing the results of the test and evaluation including specific recommendations.	3.1.2.1 3.1.2.2 3.1.2.3 3.1.3	As required. Reports are due 10 days after events or when requested by the Government
010		Design, document, and provide tech-solutions to customers for classified networks.	3.1.3	Within 10 business days of request.
011		The contractor shall document the meeting and provide the minutes to the CO and COR.	4.1.2.	Within 5 days of the meeting

012		The transition management plan will be presented at the kick off meeting with feedback being incorporated and a final	4.7	Schedule identified in section 4.7 Kick-Off Meeting

CDRL	Data Item Number	Data Item Description	PWS Paragraph	Delivery Schedule
		management plan being delivered to the government ten (10) days after the kickoff meeting.		
013		The contractor shall submit Kickoff meeting minutes to the Government CO within three (3) business after this meeting.	4.7	3 business days after the meeting
014		Trip reports will be submitted to the COR and CO within 5 business days of the completion of all trips.	4.8	Within 5 business days of travel completion.
015		Mission-Essential Contractor Services Plan	4.6	Within 60 calendar days of contract award; updated as necessary and submitted after update within 5 calendar days of change.

4.10 SERVICES SUMMARY.

The Services Summary (SS) provides information on contract requirements and the expected level of contractor performance to be successful. These thresholds are critical to mission success. Procedures as set forth in the applicable Inspection of Services Clause in the contract shall be used to remedy all deficiencies. The Government retains the right to inspect any item included in the contract.

Performance Objective	PWS Paragraph	Performance Threshold
Attend meetings, conferences, and briefings and provide minutes.	3.1	Provide detailed minutes capturing attendees, items discussed, action items in less than 2 business days is acceptable
Coordinate with supported groups to identify, account, and record all network and information processing system components, devices, hardware, and software configuration.	3.1.1	Maintaining the site specific Configuration Management Plan, updated are a modification occurs; in 5 business days or less is acceptable. Conducting quarterly reviews on time is acceptable.

Track expiration date of licenses and maintenance agreements. Coordinate supported groups to identify, track and determine if licenses are still required.	3.1.1	Provide necessary documentation to support government procurement process 120 calendar days prior to expiration date is acceptable.
Identify discrepancies, unauthorized, inappropriate, and improper connections and hardware and software additions.	3.1.1	Reporting is immediate, but no less than 12 hours is acceptable.

Performance Objective	PWS Paragraph	Performance Threshold
Coordinate, schedule, and facilitate Configuration Control Board meetings.	3.1.1	Submit agenda 1 business day prior to the meeting and provide meeting minutes two (2) business days after the meeting is acceptable.
Provide test and evaluation support for new technology. Prepare reports detailing the results of the test and evaluation including specific recommendations	3.1.2.1 3.1.2.2 3.1.2.3 3.1.3	Submit a clear, concise report detailing the test criteria and the evaluation results with a two course of action recommendations after the test period is acceptable.
Provide software application Virtual Machine (VM)/cloud performance recommendations.	3.1.2.2	Provide an input on environments and recommend management enhancement practices to allow for effective utilization of VM and/or cloud technology. Provide recommendations monthly is acceptable.
Design, document, and provide tech-solutions to customers for classified networks.	3.1.3	Provide final technical solution and all supporting documentation for the government procurement process 10 business days is acceptable.
Replace/substitute personnel.	6.1	Performance is acceptable when: a) IAW PWS Para 6.1, Personnel Maintenance, vacancies are filled with qualified personnel within 10 business days of vacancy, unless approved in writing or otherwise directed in advance by the CO AND b) There is no mission impact due to position vacancies or unqualified personnel.

4.11 COR DESIGNATION. The CO will provide the Contractor with a COR Designation Memorandum to inform the Contractor of the designated COR on the contract.

4.11.1 Performance Evaluation. Contractor performance is subject to Government COR surveillance to ensure PWS compliance. The Contractor shall comply with the following:

4.11.2 Access. The Contractor shall permit the CO or authorized representative access to all work areas, records, and data used in the performance of the contracted services. The Contractor shall provide support, and not interfere with the CO, PM, COR, state, federal, and other designated personnel in the performance of their official duties. Access shall be provided as soon as possible, but not to exceed one (1) workday after the request.

4.11.3 Non-conformances. Identify and control non-conformances through root cause analysis, corrective actions, and preventive actions. Focus on eliminating the cause to prevent reoccurrence. Maintain records of non-conformities and actions taken. Correct and provide response to all government-identified non-conformances in accordance with (IAW) time frames

specified by the CO or PM. This contract identifies two types of non-conformances: Minor and Major.

4.11.4 Minor Non-conformance. A minor non-conformance is a non-conformance, which by itself does not adversely impact mission, safety of personnel and/or equipment, performance (quality), schedule (delivery), or cost. It normally does not increase risk to the Government. Minor non-conformances are typically low risk and are communicated through notices; first notices are issued for any identified non-conformance, second notices are issued for repeat non- conformances or failing to correct issues within a reasonable amount of time. Upon receipt of a non-conformance notification (first or second notice), the Contractor shall complete applicable sections and return it to the PM within time constraints directed by the PM in the notice. A formal corrective action plan is not required for notices.

4.11.5 Major Non-conformance. A major non-conformance is a non-conformance that adversely impacts (or has the potential to impact) mission, safety of personnel and/or equipment, performance (quality), schedule (delivery), or cost. This type of non-conformance increases risk to the Government and therefore has a risk assessment rating of moderate or high. An example of increasing risk would be a significant number of recurring non-conformances, which is an indication of inadequate preventive measures/actions and lowers the Government's confidence that the Contractor can provide quality services on time and within costs. The CO will communicate major non-conformances on a Corrective Action Request (CAR) form with a suspense date for the Contractor's corrective action plan. As a minimum, the Contractor's corrective action plan will address:

- Action taken to fix the immediate problem
- Root cause analysis of the problem to determine cause
- Corrective action on the cause of the problem to include the follow-up plan (how and when)
- Actions taken to prevent recurrence

4.12 PRIVACY ACT.

Work on this task requires access to Privacy Information. The contractor shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

4.13 GOVERNMENT FURNISHED EQUIPMENT (GFE).

4.13.1 The Government will provide office space, office supplies, computer equipment, computer software, and access to military Local Area Network (LAN) services (classified and unclassified), telephone, LAN support, and reproduction facilities to support contractor contract support requirements. The contractor may not be the sole user of furnished computer equipment; therefore, coordination with other contractors and administrators may be necessary. The Government will furnish appropriate User Identification and passwords for shared resources. The contractor will be provided access to Government electronics, such as unclassified, collateral, and Sensitive Compartmentalized Information (SCI) e-mail and fax machines, in support of this requirement.

4.13.2 Intellectual Property Rights. The Government will retain all intellectual property rights.

4.14 GOVERNMENT FURNISHED INFORMATION.

The Government will provide access to relevant Government organizations, information and documentation, manuals, texts, briefs, and associated materials as required and available relative to assigned contract responsibilities. Access will be granted to classified networks as needed and in accordance with applicable governing security directives.

5.0 SPECIAL CONTRACT PROVISIONS.

5.1. SECURITY CONCERNS AND INFORMATION RELEASABILITY.

5.1.1. Foreign hostile intelligence organizations are continuing to increase the scope of their collection efforts against all aspects of DoD activities and operations. When developing advanced tools for the defense and intelligence communities, inadvertent or overt disclosure of programs currently being pursued or employed shall be avoided in order to maintain the technological advantage these capabilities provide. The contractor shall not provide any information (discussions, publications, correspondence) about this effort to any other organization, agency, or person without first requesting, in writing, and receiving release authority from Contracting Officer.

5.1.2. All personnel performing work on this contract shall possess a TS/SCI clearance unless pre-coordinated with the 480 ISRW Functional Director of Contracts or COR. Personnel performing on this PWS shall be a U.S. Citizen and shall require a security clearance. Information used to perform the above work may be classified up to TOP SECRET/SCI, SAP and NATO. The contractor must possess or obtain a facility security clearance at the level of TOP SECRET prior to proposal submission. The contractor shall request personnel security clearances (Submit Clearance Paperwork through DSS to the National Background Investigation Bureau (NBIB)) for personnel requiring access to classified information within fifteen (15) days after contract award. Due to costs involved with security investigations, requests for contractor security clearances shall be kept to an absolute minimum necessary to perform contract requirements. Contractor personnel shall have appropriate clearances prior to commencing work on any task unless otherwise approved in writing by the Government. The Contractor shall also complete visit requests for each individual that will be performing work in the Defense Manpower Data Center (DMDC) JPAS prior to performance start unless otherwise approved in writing by the CO. The Prime Contractor shall ensure that any teaming partners or subcontractors have the appropriate clearances prior to beginning performance. The 480 ISRW owns the SCI indoctrination process for this contract. Provided the contractor provides TS/SCI eligible personnel during the transition period, the 480 ISRW Security Office (SO) will ensure personnel are indoctrinated in time to perform at contract start. Once the transition period is complete, the contractor will be responsible for updating the Contractor SCI Eligibility Request Letter for incoming and outgoing personnel. The contractor will provide the letter to 480 ISRW/ SO, and scheduling an appointment for indoctrination or debriefing on an as needed basis. The contractor shall follow the security requirements outlined in the contract DD Form 254, Department of Defense (DoD) Security Classification Specifications. The contractor shall be

subject to random drug testing. If work identified at requires access to NSA systems, the contractor may be required to take a Counter Intelligence (CI) polygraph test.

5.1.3. The contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) Memorandum M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

5.1.4. The contractor shall comply with Operations Security requirements contained in AFI 10-701 and local supplements to AFI 10-701, to include all current Critical Information (CI) listings.

5.2. Information Assurance Contractor Training and Certification (Jan

2008). As prescribed in 239.7103(b), the following clause shall apply:

The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

(a) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

(b) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

6.0 CONTRACTOR PERSONNEL

6.1 The contractor shall take necessary actions to minimize employee turnover. In the event of a resignation or terminations, the contractor shall provide a replacement that meets all KSA and security clearance requirements within in 10 business days from the last day the position was last filled. The contractor will provide a weekly staffing report to minimize gaps in employee turnover.

6.2 DoD 8570.01M "*Information Assurance Training, Certification and Workforce Management,*" identifies categories and specialties within the IT workforce. Contractors supporting this tasks within this contract are required to hold and maintain DoD 8570 IA Level

II. 3.1.2, 3.1.3 and 3.1.4 IT security professionals shall maintain the Government-defined 8570 certification requirements to perform their duties under this contract.

7.0 APPLICABLE PUBLICATIONS AND INSTRUCTIONS (NOT INCLUSIVE)

PUBLICATION/INSTRUCTION	TITLE
ACCI 14-201V1	DISTRIBUTED COMMON GROUND SYSTEM (DCGS) – INTELLIGENCE TRAINING
ACCI 14-201V2	DISTRIBUTED COMMON GROUND SYSTEM (DCGS) – CREWMEMBER STANDARDIZATION/EVALUATION PROGRAM
ACCI 14-201V3	AF DISTRIBUTED COMMON GROUND SYSTEM (AF DCGS) OPERATIONS PROCEDURES
AF MPTO 00-33A-1001	METHODS AND PROCEDURES -- GENERAL COMMUNICATIONS ACTIVITIES MANAGEMENT PROCEDURES AND PRACTICE REQUIREMENTS
AFI 10-701	OPERATIONS SECURITY (OPSEC)
AFI 16-1404	INFORMATION SECURITY PROGRAM
AFI 17-100	MISSION SYSTEM INFORMATION TECHNOLOGY (IT) SERVICE MANAGEMENT
AFI 17-101, 480 ISRW SUP	MISSION SYSTEM DATA CENTER MANAGEMENT
AFI 31-101	INTEGRATED DEFENSE (FOUO)
AFI 33-322	RECORDS MANAGEMENT PROGRAM
AFI 33-332	AIR FORCE PRIVACY AND CIVIL LIBERTIES PROGRAM
AFI 16-1406	INDUSTRIAL SECURITY PROGRAM MANAGEMENT
AFMAN 16-1405	PERSONNEL SECURITY PROGRAM
AFMAN 17-1203	INFORMATION TECHNOLOGY (IT) ASSET MANAGEMENT (ITAM)
AFMAN17-1302-O	COMMUNICATIONS SECURITY (COMSEC) OPERATIONS
DJSIG	DODIIS JOINT SECURITY IMPLEMENTATION GUIDE
DOD 5400.7-R_AFMAN 33-302	DOD FREEDOM OF INFORMATION ACT PROGRAM
DOD 8570.01-M	INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM (INCORPORATING CHG 4, 10 NOV 2015)
DODD 8140.01	CYBER WORKFORCE MANAGEMENT (INCORPORATING CHG 1, 31 JUL 2017)
DODD 8500.1	INFORMATION ASSURANCE (IA)
DODD 8500.2	INFORMATION ASSURANCE (IA)IMPLEMENTATION
DODM 5105.21	SENSITIVE COMPARTMENTED INFORMATION ADMINISTRATION SECURITY MANUAL
ICD 502	INTEGRATED DEFENSE OF THE INTELLIGENCE COMMUNITY INFORMATION ENVIRONMENT
ICD 503	INFORMATION TECHNOLOGY SYSTEMS SECURITY RISK MANAGEMENT, CERTIFICATION AND ACCREDITATION
ICD 501	DISCOVERY AND DISSEMINATION OR RETRIEVAL OF INFORMATION WITHIN THE INTELLIGENCE COMMUNITY
ICS 500-27	COLLECTION AND SHARING OF AUDIT DATA
JTR	JOINT TRAVEL REGULATION
OSHA	OCCUPATIONAL SAFETY AND HEALTH ACT
TECHNICAL ORDER 00-20-14	AF METROLOGY AND CALIBRATION
TECHNICAL ORDER 00-35D-54	USAF MATERIAL DEFICIENCY REPORTING

8.0 LEVEL OF EFFORT (ANNUAL)

PWS TASK	PWS PARAGRAPH NAME	Hours per Year	# of FTEs/location
3.1.1	Configuration Management and Life Cycle Management Support	7,680	1 - Beale AFB 3 - JBLE
3.1.2	C4I Systems Management		
3.1.2.1	Systems Server Administration and Support	1,920	1 - JBLE
3.1.2.2	System Application Administration and Support	3,840	2 - JBLE
3.1.2.3	Client Systems Administration Support	1,920	1 - JBLE
3.1.3	Network Infrastructure Management	1,920	1 - JBLE
	Total	**17,280**	**9**

8.1 Optional FTE

PWS TASK	PWS PARAGRAPH NAME	Hours per Year	# of FTEs/location
3.1.1	Optional FTE Support--Configuration Management and Life Cycle Management Support	1,920	1 - Beale AFB

8.1.2 Optional FTE for Beale AFB. IAW with this paragraph, The Government may require the Offeror to provide an additional FTE as shown in the table above on a separately priced line item. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of needed optional requirement.