Attachment 1
PR#
12 July 2017

PERFORMANCE WORK STATEMENT

for

336th Training Squadron

Testing Center Administrators
at
Keesler Air Force Base, Mississippi

Attachment 1
PR#
12 July 2017

TABLE OF CONTENTS

Attachment 1
PR#
12 July 2017

PERFORMANCE WORK STATEMENT (PWS)

TESTING CENTER ADMINISTRATORS

Non-Personal Services

1. DESCRIPTION OF SERVICES AND GENERAL INFORMATION. The Contractor shall provide test administrators and a network/system administrator to support the certification test center and Initial Skills Training Information Assurance Certification Center (ISTIACC) enclave located in the 336th Training Squadron (336 TRS), 81st Training Group (81 TRG), 81st Training Wing (81 TRW), Second Air Force (2 AF), Air Education and Training Command (AETC) at Keesler Air Force Base (KAFB), Mississippi (MS). The Contractor shall provide sufficient test administrators to handle an average weekly load of 102 student tests and 75 new registrations for test vouchers, up to and including a maximum of 280 students testing on any given day on either one or two shifts per guidance as prescribed in Pearson VUE® policies and procedures. The Contractor shall provide a contingency plan for proper coverage of testing center if a sustained max load of 280 students exceeds two weeks. The test administrator shall provide a report which identifies: class number, student's name, rank, SSN, scores (initial and re-test), Training Requirement Quota Identifier, and voucher number (1st, 2nd, and/or 3rd) in a format designated by the Training Manager.

a. The 336 TRS provides initial skills training in numerous Air Force Specialty Codes (AFSCs) to include: Cyber Systems Operations (3D032), Cyber Surety (3D033), Client Systems (3D131), Cyber Transport (3D132), Cyberspace Defense Operations (1B431), and Undergraduate Cyber Training [phase 1] (17DX1). As part of their training, each student must earn a commercial certification, Computing Technology Industry Association (CompTIA®) Security+ certification, in order to be awarded their respective AFSC.

b. A Pearson VUE® authorized test center is available on-site in Thomson Hall, 336 TRS, KAFB, MS. This test center has the capability to seat 80 students at any given time. The test center is comprised of two testing rooms equipped with 40 seats in each room. The test center requires administrators who possess the necessary qualifications and skills identified in Pearson VUE® policies and procedures to oversee and manage the test center.

1.1. OBJECTIVE. The purpose of this project is to provide test administration and network/system administration support for the on-site Pearson VUE® Testing Center which is operational from 0600 to 1500 hours (6:00 a.m. to 3:00 p.m.) daily and occasionally from 1500 to 2200 hours (3:00 p.m. to 10:00 p.m.) when needed to support a second shift or excess capacity in test center. The 336 TRS tests approximately 2,500 - 2,800 students annually. Every two weeks, there are approximately 150 - 220 students who will require test registration or administration support; however, the number will vary depending on the number of graduates from the pre-requisite classes. A schedule detailing the predicted flow of trainees will be provided to the Contractor once the contract has been awarded.

1.2. TEST ADMINISTRATOR SUPPORT.

1.2.1. The Contractor shall provide test administrators who will provide daily administrative and technical support in accordance with Pearson VUE's policies and procedures in the following areas:

1.2.1.1. Register the students to obtain their vouchers for the CompTIA® exams via the Air Force Space Command (AFSPC) web-site.

1.2.1.2. Identify and correct student administrative errors that may have occurred during the registration process.

1.2.1.3. Prepare the testing center for testing.

1.2.1.4. Register students for CompTIA® exams according to Pearson VUE® policy and procedures and CompTIA® guidelines to include test compromise.

1.2.1.5. Candidates must be proctored by a Pearson VUE certified Test Administrator(s) at all times while exams are being delivered. Multiple proctors are required to monitor testing rooms with more than 15 candidates taking exams at one time.

1.2.1.6. Ensure sufficient levels of office supplies and other materials necessary for the proper operation of the testing center. Identify shortages in a timely manner to avoid any testing interruptions.

1.2.1.7. Up-channel reports to Pearson VUE® as needed, (Example; Incident reports).

1.2.1.8. Ensure programmed Pearson VUE® software downloads to include updates are administered in the testing center according to the time table identified by Pearson VUE®.

1.2.1.9. Provide a test failure report which identifies: class number, instructor, start date, grad date, student's name, rank, AFSC, scores (initial and re-test), Training Requirement Quota Identifier (TRQI), and voucher number (1st, 2nd, and/or 3rd) in accordance with the Test Failure Template no later than 3 hours after completion of the test session with minimal errors.

1.2.1.10. Maintain a visible testing schedule on Government Furnished Equipment (GFE) (white board) identifying dates the testing center will be used.

1.3. NETWORK/SYSTEM ADMINISTRATION RESPONSIBILITIES.

References:
DOD 8570.01-M, *Information Assurance Workforce Improvement Program*
DoDD 8140.01, *Cyberspace Workforce Management*

DoDI 8500.01, *Cybersecurity*
DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*
DoDI 8520.03, *Identity Authentication for Information Systems*
AFI 17-100, *Air Force Information Technology (IT) Service Management*
AFI 17-130, *Cybersecurity Program Management*
AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*
AFMAN 17-1201, *User Responsibilities and Guidance for Information Systems*
AFMAN 17-1301, *Computer Security (COMPUSEC)*
AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*
The National Institute of Standards and Technology (NIST) FISMA Resource Site
< http://csrc.nist.gov/groups/SMA/fisma/index.html >

1.3.1. The Network/System Administration Contractor:

1.3.1.1. Should have knowledge of Air Force (AF) Risk Management Framework (RMF) Assessment and Authorization (A&A) process and the Federal Information Security Management Act (FISMA) compliance requirements.

1.3.1.2. Familiar with Enterprise Mission Assurance Support Service (eMASS) a government owned web based application which provides visibility and automation of Information Assurance (IA) Program Management processes. Will be required to establish an eMASS account once hired.

1.3.1.3. Familiar with Information Technology Investment Portfolio System (ITIPS)-OPPM (Production) system of record and compliance reporting tool for all AF IT management data. Will be required to establish an ITIPS account once hired.

1.3.1.4. Contractor personnel shall have 2 - 4 years technician experience and certification in a related areas as well as expertise in managing systems and networks in a DoD environment. The ability to communicate effectively, both verbally and in writing, and demonstrated ability to work independently or in a team environment on multiple projects with little supervision, is required.

1.3.1.5. Contractor personnel shall provide the following services in support of the 336 TRS Initial Skills Training Information Assurance Certification Center (ISTIACC) enclave to maintain ~~100%~~ system operation:

1.3.1.5.1. Systems Administration and Maintenance. Perform implementation, management, and maintenance of complex computing environment of small-sized enclave. Install new software releases, system upgrades; evaluate and install patches and resolve software related problems. Perform system backups and recovery. Standardize system and network configurations. Accurately maintain configuration data files, document changes to configuration within 30 days, and monitor system configuration to ensure data integrity. Duties will also include installing, operating and maintaining a variety of operating systems (e.g. various Microsoft Windows® versions, *NIX variants, and Linux variants) and virtualization platforms (e.g. VMware,

Microsoft) to include installation, configuration, administration, system maintenance; troubleshooting as well as how to identify, install and maintain system hardware. Abilities will include partitioning a single server into multiple virtual machines (e.g. VMware, Microsoft and others) and partition a single Windows® or Linux server into multiple virtual machines which run as an application on top of the operating system. Perform system updates, recurring network administration, and management tasks using automated software (e.g. Group Policy, scheduled tasks) or scripts (e.g. PowerShell) as the preferred method. Provide and implement an action plan to automate recurring tasks which are not currently automated. Develop and document systems administration standard operating procedures & Continuity of Operations (COOP).

1.3.1.5.2. Network and Computer Support Systems Infrastructure/Hardware Maintenance and Records. Perform minor repairs to hardware, software, or peripheral equipment, following design or installation specifications for internal and external networks. Provide inputs for tech refresh to replace equipment and software reaching end-of-lifecycle. Maintain records of daily data communication transactions, problems and remedial actions taken, or installation activities. Read technical manuals, confer with users, or conduct computer diagnostics to investigate and resolve problems or to provide technical assistance and support. Refer major hardware or software problems or defective products to vendors or technicians for service. Maintain a list of all hardware and software installed in network. Develop training materials and procedures, or train users in the proper use of hardware or software. Confer with staff, users, and management to establish requirements for new systems or modifications. Conduct periodic server maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.

1.3.1.5.3. Network Administration. Develops and maintains network communications. Uses knowledge of Local Area Network (LAN)/Wide Area Network (WAN) systems to design, install, configure, and maintain network services, equipment and devices for the ISTACC enclave. Tests and evaluates network systems to eliminate problems and make improvements. Familiar with a variety of the government network concepts, practices, and procedures. Relies on experience and judgment to plan and accomplish goals. Individual must have knowledge in the following subject areas: Networking Switches, Routers, Hubs, Cables, Racks, Firewalls, LAN and WAN technologies, Transmission Control Protocol/Internet Protocol (TCP/IP), Domain Name Servers (DNS), User Datagram Protocol (UDP), Voice over Internet Protocol (VoIP), Quality of Service (QoS), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Next Hop Resolution Protocol (NHRP), Asynchronous Transfer Mode (ATM), Point-to-Point Protocol (PPP), and Multiprotocol Label Switching (MPLS).

1.3.1.5.4. Assessment and Authorization (A&A). The Contractor shall implement Risk Management Framework (RMF) requirements for the ISTIACC network, document and maintain information systems assurance and accreditation materials, as required. Update or modify Systems Concept of Operations (CONOPS), System Security Plan (SSP), Systems Configuration Management Plan (CMP), System's Contingency and Business Continuity Plan (CBCP), System's Incident Response Plan (IRP), Security Test Plan (STP), System's Hardware and Software tables, as needed. Conduct assessments of threats and vulnerabilities, determines deviations from

acceptable configurations, enterprise or local policy, assesses the level of risk, and develop and/or recommend appropriate mitigation countermeasures. For vulnerabilities that cannot be timely mitigated, provide corrective action input on the Plan of Action & Milestones (POA&M). Develop and maintain the Assessment and Authorization (A&A) accreditation package for the ISTIACC enclave.

1.3.1.6. Liaison. Liaison with the Commercial Internet Service Provider (CISP – Cable One) for outages and maintenance. The primary representative for contacting Pearson VUE to troubleshoot software and resolve test center issues.

1.3.2. The Government will provide all hardware and software deemed as necessary and approved for the performance of this work and connectivity to the internet.

1.3.3. These duties include but are not limited to ensuring system operation, maintenance, and disposition in accordance with applicable policies and directives. Attend required technical and security training as outlined by the system and facility owners. Manage access to ISTIACC system, reporting security incidents to the Program Manager (PM) and Information System Owner (ISO), conduct weekly (as required), monthly (as required), semi-annual and annual review of system to ensure compliance with applicable security requirements (e.g. Security Technical Implementation Guide (STIGs)) and provide a compliance report or get-well plan (Plan of Actions & Milestones (POA&M)), if needed. Schedule and participate in Configuration Management Board (CMB) meetings, notify Pm and ISO of any changes to systems affecting security, monitor access control to recovery procedures and media, perform audits of security records as required. Complete and comply with periodic/annual training related to network or system administration as set forth by 336 TRS, 81 TRG, 81 TRW, AETC, and higher headquarters.

1.3.4. Approval of Products. All system components or products planned for use shall be approved by the Government prior to first use. All documentation and configuration information shall be maintained in an area accessible by the Government for review. All user manuals, guides, checklists, and other handouts or control documents will include only Government approved content, unless specifically approved by the Government.

1.3.5. Deliverables. All deliverables must meet professional standards and meet the requirements set forth in contract documentation. The Contractor shall be responsible for delivering all end items specified. The following items are deliverables that fall within the scope of the aforementioned tasks and all other stated deliverables (see paragraphs 1 through 1.3.4.).

1.3.5.1. Service Deliverables.

PWS Reference	Title	Date of 1st Submission	As of Date	Date of Subsequent Submission	Distribution	Copies
1.2.1.9.	Test day Report	1st Test date after start date of contract	As Required	On each testing date in support of 336 TRS courses.	336 TRS/CC, 336 TRS/DO, 336 TRS/CCF, 336 TRS – COR and 336 TRS/UUB Security+ ISs	1EA email
1.3.1.1.	Configuration Data files	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1EA
1.3.1.4.	Concept of Operations (CONOPS)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1 EA
1.3.1.4.	System Security Plan (SSP)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1 EA
1.3.1.4.	Systems Configuration Management Plan (CMP)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1 EA
1.3.1.4.	System's Contingency and Business Continuity Plan (CBCP)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1 EA
1.3.1.4.	Continuity of Operations (COOP)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1 EA
1.3.1.4.	System's Incident Response Plan (IRP)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1 EA
1.3.1.4.	Security Test Plan (STP)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO) 336 TRS – COR 336 TRS/UUB	1 EA
1.3.1.4. and 1.3.3.	Document vulnerability scans & mitigations	As Required	As Required	Weekly as required	336 TRS/CC (ISO), 336 TRS/DO, 336 TRS/UUB, 336 TRS – COR	1 EA
		As Required	As Required	Monthly as required	336 TRS/CC (ISO), 336 TRS/DO, 336 TRS/UUB, 336 TRS – COR	1 EA
		Semi-annual	As Required	Semi-annual Report	336 TRS/CC (ISO), 336 TRS/DO, 336 TRS/UUB, 336 TRS – COR	1 EA
		Annual	As Required	Annual Report	336 TRS/CC (ISO), 336 TRS/DO, 336 TRS/UUB, 336 TRS – COR	1 EA
1.3.1.4. and 1.3.3.	Plan of Actions & Milestones (POA&M)	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO), 336 TRS/DO, 336 TRS/UUB, 336 TRS – COR	1 EA
1.3.1.2.	Maintain hardware and software list	As Required	As Required	Reviewed Yearly	336 TRS/CC (ISO), 336 TRS/DO, 336 TRS/UUB, 336 TRS – COR	1 EA

1.4. PERSONNEL CATEGORIES.

1.4.1. PROJECT MANAGER.

1.4.1.1. The Contractor shall provide a Project Manager who shall be responsible for all Contractor work performed under this project. The Project Manager shall be designated as *Key Personnel* for this project. The Project Manager shall be a single point of contact for the Contracting Officer (CO) and the Contracting Officer Representative (COR). It is anticipated that the Project Manager shall be one of the senior level employees provided by the Contractor for this work effort. The name of the Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this task order. The Project Manager and all designated alternates shall be able to read, write, speak, and understand English.

1.4.1.2. The Project Manager shall be available to the COR via telephone between 0800 through 1600 hours (8:00 am through 4:00 pm CST), Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 48 hours of notification.

1.4.2. TEST ADMININSTRATOR.

1.4.2.1. The test administrator's roles shall be filled with qualified personnel who will adhere to Pearson VUE's policies and procedures to provide daily administration of Test Center, proctor exams, and register students for exam vouchers.

1.4.3. NETWORK/SYSTEM ADMINISTRATOR.

1.4.3.1. The Network/System Administrator roles shall be filled by a qualified person with technical experience in these roles and holds a current CompTIA® Security+ or equivalent certification as required by Department of Defense (DoD) Manual 8570.01-M, Information Assurance Workforce Improvement Program.

1.5. PERSONNEL REQUIREMENTS.

1.5.1. The Contractor shall provide qualified personnel to perform all requirements specified in this PWS. The Test Administrators and Network/System Administrator shall have a favorable background investigation. (See Security, 1.9). The Test Administrators and Network/System Administrator shall obtain a Common Access Card (CAC) (See Pass and Identification Requirements in contract).

1.5.2. All selected Contractor personnel assigned to work on this project shall be required to sign a non-disclosure statement regarding key aspects of the project and project content. All materials developed and data generated under this contract are the sole property of the United States

Government and may not be used for any purposes not directly associated to this contract without the express approval of the COR.

1.5.3. All personnel who perform on this contract must be certified by Pearson VUE® and provide documentation that they have attained Pearson VUE® certification in accordance with (IAW) Pearson VUE® Certified Administrator.

1.5.4. The Contractor shall not employ any person who is an employee of the United States Government, if that employment would or would appear to cause a conflict of interest.

1.5.5. Target audience of the test center will be officer and enlisted personnel from the following Air Force Specialty Codes (AFSCs): Cyber Systems Operations (3D032), Cyber Surety (3D033), Client Systems (3D131), Cyber Transport (3D132), Cyberspace Defense Operations (1B431), and Undergraduate Cyber Training [phase 1](17DX1) and other Department of Defense personnel seeking CompTIA® Security+ or International Information Systems Security Certification Consortium, Inc. (ISC)2® Certified Information Systems Security Professional (CISSP®) certification testing.

1.5.6. Availability. Contractor personnel shall be in the work area and available for work at the appointed times in accordance with paragraphs 1.5.6.1. through 1.5.6.3.

1.5.6.1. The Contractor personnel shall be assigned to the 336 TRS, 108 Phantom Street, Bldg. 4213, KAFB, MS 39534. Contractor personnel shall perform their duties as defined in the paragraph 1.2. with minimal supervisory direction. Test Administrator contractors working locations are rooms 129 and 223, and the Network/System Administrator contractor working location will be in room 340 of Thomson Hall.

1.5.6.2. Contractor personnel shall work shifts from 0600 to 1600 hours (6:00 a.m. to 4:00 p.m.) or 1500 to 2400 (3:00 p.m. to 12:00 a.m.), Monday thru Friday, depending upon the current shift requirement. Contractor personnel shall be provided reasonable advance notice of any scheduled shift requirement. The 81 TRG adheres to a compressed work schedule, which equates to 8 nine-hour days, one eight-hour day, and one down Friday per 2-week period.

Example Compressed Work Schedule:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	9 hours	9 hours	9 hours	9 hours	8 hours	
	0600-1600	0600-1600	0600-1600	0600-1600	0600-1500	
Sun	Mon	Tue	Wed	Thu	Fri	Sat
	9 hours	9 hours	9 hours	9 hours		80 hours
	0600-1600	0600-1600	0600-1600	0600-1600	CWS down day	

1.5.6.3. Holidays. Contractor personnel shall not be required to provide routine services on the following Federal holidays (or the actual day set aside for observation): New Year's Day, Martin Luther King Jr.'s Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans' Day, Thanksgiving Day, and/or Christmas Day. If performance is required for these holidays, it will be approved and scheduled in advance with the COR. If the holiday falls on a Saturday, it is observed on the preceding Friday. If the holiday falls on a Sunday, it is observed on the following Monday. If the holiday falls on a down Friday, it is observed the day prior.

1.5.7. Contractor Manpower Reporting. The Contractor shall report ALL Contractor labor hours (including subcontractor labor hours) for performance of services under this contract via a secure data collection site. The Contractor is required to completely fill in all required data fields at http://www.ecmra.mil. Reporting inputs will be for all labor executed during the performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported at any time during the FY, all data shall be reported no later than 31 October of each calendar year. Contractors may direct questions to the Contractor Manpower Reporting Application (CMRA) help desk.

1.6. SECURITY REQUIREMENTS. All Contractor Personnel employed by the Contractor in the performance of this contract, or any representative of the Contractor entering the Government installation, shall abide by all security regulations of the installation (i.e., Keesler, AFI 31-101, *Integrated Defense*). The Contractor shall sign an agreement stipulating the security requirements of this contract.

1.6.1. Base Access. The Contractor shall obtain personal identification passes for all Contractor Personnel and vehicle passes for all Contractor Personnel's personal vehicles, to include prospective Contractor Personnel, requiring entry onto KAFB. Additionally, the Contractor shall keep current, for Government inspection, a list of the names of Contractor Personnel employed on this contract. Contractor Personnel shall complete Keesler AFB Form 299, *Application for KAFB Identification Card*, and submit it through the CO to the Security Forces and Pass and Registration. Vehicle registration, proof of insurance, and a valid driver's license must be presented for all vehicles to be registered.

1.6.2. Pass and Identification Requirements. Contractor Personnel whose duties require access to KAFB computer system are required to obtain a Common Access Card (CAC). To obtain a CAC, Contractor Personnel shall coordinate with their gaining unit's security manager or the 81st Communications Squadron Consolidated Client Support Activity (CSA) at 228-376-4335.

1.6.2.1. Applicability.

a. These requirements apply to Contractor Personnel requiring entry/access to KAFB for service contracts with periods of performance (POP) exceeding 60 days when a CAC is not issued.

(1) Contract POP begins at performance start date. The POP end date is based on the contract completion date.

(2) These requirements shall be included (flow down) to subcontracts at every tier.

b. These requirements do not apply to Contractor Personnel requiring entry/access to KAFB with a POP of 60 days or less. Entry/Access to KAFB for Contractor Personnel with a POP of 60 days or less will be coordinated between the Contractor and the 81st Security Forces Squadron (81 SFS).

c. When work under this contract requires unescorted entry to controlled or restricted areas, the Contractor shall comply with AFI 31-101, *Integrated Defense*, 8 Oct 09, and AFI 31-501, *Personnel Security Program Management*, 27 Jan 05, as applicable.

d. Contractor Personnel are not covered by Federal Acquisition Regulation (FAR) 52.222-3, *Convict Labor*, for the purposes of entry/access to installations/locations.

1.6.2.2. Badging System Data Requirements.

a. The Contractor shall provide the following to the Contracting Office:

(1) "Listing of personnel requiring access/entry." The list shall contain the following:

(a) Contract number.

(b) Contract award date.

(c) POP dates.

(d) Work site(s) or location(s).

(e) Each employee's full name and Social Security Number (SSN). For those without SSNs, a working visa or Permanent Resident Card with a Resident Alien number must be provided, or base entry will be denied.

(f) Identify up to two (2) Contractor Personnel for designation as "sponsor" authorities. Badges will identify the Contractor Personnel with sponsorship privileges.

(2) Completed KAFB Form 299 shall authorize Security Forces to fingerprint Contractor Personnel and conduct additional background checks. The consent form will outline the following:

(a) The Contractor Personnel for the purpose of the KAFB Form 299.

(b) The information on the form is collected IAW 18 U.S.C. 1382 and DoD Directive 5200.8, both of which permit installation commanders to limit access to installations for security reasons.

(c) Completion of the form is voluntary.

(d) Agreement to provide a specimen of fingerprints.

(e) Awareness of a list of "disqualifying factors."

(f) Consent and authorization for Security Forces to conduct background screening and to compare fingerprints against State and Federal criminal databases.

(g) Knowing and willful false statements on the form can be punished by a fine, imprisonment, or both (10 U.S.C. 1001).

(h) The consent form shall remain valid for 24 months after the end of the contract.

b. The Contractor Personnel list and consent form(s) shall be submitted as follows:

(1) 81 SFS/PASS & ID e-mail account: 81 sfs.pass.id@us.af.mil. Personnel list must be submitted IAW the PWS. The signed KAFB Form 299 must be submitted in person to the 81 SFS/PASS & ID office.

(2) Refer questions regarding the Contractor Personnel list and KAFB Form 299 to 81 SFS/PASS & ID at 228-377-1845 or 228-377-3844.

1.6.2.3. Background Checks.

1.6.2.3.1. Upon receipt of the KAFB Form 299 with a copy of Driver's License and Social Security card, a background check will be accomplished. Background checks will be categorized as favorable or unfavorable. Unfavorable background checks contain any one of the "disqualifying factors." Any person with an unfavorable background check will be denied entry/access to the installation.

1.6.2.3.2. "Disqualifying factors" include:

a. You are or have been known to be or reasonably suspected of being a terrorist or belong to an organization with known terrorism links/support.

b. This installation is unable to verify your claimed identity.

c. You have previously been barred from access to a federal installation or stand-alone facility.

d. You are wanted by federal, state, local or civil law enforcement authorities regardless of the offense/violation.

e. You have been convicted of espionage, sabotage, treason, terrorism or murder.

f. Your name appears on federal agencies "watch lisf' or "hit lisf' for criminal/te1rnrist activity.

g. You have been convicted of a firearm or explosive violation.

h. You have been convicted of sexual assault, armed robbery, rape, child molestation, child pornography, trafficking in humans, drug possession with intent to sell, or drug distribution.

i. You have knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

j. You present a threat to the good order, discipline and morale of the installation.

1.6.2.3.3. An unfavorable background check/denial may be appealed through the 81 SFS/PASS & ID. The appeal shall include a signed letter of rebuttal and any associated supporting documentation to the 81 SFS/PASS & ID.

1.6.2.3.4. Given a reasonable cause, condition, or reason, these requirements do not circumvent the installation/location commander's unilateral authority to deny or withdraw any individual's entry/access to an installation/location.

1.6.2.3.5. Badge and Fingerprint Schedule. 81 SFS/Pass & ID will notify the Contractor upon completion of background checks. Badging and fingerprinting shall be scheduled by contacting the Contractor by phone. Contractor Personnel shall report to the 81 SFS/Pass & ID with a photo ID issued by a federal/state organization (i.e. Driver's License, State ID card, U.S. Passport, etc.). IAW the Real ID Act, Individuals will no longer be able to access Air Force installations with a state-issued identification card or driver's license from Minnesota, Missouri, Washington or American Samoa beginning 15 Aug 2016. If no approved photo ID is shown, a badge will not be issued.

1.6.2.3.6. Change in Employee Entry/Access Status (Deletions).

a. No later than five (5) workdays after a change in status for Contractor Personnel requiring entry/access, the Contractor shall return identified badges to the 81 SFS/Pass & ID.

b. The Contractor shall notify the Contractor Personnel of their change in status for entry/access.

c. Unfavorable fingerprints shall constitute immediate deactivation of the issued badge(s) to the disqualified Contractor Personnel.

(1) 81 SFS may confiscate badge(s) of the Contractor Personnel present on base at the time of the unfavorable result notification. 81 SFS may escort the Contractor Personnel from KAFB IAW Security Forces guidelines.

(2) 81 SFS/Pass &ID shall notify Contractor of an unfavorable fingerprint result and request the Contractor to return the badge IAW this PWS (unless already confiscated).

1.6.2.3.7. Badge Loss/Replacement.

a. Contractor Personnel requiring a replacement badge shall contact the 81 SFS/Pass &ID at 228-377-3844 to schedule a badge appointment.

b. Lost badge(s) require a signed letter from the Contractor and Contractor Personnel that lost the badge requesting replacement of badge(s) due to loss or damage.

1.6.2.3.8. Contract Completion, Return of Badges. No later than five workdays after contract completion, the Contractor shall return all badges to 81 SFS/Pass & ID. All badges are returned collectively by the Contractor, not incrementally/individually by the Contractor Personnel. The badge turn-in shall identify the contract name.

1.7. RECORDS. The Contractor shall create, maintain, and provide Government-owned/Contractor-held records, regardless of media, in performance of this contract IAW the following directives:

AFI 33-322, *Records Management Program*, 4 Jun 12, Incorporating Change 2, 25 May 17, and Keesler AFB Sup 1, 29 Oct 12
AFMAN 33-363, *Management of Records*, 1 Mar 08; Incorporating Change 2, 9 Jun 16, AFGM2017-01, 2 Jun 17, and Keesler Supplement, 23 Apr 15
AFI 33-364, *Records Disposition—Procedures and Responsibilities*, 22 Dec 06, Incorporating Change 1, 6 Nov 14 and AFGM2017-01, 30 Mar 17
Air Force Information Management System database (AFRIMS) (access through the Air Force Portal at https://www.my.af.mil/afrims/afrims/afrims/rims.cfm)
Air Force Electronic Records Management Solution

1.7.1. The Contractor shall segregate the Government-owned records from the Contractor-owned records and identify all records required to be created by the PWS on the AFRIMS file plans. The Contractor shall create and maintain paper and electronic records (\\52mahg-fs-106) as appropriate. The Contractor shall maintain the software and background data to retrieve official electronic Government records throughout the lifecycle of the records.

1.7.2. The Contractor maintains and disposes of records IAW the AF records disposition schedules.

1.7.3. Electronically Stored Information (ESI). The Contractor shall maintain Government owned electronic non-official records on the organizational shared network drive according the subjective

categories (example: template, common, reference material, and working files). The Contractor shall grant the base records manager access to all files located on the organizational shared network drive. The Contractor shall maintain the official electronic records on the base designated shared network drive (\\52mahg-fs-106) IAW the Air Force Electronic Records Management System and AFMAN 33-363, Chapter 6.

1.7.4. Upon completion of this contract, all Government-owned/Contractor-held records (regardless of media) received, created, maintained, or provided in the performance of the PWS shall be turned over to the Government. Background electronic data and records specified for delivery to the contracting agency must be accompanied by sufficient technical documentation and software to permit the Air Force to use the data. In the event of default or non-performance, the Government will have access to all records in order to ensure mission support is not interrupted.

1.7.5. Contractor-Owned Records. The Contractor shall maintain records that relate exclusively to the Contractor's internal business or are of a general nature not specifically related the performance of work under the contract separately from the Government-owned records.

1.7.6. Freedom of Information Act (FOIA) Program. The Contractor shall comply with the requirements of DoD 5400.7-R/AFMAN 33-302, Freedom of Information Act Program, 21 Oct 10, incorporating through Change 3, 16 May 2016, and AFGM2017-01, 15 Mar 17. If the Contractor receives a FOIA request, the Contractor shall ensure it is delivered immediately to the base FOIA manager (81 CS/SCOK) for processing. The FOIA manager will task a Government official who, as the authorized official, will make the decision on releasing Government records.

1.7.7. Privacy Act Program. The Contractor shall create, maintain, and destroy Privacy Act data IAW AFI 33-332, The Air Force Privacy and Civil Liberties Program, 12 Jan 15, Incorporating change 1, 17 Nov 16; and Privacy Act systems of records notice(s) (http://dpcld.defense.gov/Privacy/SORNs.aspx). The Contractor shall not create or maintain a Privacy Act system of records prior to public notice. If the Contractor receives a Privacy Act request, the Contractor shall be responsible for searching for the records and providing those records to a Government official who, as the authorized official, will make the decision on releasing the Government records.

1.7.8. Functional Requests. A functional request is a written request for DOD records received from any person (including a member of the public), or a business that does not cite either the FOIA or Privacy Act. The Contractor shall be responsible for searching for the records and providing those records to a Government official who, as the authorized official, will make the decision on releasing the Government records.

1.8. SECURITY.

1.8.1. Security Clearance: National Agency Check with Written Inquiries (TIER 1). As a minimum, Contractor personnel shall successfully complete a Tier 1 before operating Government-furnished workstations that have access to AF automated information systems. Requests for Contractor personnel hired at the beginning of the contract shall be submitted to the

Government not later than 45 workdays from the contract start date. Requests for Contractor personnel hired subsequent to contract start date shall be submitted to the Government not later than 10 workdays from the Contractor personnel's first duty day. Contractor personnel receiving unfavorable Tier 1's shall not be employed. The Government will submit requests for investigations on AF IMT 2583, *Request for Personnel Security Action*, at no additional cost to the Contractor. Any personnel with access to classified material will be submitted by the Contractor's Facility Security Officer (FSO) for a Secret security clearance. The Contractor shall comply with the requirements of DOD 5200.2-R, *Personnel Security Program*; AFI 31-501, *Personnel Security Program Management*, 25 Jan 05; and AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, 1 Jun 12.

1.8.2. Contractor personnel shall comply with the requirements of AFI 71-101, Volume 1, *Criminal Investigations*, 4 Feb 15 and AFI 71-101, Volume 2, *Protective Service Matters*, 23 Jan 15. These regulations require Contractor personnel to report any information or circumstances of which they are aware that may pose a threat to the security of DoD personnel, Contractor personnel, resources, and classified or unclassified Defense information to their immediate supervisor. The immediate supervisor of Contractor personnel shall brief on this requirement during initial on-base assignment and as required thereafter.

1.8.3. The Unit Security Manager will assist the Contractor with any Joint Personnel Adjudication System (JPAS) Joint Clearance and Access Verification System (JCAVS) and eQIP by Design information for inputting Tier 1's with assistance from 81 TRW/IP.

1.8.4. Security Monitoring. The Contractor shall comply with all security requirements. Submit reports, classified if appropriate, of any information coming to their attention concerning any of their employees who have been cleared or are in the process of being cleared for access to classified information, which indicates that such access or determination may not be clearly consistent with the national interest. Reports shall be submitted to the Defense Industrial Security Clearance Office (DISCO) immediately upon notification of any adverse information, change in employee's status, official investigation, or any other reason. In addition, a copy of this report shall be furnished to the Contracting Officer's Representative(s) (COR(s)) and 81 TRW Installation Commander (81 TRW/CC).

1.8.5. Listing of Employees. The Contractor shall maintain a current listing of all Contractor personnel. The list shall include Contractor personnel's names, Social Security numbers, and level of security clearance. The list will be validated and signed by the FSO and provided to the CO, COR, Base Visual Information Manager (BVIM), 81 TRW/IP, Unit Security Manager, and FSO prior to the contract start date. Updated listings shall be provided when a Contractor personnel's status or information changes. Documents will be marked as FOUO as a minimum.

1.9. PHYSICAL SECURITY. The Contractor shall safeguard all Government property, including controlled forms provided for Contractor use. At the close of each work period, Government equipment, facilities, and other valuable materials shall be secured.

1.9.1. Entry Procedures to Controlled/Restricted Areas. The Contractor shall implement local base procedures for entry to AF controlled/restricted areas where Contractor will work.

1.10. Operational Security (OPSEC).

1.10.1. OPSEC Training.

1.10.1.1. All OPSEC training shall be provided by the 81st Medical Group OPSEC Coordinator.

1.10.1.2. All Contractor personnel and Contractor Management Staff shall complete initial OPSEC training within 30 calendar days of reporting for duty.

1.10.1.3. All Contractor personnel and Contractor Management Staff shall complete annual refresher OPSEC Awareness Training.

1.10.2. Disclosure of Information.

1.10.2.1. Contractor personnel or Contract Management Staff shall not release any unclassified information to anyone outside the Contractor's organization. Unclassified information, regardless of medium (e.g., film, tape, document), pertaining to the execution of any part of this contract or any program related to this contract shall not be released unless:

1.10.2.1.1. The CO, the squadron Commander, or OPSEC Coordinator has given prior written approval; or

1.10.2.1.2. The information is otherwise in the public domain before the date of release.

1.10.2.2. Requests for authorization to release information shall identify the specific information to be released, the medium to be used, and the purpose for the release.

1.10.2.2.1. The Contractor shall submit the request to the CO, the squadron Commander, or OPSEC Coordinator at least 45 days prior to the proposed release date.

1.10.2.2.2. Contract Management Staff shall submit requests through the prime Contractor to the CO, Squadron Commander, or OPSEC Coordinator.

1.11. LEVEL I ANTI-TERRORISM (AT) AWARENESS. Level I Anti-Terrorism (AT) Awareness Training is available upon request and will be conducted by the Installation Anti-Terrorism Officer (ATO). Contact the 81st Security Forces Squadron (81 SFS/S2AT), at 228-376-6613.

1.12. SAFETY.

1.12.1. Obligations. Contractors shall comply with the Occupational Safety and Health Act (OSHA, Public Law 91-596) and the resulting standards, OSHA Standards 29 CFR 1910 and 1926. The detailed provisions of the act for accident prevention are directly applicable to all Contractor operations. Prime Contractors are also responsible for ensuring any sub-contractors also adhere to OSHA Guidance. OSHA compliance officers visit Contractor worksites on the installation.

1.12.2. Responsibilities. Following is a list of responsibilities for Contracting, Contractor, and Wing Safety personnel.

a. Contractor Responsibilities.

(1) Contractors are responsible for ensuring all industrial safety provisions are followed.

(2) Contractors must report all accidents involving Air Force people, property, or equipment damage, and any Contractor personnel injured in the performance of the Air Force contract to the CO.

(3) Take immediate corrective action to comply with safety regulations if informed of a violation by the CO.

b. Contracting Officer (CO) Responsibilities.

(1) Inform Contractor of non-compliance with safety regulations, which may cause injury to Air Force personnel or property.

(2) Notify Wing Safety of any injuries or damage to AF property reported by the Contractor, in performance of an Air Force contract.

c. Wing Safety Responsibilities.

(1) 81st Training Wing Safety Personnel will periodically monitor Contractor operations to ensure safety regulation compliance as it applies to Air Force personnel and equipment.

(2) Wing Safety personnel are available to the CO for technical assistance on matters pertaining to accident prevention.

(3) Notify the CO if a safety procedure or condition exists which requires correction by the Contractor.

1.12.3. Safety Rules. Contractors shall pay particular attention to the following safety rules and ensure strict compliance while on the installation.

a. General Safety Rules While on the Installation.

(1) Ensure adequate lighting and barricading is available and used for day and night operations.

(2) Use proper shoring during trenching operations.

(3) Post proper warning signs at indoor and outdoor operations.

(4) Secure materials when doing high work, during high winds, or when high winds are forecasted.

(5) Use warning signs, barricades, or flagmen when operations present a hazard to drivers, pedestrians, or workers.

b. Traffic Rules While on the Installation. All drivers, mobile equipment, and vehicles must comply with applicable federal, state, and local laws.

(1) Seat belts are mandatory for all passengers as well as drivers

(2) An approved bicycle helmet is required to be properly worn while riding bicycles on the installation.

(3) Drive the speed limit:

(a) Base proper speed limit is 25 mph or as posted.

(b) Housing area speed limit is 15 mph.

(c) Parking lot speed limit is 5 mph.

(4) Give full attention to the operation of the vehicle. Do not operate any form of electronic device while driving to include cellular phones, iPads, laptops, etc. Mobile electronic devices are only allowed to be utilized while driving if equipped with a hands-free option such as Bluetooth.

(5) Park in designated areas and IAW Keesler AFB Instruction (KAFBI) 31-218, *Installation Traffic Code*.

(6) No riding in the beds of trucks, buckets of front end loaders, or tandem riding on vehicles designed for one-person operation.

(7) Use safety chains in addition to towing hooks when towing equipment.

(8) Place a light on the rear of equipment being towed during the hours of darkness.

(9) Mark overhanging portions of loads with warning flags or lights.

(10) When driving or using a crane or cherry picker, be cautious around power lines crossing the road and don't position booms closer than 10 feet to overhead high voltage lines.

(11) Ensure electrical work is IAW the National Electric Code.

(12) Upon encountering troop formations on the installation:

(a) Maintain 50-foot distance behind formations until signaled to pass by the troop commander. When signed to pass troop formation, do not exceed 10 mph while passing.

(b) When passing from the front, proceed without stopping, but slow to 10 mph while passing.

1.13. SMOKING IN AETC FACILITIES. Contractors are advised that the Commander has placed restrictions on the smoking of tobacco products in AETC facilities. AFI 40-102, *Tobacco Free Living, 4 Mar 15*, outline the procedures used by the commander to control smoking in our facilities. Contractors and visitors are subject to the same restrictions as Government personnel. Smoking is permitted only in designated smoking areas.

1.14. ENVIRONMENTAL MANAGEMENT SYSTEM (EMS). All Contractor personnel shall complete Environmental Management System (EMS) Awareness training prior to commencement of any activities. Training is available through the Air Force Advanced Distributed Learning Service (ADLS), the Environmental, Safety and Occupational Health Training Network (ESOHTN), or through the Environmental Office (KBOS/CEV).

1.15. HAZARDOUS MATERIALS. In the event that hazardous materials will be used in the execution of this contract, the Contractor shall be required to obtain authorization from the Installation Hazardous Materials Management Program before ordering or purchasing the hazardous product, IAW AFI 32-7086, *Hazardous Materials Management, 2 Feb 15*. This authorization process may take up to two weeks, which should be considered in the performance period of this contract.

2. SERVICES SUMMARY (SS).

Performance Objectives	PWS Para	Performance Thresholds
1. Contractor personnel shall be in the work area and available for work at the appointed times.	1.5.6.	No more than 2 instances of tardiness or unexcused absences in one quarter
2. Test Administrators will comply with Pearson VUE®'s policies and procedures.	1.2.1.	Zero verified complaints from Pearson VUE®
3. Provide a test failure report for each test session timely and with minimal errors	1.2.1.9.	95% Compliance
4. Maintains a visible testing schedule on GFE (white board).	1.2.1.10.	100% Compliance
5. Accurately document ISTIACC system configuration changes within 30 days.	1.3.1.5.1.	100% Compliance
6. Maintain ISTIACC system operation, maintenance, and disposition in accordance with applicable policies and directives.	1.3.1.5.-1.3.1.5.4.; and 1.3.3	100% Compliance

3. GOVERNMENT-FURNISHED PROPERTY (GFP) AND/OR SERVICES.

3.1. The Government will provide the limited facilities, equipment, materials, and services listed here. Specific responsibilities are detailed in this section.

3.2. FACILITIES. The Government will furnish or make available workspace at the 336 TRS, KAFB, MS. The Government retains the authority to modify or realign facilities and space provided to the Contractor based on current or future AF guidelines for space utilization, mission requirements, and personnel requirements of the Contractor as necessary. Government facilities have been inspected for compliance with Occupational Safety and Health Administration (OSHA). No hazards have been identified for which workarounds have been established. Should a hazard be subsequently identified, the Government will correct the hazard according to base-wide Government developed and approved plans of abatement taking into account safety and health priorities. The fact that no such conditions have been identified does not warrant or guarantee that no possible hazard exists, that workaround procedures will not be necessary, or that the facilities as furnished will be adequate to meet the responsibilities of the Contractor. Compliance with OSHA and other applicable laws and regulations for the protection of employees shall be exclusively the obligation of the Contractor.

3.3. AUTOMATIC DATA PROCESSING EQUIPMENT (ADPE). The Government host unit will grant access to ADPE and training to the minimum extent necessary for mission

accomplishment. The Contractor shall use ADPE for controlling and tracking data and information, as well as any other duties related to contract performance. The Contractor shall not use Government furnished ADPE or services for non-contractual related purposes. The Contractor shall comply with all computer system security procedures required by the Government.

3.3.1. Local Area Network Access (LAN). IAW AFMAN 17-1201_AFGM2016-01, *User Responsibilities and Guidance for Information Systems*, 19 May 16, AFMAN 33-152 has been renumbered as AFMAN 17-1201, however, the rest of the content remain unchanged. Contractor personnel using unclassified automated information systems that have access to sensitive information must possess, at a minimum, a National Agency Check (NAC) or Entrance National Agency Check IAW DoD 5200.2-R, *Personnel Security Program*, 1 Jan 87, or screening IAW AFI 31-501_AFGM2016-01, *Personnel Security Program Management*, 17 Nov 16 and any updated or supplements to the policies and directives that address or state the requirements.

3.3.2. Computer Security. The Contractor shall maintain computer systems security integrity IAW AFMAN 17-1301, Computer Security (COMPUSEC), 10 Feb 17. Contractor personnel shall be required to complete testing IAW AFI 17-130, *Air Force Cybersecurity Program Management* 18 Oct 16, any updated or supplements to the policies and directives that address or state the requirements, and satisfy any other local requirements set forth by the 81st Communications Squadron (81 CS) or other Government agencies prior to being allowed access to Government computers.

3.3.3. Administrative Supplies and Special Duty Items. The Government will provide reasonable amounts of administrative supplies (e.g., office supplies) and special duty related items (e.g., deployment gear).

3.3.4. Facilities, Supplies, and Services. The 336 TRS course materials are not authorized to be stored on personal systems. The Government will provide office space, office supplies, computer equipment, and office automation software, telephone with long distance access (provided PIN code), and reproduction facilities commensurate with 336 TRS program mission needs. When required, the Government will provide laptops to enable the Contractor to conduct activities associated with this contract offsite or at alternate locations.

3.3.4.1. Source Material. Manuals, texts, briefs, and other materials associated with this PWS.

3.3.4.2. Orientation. Initial familiarization/orientation will be provided by the 336 TRS. Standard Operational Procedures (SOP) will be available to the Contractor at the place of performance.

3.4. GOVERNMENT-FURNISHED SERVICES.

3.4.1. Security Forces. The Government will provide general security service. Security Forces phone extensions are 9-1-1 for emergencies at all locations. For routine calls to the Keesler Air Force Base call the 81st Security Forces Squadron, Law Enforcement Desk at 228-376-3040, 228-376-3044 or 228-377-3045.

3.4.2. Postal or Installation Distribution. Official Government or Contractor mail that is generated as a result of performance of this contract will be handled at Government expense via the Base Information Transfer System (BITS) at KAFB, MS. The Contractor shall not use BITS to handle non-Government or non-contract-related mail.

3.5. OPSEC MATERIAL. The unit will provide a copy of the 81 TRW OPSEC Plan, along with wing and unit CILs.