AIR FORCE OFFICE OF SPECIAL INVESTIGATION (AFOSI)

PROFESSIONAL INFORMATION TECHNOLOGY (IT) SERVICES

PERFORMANCE WORK STATEMENT (PWS)

26 February 2019

Table of Contents

1.0 DESCRIPTION OF SERVICES

1.1 General. This is a non-personnel services contract to provide Information Technology (IT) Support Service to the Air Force Office of Special Investigations (AFOSI). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.2 Background. The Directorate of Warfighting Integration (XI) and Field Support Squadron/Computer Systems Operations (FSS/SCO) of the Headquarters Air Force Office of Special Investigations (AFOSI) in Marine Corp Base Quantico (MCBQ), Quantico, VA, is responsible for Information Technology (IT) support for 3500+ personnel located at 220+ locations worldwide.

AFOSI serves as a communications focal point for all AFOSI members, globally. This is accomplished via five primary operating locations. These locations include Headquarters (HQ) Quantico MCB, VA, Operating Location (OL)-A (Randolph AFB, TX), OL-B (Ramstein AFB, Germany), OL-C (Yokota AFB, Japan), and OL-D (Langley AFB, VA).

The United States Navy's Information Technology Common Services Unit (ITCSU) (via the Quantico boundary) has primary responsibility for ingress and egress network traffic that crosses its perimeter boundary; therefore, coordination between ITCSU and AFOSI IT personnel shall be a requirement. Also, AFOSI is co-located with other law enforcement and intelligence agencies so coordination with those agencies shall be required for joint efforts.

1.3 Purpose. AFOSI/XI and FSS/SCO have a requirement for the technical support and expertise necessary for enterprise IT support ranging in scope from operations and maintenance (O&M) to the support of new projects and IT Engineering. The Contractor shall provide resources at the HQ facility and interact with the government staff at the Operating Locations.

1.4 Scope. The contractor shall provide all necessary managerial, personnel, expertise, and non-personal services necessary to perform enterprise-wide IT support as defined in this PWS and in accordance with (IAW) applicable AFOSI, Air Force (AF), Department of Defense (DoD) and Intelligence Community Directive (ICD) policies, processes and regulations. This support encompasses all technical services required to support the following enclaves: Non-secure Internet Protocol Router Network (NIPRNet), the Secure Internet Protocol Router Network (SIPRNet), the Joint Worldwide Intelligence Communications System (JWICS), Special Access Program Network (SAPnet) and Testing Integration Center/Development (TIC/DEV).

AFOSI utilizes the AFNet on the NIPRNet and JWICS on the AF-JWICS Network. All other networks/systems (SIPR, SAP, TIC/DEV) are maintained and operated on an independent domain and will require full technical support. In addition to the technical

support required to sustain and maintain the enclaves, the contractor is also responsible for supporting and assisting with any network migration.

AFOSI's Enterprise Services are identified as services that are utilized in support of commands daily mission

- Active Directory (AD)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Internet
- Email
- Web
- AFOSI Learning Management System (LMS)
- OSILINK
- Investigative Information Management System (I2MS), WEB I2MS, CI2MS, WEB CI2MS
- Defense Ready
- Global Address Updates

The services necessary for the ongoing maintenance and sustainment include the following focus areas:

- Service Desk/Customer Support
- Network Engineering and Operations Management
- Systems Engineering
- System Administration
- Application Maintenance and Development
- Database Administration and Automation
- Circuit Management
- Information Assurance / Information Protection Support
- Configuration Management
- Plans and Projects
- Website Development and Administration
- Software/Hardware Maintenance and Warrant

2.0 SUMMARY OF REQUIREMENTS The following list represents cross functional requirements for all tasks outlined in this PWS.

2.1 Priority Response Matrix. The contractor shall track all requests, issues or outages in a ticket. Appendix F provides required Response and Resolution Times for tickets and provides an explanation of the different impacts to assist in determining the priority level. Response time shall begin when a ticket is opened by or assigned to the Communications Focal Point. For all other networks, response time starts at customer request and resolution time starts when the ticket is opened and ends when the ticket is closed.

2.2 Response to Incidents. Any ticket that meets the criteria of critical or high priority in the Response Matrix shall be treated as an outage. All outages shall be handled in accordance with the Notification Matrix located in Appendix C. Tickets shall be opened immediately upon report of an outage or event at the applicable priority in accordance with the Priority Response Matrix located in Appendix F. Issues affecting more than five (5) people shall be tracked on one group ticket at the appropriate priority level which accurately reflects the start time of the issue for metric purposes. All

ticket shall include a comprehensive work log of all troubleshooting, status updates, as well as list every effected known user or group by name, computer number, and time reported. The contractor shall develop and follow a troubleshooting process to improve efficiency and accuracy in problem resolution. An After Action Report (AAR) shall be completed and submitted to the government within 24 hours of resolution of all high or critical priority tickets or as requested.

2.2.1 On Call Support. Contractor personnel must be available for on-call and after-hours support during high or critical priority outages or for Authorized Service Interruptions (ASI). In cases of extreme weather or after hours support, the Government may provide the option to remotely access and resolve issues off-site.

2.3 Authorized Service Interruption (ASI). In support of operations and networks, an ASI allows for scheduled network downtime with minimum service interruptions.

An ASI(s) shall be performed between 1800ET on Friday and 1900ET on Sundays. The Government reserves the right to change the ASI time slots. ASI request forms shall be drafted by the contractor in accordance with Air Force Instruction (AFI) 33-138 and routed through appropriate channels for approval. All non-emergency ASIs must be submitted one week prior to implementation in order to allow for adequate staffing and advertising to the AFOSI command. Emergency ASI requests, as defined by FSS/SCO, shall be submitted at least 24 hours in advance. The contractor shall generate and follow an approved ASI execution plan during an ASI. The contractor shall complete an ASI checklist after each ASI to ensure best practices were used to avoid outages and identify issues quickly. An ASI checklist shall include a functional check of all network services upon completion of the ASI.

2.4 Daily Stand-Up Meetings. Each section shall be represented at daily meetings with the Field Support Squadron Commander, Chief of Network Operations, or designee. The purpose of this meeting will be a quick status of the previous day's operations and any significant events. Status data points may include the number of tickets opened, new tasking orders directives, and significant trends.

2.5 Testing Integration Center and Development (TIC/DEV). Contractor shall provide services to support the formulation, design, development, integration, testing, verification, operation, and data analysis of hardware and software, including the development and validation of technologies to enable future AFOSI missions. Tasks range from supporting mission concept design and feasibility analyses through to the production networks, the analysis of engineering data obtained from them, and the development and operation of algorithms for analyzing data. The requirement includes providing on-site multi-disciplinary engineering and management services to support the development, implementation and use of components, subsystems, software, and systems for AFOSI enclaves. All aspects of TIC/DEV infrastructure shall conform to Security Technical Implementation Guides (STIGs) requirements and all applicable IA Security Controls.

2.6.5 The AFNET Enterprise Service Desk (ESD) and Enterprise Service Unit are responsible for trouble tickets, operating system level problem resolution on migrated workstations and servers on NIPRNet. It shall be the responsibility of the contractor to work with the AFNET to resolve any outages or issues in accordance with Appendix F and to work any AFOSI specific tickets or outages including those related to AFOSI applications and services.

3.0 TASK OBJECTIVES. The following provides the overall functional objectives of this PWS:

3.1 IT Customer Support/Service Desk. As the single primary point of contact, the Service Desk is the interface between the user and the service and provides ongoing support, monitoring, and lifecycle management of incident tickets. The goal of the Service Desk is to support the agreed IT service provision by ensuring the accessibility, availability, and by performing various supporting activities such as account management, troubleshooting, etc.

In support of this goal, the contract shall provide courteous, timely and professional treatment of all customers when a problem is reported through necessary troubleshooting, elevations, collaboration and resolution. The contractor shall deliver comprehensive, end-to-end customer IT support to include transitioning, operating, maintaining, tracking, restoring, protecting, and backups. If any of the below listed items cannot be accomplished due to AFNET restrictions, then the contractor is responsible for opening tickets with the AFNET ESD and following up on the issue until it is resolved to the customer's satisfaction. The contractor shall also monitor ESD queues proactively for AFOSI tickets and resolve tickets IAW Appendix F or as requested by the Government.

3.1.1 Service Desk Requirements. Provide Service Desk management/customer support for all AFOSI computer networks and systems with an emphasis on customer services and call/ticket resolution at differing classification levels including controlled unclassified information, Secret, Top Secret, and Counter-Intelligence. The Service Desk shall be responsible for providing services and meeting metrics listed in Appendix F. Reported problems shall be posted, documented, and tracked through an Information Technology Service Management (ITSM) System including the documentation of all trouble-shooting and customer interaction in the tracking system work log. The contractor shall recognize application and technical problem trends and provide mitigation plans in order to avoid future occurrence. Customers located in the field (detachments and regions) shall be supported remotely; HQ customers shall be given hands-on support when necessary. Notify customers when there is a change in ticket status or priority or when necessary to ensure good customer service. Technicians shall attempt to contact customers three times before a ticket can be closed due to an unresponsive customer.

Contractor shall manage the service desk by providing necessary support Monday through Friday. The Service Desk operates from 0600ET to 1800ET. The Service Desk shall monitor tickets for trends and patterns indicating a significant outage or event and ensure affected customers are notified early and are updated regularly. Provide industry-standard, enterprise-wide Service Desk support for administrative and technical assistance, support of multiple software/hardware versions, training, warranty, and maintenance.

Service Desk contractor support includes the following: Accounts Management, Air Force Standard Desktop Configuration loads, and general network troubleshooting. Shall field IA policy questions and independently research and answer user questions. Resolve customers' administrative and technical communications problems and install, configure, and operate client/server devices. Perform the installation of equipment, connection of peripherals, and the installing/deleting of client level software and ensure all documentation is in accordance with AF and DoD policies, guidance, and

directives. Implement client workstation software patches, security fixes, and service releases according to local instructions. Manage and establish network user accounts. Place emphasis on first call resolution of a ticket. Support password resets, imaging of workstation, run cables from the user workstation to the Local Area Network / Unified Communications Center junction box, coordination with the Navy's ITCSU on a range of trouble ticket issues to include Voice over Internet Protocol (VoIP) phones. Recognize application and technical problem trends and provide mitigation plans in order to avoid future occurrence. Support customer requests and troubleshoot including administrative and technical assistance for all aspects and types of workstations, mobile phones, tablets, Virtual Private Network (VPN), laptops, and tier one (1) troubleshooting of Video Teleconference (VTC) / Global Video System (GVS) issues prior to escalation.

3.1.2 Executive Customer Support. The contractor shall ensure immediate attention and support is provided to the AFOSI Top Four (Executive tickets/issues). The Executive staff consist of the AFOSI Commander, Executive Director, Vice Commander, and Command Chief Master Sergeant,

3.1.3 Mobile Device Support. Administration of user account creations/deletions, configuring devices, device policy creation/management, troubleshooting/resolving problems users have with their devices, and issuing new/replacement hardware, including preparing and obtaining user signatures on US Air Force Unclassified Wireless Mobile Device User Agreements (AF Form 4433) and Temporary Issue Receipt (AF Form 1297) prior to issuing hardware. All requests to activate new lines, reactivate suspended lines, change plans, add optional services to lines, or order new equipment must be forwarded to the Government Personal Wireless Communication Systems (PWCS) Manager for approval. NOTE: Only the government PWCS can obligate the Government to expend additional funds with the service provider.

The Air Force utilizes the Blackberry Unified Endpoint Management (BUEM) software on mobile devices. The contractor shall be responsible for supporting this platform and any new platform used in the future.

3.1.4 Information Technology Service Management Best Practices. The contractor shall implement and manage a quality ITSM program. The contractor shall coordinate and carry out the activities and processes required to deliver and manage services at the level required in this PWS. This includes providing ongoing management of technology that is used to deliver and support services.

The contractor shall align IT services with changing business needs by identifying and implementing improvements to IT services that support business processes, review, analyze, and recommend improvement opportunities across the service lifecycle, maintain customer satisfaction after improvements are implemented, ensure processes have clearly defined objectives and actionable measurements, capture and document all baselines and create user guides, instructions and process flow charts.

Contractor shall implement a minimum of the following processes:

3.1.4.1 Event Management. Manage events (i.e., informational, warning, and exception) through their lifecycle. Provide the basis for operational monitoring and control.

3.1.4.2 Incident Management. Restore normal service operation in accordance with Appendix F. Minimize the adverse effects on business operations. Handle unplanned interruption to or any reduction in the quality of an IT service. Mitigate a failure in a configuration item that has not yet impacted a service. Increase visibility and communication of incidents. Develop predefined steps to handle known types of incidents via methods agreed upon by the government.

3.1.4.3 Problem Management. Manage the lifecycle of all problems from identification to removal. Understand, document, and communicate known errors and initiate actions to improve or correct the situation. Reactively minimize the adverse impacts of incidents and problems. Proactively prevent recurrence of incidents related to errors. Prevent problems and resulting incidents from happening. Eliminate recurring incidents. Minimize the impact of incidents that cannot be prevented.

3.1.4.4 Request Fulfillment. Manage the lifecycle of requests from users. Efficiently handle requests. Provide information about services to customers and users. Assist with informational requests, complaints, service related issues.

3.1.4.5 Access Management. Efficiently respond to access requests. Manage access to services based on policies and actions defined in information security management. Monitor access to services to ensure rights are not improperly used. Protect confidentiality, integrity, and availability of data and intellectual property by executing information security policies. Log and track access.

3.2 IT Network Engineering and Management. Network engineering and network management includes tasks such as building and/or implementing and executing solutions to connect workstations, servers, and peripheral devices to local area and wide area networks. It also includes, installing, configuring, operating and maintaining network equipment such as cables, switches, routers, firewalls, network monitoring devices, network management platforms, and identify network issues.

The contractor shall perform technical services on the four AFOSI operational enclaves, AFOSI to AFNET points-of-presence, and the local test/integration network. The networks shall be monitored daily via centralized network management platform(s) to identify and resolve network issues (packet loss, CPU, hard drive size, memory, trending issues, etc.).

3.2.1 Building/Implementing Network Solutions. The contractor shall design/build and implement/execute network solutions. The contractor shall deploy solutions that ride on the infrastructure within the facility, as well as existing Air Force and Joint-Service network topology designs and designated network protocols.

3.2.2 Installing and Maintaining Network Equipment. The contractor shall install, configure, and maintain network equipment. IT infrastructure shall be installed according to Building Industry Consulting Service International (BICSI) and commercial best practices. All cables shall be labeled with Termination “A” and “Z” points and in accordance with ITCSU/AF policy.

3.2.3 Troubleshooting/resolving Network Problems. The contractor shall troubleshoot and resolve problems ranging from minor to significant. The contractor shall also assist other DoD installations when troubleshooting network problems at AFOSI HQ or off-site locations.

3.2.4 Network Configuration Management. The contractor shall develop and maintain current Network Baseline Documentation as described in PWS paragraph 5.10 on the configuration of the AFOSI networks. As a baseline, current documentation shall be turned over to the contractor for their use, but the contractor shall be responsible for completing, updating and organizing documentation within six months after contract award. Afterwards, the contractor must conduct two audits per year or upon request of the Government and submit updated/final documents every six months.

3.2.5 Video Teleconference (VTC) Operations and Maintenance. VTC O&M consists of tasks such as routine, preventive, scheduled and unscheduled maintenance actions required to keep the VTC infrastructure in an operational state. It also includes the task of monitoring bridge operations and assisting customers in establishing VTC sessions.

3.2.5.1 VTC End-User Operations. The contractor shall assist AFOSI users in establishing connectivity when their own efforts fail. For the Top Four leaders (Commander, Executive Director, Vice Commander, and Command Chief Master Sergeant) of AFOSI, the contractor shall be available at the VTC location within the MCBQ Russell-Knox Building to ensure the VTC sessions are established. For off-site customers, the contractor shall be available as time permits. The contractor is also responsible for configuration and operation of the VTC management system, currently Tandberg Management Server. The contractor is required to support this capability on NIPRNet, SIPRNet, and JWICS.

The contractor is also responsible for configuration and operation of the Defense Information Systems Agency (DISA) Global Video System (GVS) hardware assigned to AFOSI and located within the Russell Knox Building and located in the various Conference Rooms.

3.2.5.2 VTC Infrastructure Operations. The contractor shall monitor operations of the Multipoint Control Units and adjust audio levels, video levels, monitor and adjust all connection issues ranging from Integrated Services Digital Network (ISDN) port connections and Internet Protocol (IP) registration at the Video Communications Server as necessary during the course of the AFOSI Top Four VTC sessions. Contractor shall support bridge connections from the Defense Integrated Systems Network Video Services for ISDN. A log shall be kept of all issues requiring down speeding, calls failed, General Officer or Equivalent VTC problems. Contractor shall take appropriate actions to ensure a transparent connection to the end users.

3.2.5.3 VTC Maintenance. The contractor shall perform routine, preventive, scheduled, and unscheduled maintenance actions required to keep the AFOSI global VTC infrastructure in an operational state. AFOSI maintains VTC end-user and infrastructure equipment on NIPRNet and SIPRNet, and only end-user equipment on JWICS.

3.3 IT Systems Engineering. IT systems engineering consists of tasks such as designing, building, and testing minor to significant IT solutions that meet customer requirements. These solutions may consist of software, hardware, and integration of software/hardware. When called upon, contractors performing systems engineering activities must be available to assist system administrators and other team members in troubleshooting IT system problems. For AFOSI, the contractor shall perform the following tasks on the four AFOSI operational enclaves and the local test/integration network.

3.3.1 IT systems Engineering. The contractor shall design, build, test, and implement software, hardware, and integrated software/hardware solutions that meet customer requirements. Solutions shall incorporate state-of-the-art technologies, industry best practices, and design and operation when advantageous to the Government.

3.3.2 Troubleshooting/Problem Resolution Assistance. Contractors performing systems engineering roles shall provide assistance to other team members comprising of both contractor and government employees, when needed.

3.3.3 System Configuration. The contractor shall develop and maintain current documentation on the configuration and testing of AFOSI IT systems. As a baseline, current documentation will be turned over to the contractor for their use but the contractor shall be responsible for completing, updating and organizing documentation within 90 days after contract award.

3.4 IT Systems Administration. IT systems administration consists of, but is not limited to, tasks such as planning for, installing, and maintaining computer systems, to include servers, storage area networks, and network attached storage. Tasks also include all industry standard roles and responsibilities such as performance monitoring and tuning, upgrading, patching, backup and recovery, troubleshooting and problem resolution. These computer systems serve in a variety of roles including email servers, database servers, web servers, file and print servers, and use of other object authentication servers. All enterprise services shall be monitored daily via centralized network management platform(s) to identify and resolve issues (server, Central Processing Unit (CPU), Hard Drive (HD) size, memory, trending issues, etc.).

3.4.1 Systems Administration. The contractor shall administer the full suite of computers servers, storage area networks, and network attached storage on the five AFOSI enclaves.

3.4.2 Configuration Management. The contractor shall manage the configuration of all servers to ensure baselines are established, and changes are tracked and logged. Active Directory (AD) and exchange topology documentation (physical/logical Visio diagrams) shall be maintained, and made available in a centralized location, on all networks. Contractor shall create a snapshot on the SIPRNet, SAPNet, JWICS and TIC/DEV enclaves within 60 days of contract award and keep them current within one week of changes. Other industry standard server configuration management principles shall be applied to capture applicable service accounts including user name and dependent services that are actively being used.

Contractor shall maintain an execution plan/schedule for system updates and patching on all networks. Include frequency, exclusions, testing conducted on patches to prevent enterprise level issues, and changes requiring ASI's in accordance with paragraph 2.3. This does not apply to NIPRNet with the exception of functional systems as those patches are tested by AFNET. Contractor shall submit plan for approval within six months after award and then keep plans current within one week of change. Other industry standard server configuration management principles shall be applied where needed.

3.4.3 Group Policy Objects Management. Ensure Group Policy Objects (GPOs) are edited offline, outside of production networks, audit changes and identify differences with GPOs before changes are

implemented. Create snapshot of GPO's on the SIPRNet, SAPNet and JWICS enclave within 30 days after contract award and then keep GPO Management current on a weekly basis.

3.5 IT Application Maintenance and Development. IT application development and maintenance shall consist of writing and assembling source code that produces a software product used by customers. Contractor shall modify previously written source code to add enhancements, fixes problems, and makes changes to ensure compatibility with current security and other configuration requirements. Quality control is applied to ensure the end product is error free and compliant with pertinent security rules. Configuration management principles are applied to ensure synchronization between source code and executable code. Also included in this section is the requirement for the contractor to assist customers in producing applications designed using systems such as Microsoft SharePoint, where code may not be produced, but rather where user configurable parameters and options are set to produce an application. Systems shall be compatible with existing and future vendor supported software and conform to compliance with DoD and USAF requirements. The software shall be enterprise deployable and manageable and all components shall be in compliance with existing and future DISA Security Technical Implementation Guides (STIGs) and security software. Further, the application or its components shall not fall out of support from any vendor during the period of use. NOTE: Any development of new, major IT system would be considered beyond the scope of this contract.

3.5.1 Application Development. The contractor shall design, build, test, implement and maintain software applications for AFOSI. Application development/testing is performed on the AFOSI development environment and moved into the production environment when approved by the Government. The larger task required in this body of work is maintaining previously written programs. When a significant new development is required, the on-site contractors shall offer technical advice and assistance when any new development is required. These programs are identified in detail in Appendix D.

3.5.2 AFOSI-owned Applications Systems. AFOSI utilizes several custom applications for mission support and communication purposes which range in uniqueness from custom developed to commercial off-the-shelf products. The contractor shall be responsible for supporting these applications including O&M, projects as approved by the Project Action Board (PAB), user support, and development work for improvements to the application which are released in quarterly patches or as required and giving technical solutions for new system requirements. Appendix D lists AFOSI custom applications with relevant information.

3.5.3 Application Design. The contractor shall assist customers in the design and implementation of applications.

3.5.4 Quality Control. The contractor shall ensure applications are developed, modified and tested to ensure minimal errors exist. The contractor shall also ensure that all code is written to be compliant with all pertinent DoD security guidelines.

3.5.5 Configuration management. The contractor shall manage the configuration of all software code to ensure baselines are established, changes are tracked and logged, and synchronization between source code and executable code. Other industry standard software configuration management principles shall be applied where needed such as protect critical data and other

resources, monitor and control software procedures and processes, automate when cost effective, ensuring reliability and redundancy of software systems, ensure products only provide the necessary features, systems should be maintainable, used critical resources effectively and efficiently, minimize development effort.

The contractor shall also maintain, in a centralized location, the following information on each application:

- Code developed for the Government in the form of an authorized version controlled code management repository
- Required technical architectures which captures relationships to other applications, hardware and systems components
- Other documentation such as: admin/user guides, technical cut sheets, Standard Operating Procedures (SOPs), database schemas and system design documents

This documentation shall be available for review within six months after contract award. Other industry standard software configuration management principles; such as monitoring and controlling software development procedures, processes, and ensuring reliable software systems shall be applied where needed.

3.5.6 Commercial Off The Shelf (COTS) Based Applications/Services.

3.5.6.1 Remedy. AFOSI currently uses Remedy Suite software primarily as an ITSM for user and internal requests. Currently, AFOSI team members use Remedy to submit, track and resolve trouble tickets related to non-AFNET/AFNET issues. The contractor shall submit tickets for AFNET related issues that require AFOSI personnel to take action and assist in resolving. The database shall also be used to track higher classification systems that do not fall under AFNET. Contractor shall provide IT application development support for Remedy. The system also provides asset management, configuration control capabilities, and incident and problem management. The contractor shall provide support to ensure ITSM/Remedy meets established requirements, and perform day-to-day software and database maintenance on the Remedy system. The contractor shall troubleshoot, identify and resolve software and database errors, and perform daily and weekly backup of Remedy servers. Application developers and database administrators must be available to on-call and/or recall during system outages or scheduled system upgrades.

3.5.6.2 Project, Workflow, Requirements, and Resource (PWRR) Manager or future replacement. PWRR Manager is a web-enabled requirements processing application that runs on Microsoft Windows 2008 Server using Microsoft Internet Information Services 6.0 or higher and Microsoft Structured Query Language (SQL) Server 2008. PWRR is a Microsoft (MS) SQL database that AFOSI uses to request IT and Communications requirements such as hardware, software, and IT projects as part of its ITSM solution. PWRR is also used to track lifecycle management of IT requirements from initial customer request to implementation. PWRR may be used by itself or in conjunction with other ITSM systems used (i.e. Remedy or other systems implemented for this purpose). The contractor shall maintain and use PWRR. Contractor shall be required to establish PWRR User accounts for routing requests for technical assessments/solutions to appropriate functional area or approvals. Contractor shall also be required to maintain the server the hosting the

database and apply all applicable Operating System and SQL patches. In the event of patch compatibility issue the contractor is required to submit a waiver or patch exemption to ensure all Information Assurance (IA security controls are met. The contractor shall use this database to request all IT requirements needed to enhance, upgrade or replace AFOSI assets. Contractor shall document appropriate technical solutions and/or offer possible courses of actions to meet customer requests.

3.5.6.3 OpenFox. AFOSI uses OpenFox software access to both the state and federal law enforcement databases. The state law enforcement database is called National Law Enforcement Telecommunications System (NLETS) and the federal is called National Criminal Information Center (NCIC). OpenFox licenses and support are provided by the Original Equipment Manufacturer (OEM) but the contractor shall be required to provide on-site assistance with maintenance and troubleshooting of the two International Business Machines Corporation (IBM) servers. Historically, this has taken very little time and effort from the on-site engineers. The following skills shall be required:

- Working knowledge of Java (ability to install and reload)
- Be available via telephone to discuss using the OpenFox configurator
- Knowledge of AIX or ability to be talked through AIX commands
- Basic knowledge of networking to understand issues as described by OEM
- Ability to physically access NCIC Servers A & B (Data Center—HQ AFOSI)
- Basic knowledge of IBM Servers (IBM 9131 Model 52A & IBM 8406 Model 70Y)

3.5.6.4 Business Intelligence/Analytics. Business Intelligence/Analytics (BI/BA) refers to the skills, technologies, applications and practices for continuous iterative exploration and investigation of past business performance to gain insight and drive business planning. BI/BA focuses on developing new insights and understanding of business performance based on data and statistical methods. BI/BA focuses on using a consistent set of metrics to both measure past performance and guide business planning, which is also based on data and statistical methods. BI/BA makes extensive use of data, statistical and quantitative analysis, explanatory and predictive modeling, and fact-based management to drive decision making; through the practice of querying, reporting, Online Analytical Processing, and (predefined) performance threshold and 'key event alerts'.

The contractor shall:

- Provide technical expertise and systems support for the successful establishment of Business Intelligence/Analytics (BI/BA) service delivery in the MS Technology Stack while leveraging and exploiting all forms of AFOSI MS Native SQL and 3rd party data stores (SQL, DB2, Oracle)
- Develop (and connectivity to) data warehouse views of all AFOSI data stores in a variety of database applications and schemas (i.e. SQL, DB2, Oracle)
- Provide the Government documentation of all relevant (BI/BA) service delivery configuration technical specifications; to include interfaces into and out of SharePoint 'Performance Point' (or other BI/BA development platforms) to third party data stores thru Microsoft Business Connectivity Services (or similar).

3.5.6.4.1 SMART-OSI on I2MS / CI2MS. The contractor shall maintain SMARTOSI on NIPR and SIPR. The contractor shall ensure the system is operational and conduct the following task:

- Compile statistics for Power Rankings, the rankings will be defined during the Requirements Gathering stage
- Produce Timeliness Reports developed using business rules
- Produce Standardized reports developed during the Requirements and Gathering Stage
- Ad hoc reporting capabilities – this would require the contractor training a small number of staff using an ad hoc query tool entitled "Query Studio". This will give the users flexibility to access data, case counts and other metrics on-the-fly and give the users the ability to answer one time questions without the support of the SMART-OSI developers
- Provide access to the Cognos Workspace (dashboard)

3.5.6.5 SharePoint Enterprise Content Management Support. The contractor shall provide O&M support for (relevant versions of) Microsoft (MS) SharePoint (SP) Enterprise Services in AFOSI SIPR and NIPR environments. The contractor shall provide all necessary systems support for the successful operations of the application at the server-level and ensure all system application files are version compliant and software patched per AF Notice To Airmen (NOTAM).

The contactor shall provide all necessary service actions and technical support to ensure all data files are backed-up to guarantee seamless recovery in case of a service disruption on data-loss event.

If MS SP is operationally utilized as a 5015.2-STD compliant records management repository, the contractor shall support the Base-level or Agency Records Manager to ensure all Official Electronic Records are maintained in accordance with AFI 33-332 and relevant Federal and DoD policy and procedures. If data files (Official Records and general content) are identified for systems Migration, the contractor shall complete the successful migration of the data without service disruption.

The contractor shall develop and maintain operational procedures and systems/service-level architectures as required during the implementation of SP application services, and as components and business processes are enhanced and expanded; to include producing activity logs to document operations and maintenance.

The contractor shall comply with the scope of the O&M server-side SP responsibilities following AF established standard operating procedures as for all other applications hosted by AFOSI at Russell Knox Building, Quantico, VA. The contractor shall provide the Government SharePoint Program Manager documentation of SP Systems, (COTS or Custom) Software and/or Application configuration technical specifications; to include interfaces into and out of SP. The contractor shall provide SharePoint consultations and expertise as requested.

The contractor shall provide technical assistance in the development, testing, and implementation of all approved projects residing on any of AFOSI's SP environments. This includes creating, updating and removing all SP components (i.e. sites, pages, libraries, lists, workflows, web parts).

3.6 AFOSI Classified Website Presence. AFOSI maintains websites on three classified networks: SIPRNET, SAPnet and JWICS. These websites provide a variety of information and services for AFOSI personnel, and serve as AFOSI's primary means of analytical dissemination to the operations and intelligence communities. The contractor shall further design, develop, and maintain these websites with guidance provided by AFOSI PM on functionality, content, ease of use, continuity between networks, and aesthetic suitability. The contractor shall facilitate the publication of new content and production to ensure compliance with community policies and directives.

3.6.1 SIPRNet Web Presence. AFOSI's SIPRNet website serves as the primary means of information and intelligence distribution to the operational community. This website hosts the bulk of AFOSI's analytical production workflow, providing a method to receive support requests, managing the requests and corresponding analytical products, and providing for the formal publication of products. The website provides a search mechanism, allowing users to locate and retrieve products meeting their criteria. These websites are also leveraged to provide access to various other resources, largely consisting of static pages and a handful of existing web-applications. AFOSI is in the process of migrating a significant portion of the SIPRNet web requirements to SharePoint. Upon the implementation of SharePoint, it is expected that content producers (users) would be provided the ability to update and publish website content without direct support from the contractor. Within SharePoint, the contractor shall provide content management support to facilitate the continued distribution of AFOSI analytical production, user access to AFOSI owned web-based resources. Until this time, the contractor shall update and publish content as needed.

3.6.2 JWICS Web Presence. AFOSI's JWICS website is largely a mirrored subset of the SIPRNet website, specifically geared toward the intelligence community. A production workflow is not maintained on JWICS, however AFOSI analytical products must also be published in accordance with community policies. The contractor shall design and implement a mechanism that allows users to mirror SIPRNet published products, as well as publish directly to JWICS.

3.6.3 SAPnet Web Presence. AFOSI SAPnet is a vastly smaller website (a handful of static pages) with very limited distribution. Currently severely out-of-date, this small set of pages requires re-design and updating. After the initial re-design, updates to these pages will be extremely sporadic. The contractor shall update/maintain these pages as needed, with input provided by AFOSI ICON.

3.6.4 Web Requirements for Maintenance on all networks. Current production levels provide approximately 3-6 publications weekly, though this may vary. Content update requests are generally sporadic, often less than ten per month. Initial development/design efforts to establish the necessary systems will likely require the contractor to develop less than 50 individual webpages in total, many with functional code and dynamic content. Skills required include IIS 7.5, ASP.Net, C#, SQL, Hypertext Markup Language (HTML) and XML.

3.7 Database Administration and Automation. Database administration and management responsibilities consist of managing and maintaining database management systems (DBMS) such as Oracle and MS SQL in support of above mentioned applications. DBMS management tasks include creating and managing users and roles, assigning permissions, capacity planning, troubleshooting and restoration.

3.7.1 Database Administration. The contractor shall perform all industry standard database administration roles and responsibilities including creating, installing, configuring, modifying and tuning databases on the five AFOSI enclaves. Additional duties required include ensuring that databases are backed up and can be recovered, assigning user permissions and roles, troubleshooting, performance monitoring, and capacity planning.

The databases currently in operation are identified within the AFOSI-owned Applications Systems section above. Development and maintenance tools and technologies currently include the following:

- PL/SQL
- SQL
- Oracle Database 10g, 11g
- Windows Scripts
- Batch Files
- Rich Text Formatting
- Extensible Markup Language (XML)
- Tool for Oracle Application Developers
- Windows Server 2003, 2008 and future versions
- Linux/Unix Servers
- TomCat
- Apache
- Secure File Transfer Protocol (FTP)
- MS Office Suite

3.8 Circuit Management

3.8.1 Requirements. The contractor shall submit and track Telecommunications Service Requests (TSRs) and Web Orders (WOs) via DISA, Direct Order Entry for long-haul telecommunications requirements on all three stated classification levels in accordance with DISA Circular 310-130-1. The contractor shall access and update data and receive authorization to connect telecommunications networks via the DISA's Connection Approval Process (CAP), the DISA-owned Global Information Grid (GIG) Internet Approval Process (GIAP) and System/Network Approval Process (SNAP) Databases.

The contractor shall coordinate with DISA at least five working days before the scheduled service date. The contractor shall validate service received by customers meets all details of the WO/TSR and Telecommunications Service Order (TSO) and technical parameters of the specified technical schedule in DISA Circular 300-175-9.

The contractor shall prepare and submit appropriate completion reports (delayed service, exception, ready for use, or in-effect report) within 72 hours of the service date as contained on the TSR, TSO, or Status of Acquisition Message (SAM) in accordance with DISA Circular 310-70-1. The contractor shall clear all delayed service reports and exception reports with an in-effect report after resolving any delays or exceptions. The contractor shall follow-up on any on-going efforts/issues every three days.

The contractor shall conduct an annual audit in the first contract year of all paper or automated circuit history folders for all active circuits, trunks and IT equipment. All diagrams or circuit drawings will be marked with the most current date, month and year; circuit drawings and diagrams will not have a

date older than two years from the last audit conducted. Quality Assurance audit will take place once a year to ensure Circuit history folders/files contain the following documents:

- Approval document or cross-reference to source document (AF Form 3215) for the requirement
- The Request for Service, Work Order, TSR, TSO, circuit demand, SAM, and appropriate completion report (e.g., in-effect report, delayed service report, exception report, or ready-for-use report)
- DD Form 1367, Commercial Communication Work Order (if applicable)
- DD Form 1368, Modified Use of Leased Communication Facilities (if applicable)
- Switch revision notices (if applicable)
- Circuit demands (if applicable)
- Review & Revalidation (R&R)documentation, or cross-reference to the documentation
- DD Form 1697, Circuit Parameter Test Data - Analog
- Update R&R database biannually or whenever a circuit is discontinued

3.9 IT Enterprise Cyber Surety System Engineering/Analysis. The contractor shall develop and construct network designs and system configurations for long-haul telecommunications data networks at three separate classification levels. The contractor shall plan, design, and implement Network Architecture tasks in support of providing unclassified and classified data connectivity at various bandwidths both on-site and off-site. The contractor shall configure, trouble-shoot, re-design and provide technical solutions for network hardware and software in order to overcome network outages. The contractor shall ensure completion of engineering tasks to bring data circuits into an operational state as part of the Defense Information System Agency (DISA) Circuit Provisioning process which requires all designs conforms to DISA's Configuration Control Board (CCB) and that all designs conform to DoD Ports, Protocols and Services Management. The contractor shall coordinate and collaborate with external agencies as required, such as DISA, National Security Agency (NSA), Pentagon SIPRNET Network Operations Center, Air Force Network Integration Center, and Air Force Systems Network Office, Gunter in order to complete required implementation of engineering plans.

The contractor shall draft, compile and document network designs to receive connection approval via the DISA CAP. The contractor shall access and update data via the DISA owned GIAP and SNAP Databases.

3.10 Information Assurance(IA) / Information Protection Support. IA consists of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Successful protection of AFOSI assets requires policy compliance and an understanding of the vulnerabilities humans face when interacting with information systems. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

3.10.1 Assessment and Authorization (A&A). In accordance with DoD, ICD, and AF policy, the contractor shall be responsible for building, coordinating, maintaining, changing, and keeping updated, the Risk Management Framework (RMF) Assessment and Authorization (A&A) packages for the five enclaves administered by AFOSI. The contractor shall develop and complete System

Security Documents in accordance with the DoD Information Assurance Certification and Accreditation (DIACAP) Process (e.g. DoDI 8500.1, DoDI 8510.01, NIST SP 800-53aR4; AFMAN 17-1302, and AFI 17-101), Joint Air Force -Army -Navy 6 series issuances (e.g. Joint Air Force – Army – Navy (JAFAN) 6/3, etc.), and applicable Intelligence Community issuances (e.g. ICD 503). The contractor shall draft, develop and monitor policy for the IT Enterprise Cyber Surety Division relating to the compliance, validation and assessment of the four networks (NIPRNET, SIPRNET, SAPnet and JWICS) and Major Information Technology Systems (MITS). The contractor shall maintain and update HQ's AFOSI database for assessing/managing risk, and authorizations for all AFOSI data networks, and maintain and monitor progress of AFOSI assigned IT personnel's progress in maintaining compliance with the Federal Information Security Management Act, Intelligence Community, and DoD compliance requirements. A&A documentation shall be kept current at all times in accordance with RMF, JAFAN, and ICD policy and contractor shall obtain approval prior to implementing changes. Artifacts substantiate 100% compliance with IT activities or provide appropriate waiver authority in implementing IT configurations.

3.10.2 IA Controls. The contractor shall be responsible for implementing IA controls that are within their area of responsibility, and assisting AFOSI customers with the implementation on IA controls where the IA controls fall outside of their area of responsibility. The contractor shall continuously monitor for control compliance and take immediate actions to bring systems into compliance. This includes ensuring that the latest DoD configuration standards (e.g. DISA STIG, NASA Configuration Guides, Common Criteria approved configurations, configuration specified in official orders, etc.) are applied when a system is initially deployed, whenever an operating system or application configuration changes, applications or features are added or removed, or when new standards are published. When 100% compliance with IA controls hinders mission or is not technically or fiscally possible, contractor shall document justification for control waivers or vulnerability severity downgrades.

3.10.3 Demilitarized Zone (DMZ). The DMZ is the perimeter network segment that is logically between internal and external networks. The contractor shall be responsible for implementing and maintaining the AFOSI DMZ and boundary control devices.

3.10.4 Public Key Infrastructure (PKI). The contractor shall be responsible for implementing and maintaining PKI requirements for AFOSI. PKI technologies shall be incorporated in all upgrades and replacements of IT systems when in the best interest of the Government.

3.10.5 Computer Network Defense (CND) and Computer Network Exploitation (CNE). The contractor shall be responsible for conducting Computer Network Defense (CND) actions, and Computer Network Exploitation (CNE) enabling activities. The contractor shall defend against unauthorized activity within computer networks including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. The contractor shall use computer networks to gather data from internal target or adversary information systems or networks in support of operations and intelligence collection capabilities. At the direction of command Information Assurance Officer, Cyber Surety Office or appointed Inquiry Officials, the contractor shall determine the attribution and actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein to develop incident response plans using forensically sound methods and procedures.

3.10.6 Application Security. The contractor shall be responsible for ensuring that all application deliverables comply with the DISA Application Security & Development and Database STIG, which includes the need for source code scanning and a Web Penetration Test to mitigate vulnerabilities (including as examples, SQL injections, cross-site scripting, and buffer overflows).

3.10.7 IT System Maintenance Compliance. The contractor shall be responsible for ensuring successful implementation and tracking of all Network Tasking Orders (NTO), Maintenance Tasking Orders (MTO), Time Compliance Network Orders (TCNO), NOTAM, Time Compliance Technical Order (TCTO), Data Call Orders (DCO) for the systems included in the five AFOSI enclaves identified within this PWS. All compliance orders or tasking order must be implemented by the required compliance date. If it is not possible to meet the compliance a Plan of Action and Milestone (POA&M)s must be submitted to the Field Support Squadron commander and/or Chief of Network Operations NLT one week prior to the required compliance date. The POA&M must be approved by the Government prior to being submitted to higher network operations entities such as the Network Operations Squadron or 624 Operations Center. Contractor shall report compliance in Monthly Status Report (MSR).

3.10.8 Command Cyber Readiness Inspection (CCRI). AFOSI is expecting a CCRI approximately every 18 months but has not been inspected in several years. The contractor shall review current CCRI requirements and ensure systems and their operations are compliant. Contractor shall perform self-inspections every nine months and routinely as needed. Findings shall be reported to the Information Assurance Manager (IAM), FSS Commander and Chief of Network Operations in accordance with current CCRI assessment factors. The current estimated score is around 40 – 60 but the contractor is required to achieve a score of 87 within the first six months of the contract and then achieve and maintain a score of 95 through completion of contract performance period.

3.11 Configuration Management. The contractor shall accomplish Configuration Management (CM) activities by improving and maintaining a CM program, baseline identification, change control, status accounting, and auditing. The CM process shall pertain to all networks, functions and systems in accordance with best practices. The contractor shall also conduct CCB meetings to review and coordinate change requests to custom applications. These changes may range from a change in verbiage to a change in the layout or content of an application to make the system more functional for users. Configuration management includes Network Architecture and hardware and software configuration.

The contractor shall submit final/updated configuration documents to the COR within three months of contract award. Afterwards, the contractor must conduct two audits per year or upon request of the Government and submit updated/final documents every six months.

3.11.1 Change Management. The objective of change management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure and minimize the number and impact of any related incidents upon service. Changes in the IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. regulatory changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. The contractor shall utilize Change Management to ensure standardized

methods, processes and procedures which are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes. Ensure assets required to deliver services are properly controlled. Ensure accurate and reliable information about service assets exists and is available when and where it is needed. The contractor shall:

- Create and record request for change (RFC)
- Review RFC by performing an internal technical peer review
- Assess and evaluate change
- Submit RFC to Government for approval to deploy and implement
- Coordinate change build and test
- Coordinate change deployment
- Update Government on failure or success of approved changes and any follow on courses of actions if required

3.12 IT Plans and Projects.

3.12.1 Projects. As with any enterprise-wide IT organization, there are requirements which are not daily, weekly or monthly routine requirements, but rather requirements triggered by policy changes, discovery of weakness, new technology, or a request for a new capability or modified current capability that go beyond resource allocation for standard O&M. Based on the scope and level of effort to meet these requirements they may be classified as projects or major IT efforts, some which may actually be viewed as O&M tasks. These projects shall be on networks covered by this PWS. The number and size of projects are often difficult to anticipate as they vary constantly. To mitigate this, AFOSI designates up to 10 top priorities IT projects which the contractor shall provide the adequate resources and expertise for meeting timelines in accordance with Project Plans.

3.12.2 Project Action Board (PAB) Process. AFOSI projects vary in level of effort, complexity, and resources required. In addition, implementation timelines may be negotiated with customers or mandated by higher authority which may result in reprioritization of projects and/or their delivery dates. AFOSI's IT PAB meets regularly (typically weekly) to review and validate customer requests for projects and obtain current status of the top ten projects. The PAB has representation from the various IT service providers within AFOSI, the FSS, and professional IT contract staff.

The Contractor shall provide support for project planning, management and implementation. Contractor shall be required to provide Project Management services which shall include attendance of PAB meeting, providing weekly status updates on top ten projects and submission/updating of project plans containing; work breakdown structures, required resources, risks/risk mitigation, estimated days required to complete individual tasks and overall project, etc. Some projects may require reach-back escalation to subject matter experts for completion. Projects often require specialized knowledge, skills and abilities of AFOSI's platforms, networks, applications, service, processes etc. However, adequate resources must be provided to simultaneously work projects and O&M. In addition, there may be occasional projects that requires technical resources be brought in as needed. Projects shall require knowledge, skills and abilities of, project management, Oracle, Moodle, Cognos, Linux application development, network/ system/architecture engineering, system administration, and knowledge of the various AFOSI applications presented within this PWS.

The contract Project Manager shall work with Government Project/Program Manager throughout the life of the project. After the PAB validates a new requirement, the contractor shall prepare and submit a Project Plan to the PAB for approval at the next PAB meeting or within seven duty days.

3.13 Technology Insertion. The Contractor shall investigate and analyze innovative and emerging technologies that in the most economic and efficient manner improve not only IT system performance and support but also mission performance. Changing technology, changing laws and compliance, internal governance requirements, evolving best practices and operational risk analysis all contribute to systems being in varying states of compliance and vulnerability. Systems, when deployed or refreshed default to a vulnerable or non-compliant status and must be actively configured in order to mitigate vulnerabilities and achieve compliance. Maintaining a secure environment requires continuous process improvement (CPI). CPI requires experienced personnel to constantly evaluate the existing and planned information technology environment, assess areas for improvement, make recommendations and implement directed changes.

The Contractor shall:

- Perform IT strategic planning with the government.
- Investigate emerging technologies and present alternatives to the Government.
- Document alternatives in the Technology Insertion Plan.
- Develop and coordinate detailed proposals for implementation of new technologies to the PAB for approval and funding.
- Ensure recommended alternatives are in concert with overall AF recommended and proposed technologies.
- Provide the Government with a Life Cycle Support Plan (LCSP) for all new technologies.
- Implement approved plans.

3.14 Software/Hardware Maintenance and Warranty. When Government purchased software/hardware maintenance packages are available, the contractor shall utilize the software updates and patches for software and hardware replacements as needed. The contractor shall utilize these maintenance agreements as necessary and provide feedback to the Government if any issues are experienced with unsupported technology or unresponsive services. As the party responsible for software upgrades and hardware replacements, the contractor shall utilize OEM support, track hardware in the Equipment Tracking Report, and maintain a five (5) year hardware, software, and cert refresh schedule for all equipment/applications.

Any issues outside of technical support shall be referred to the Acquisition Program Manager. Contractor shall follow AFI 33-112 for all equipment transfer. Any transfer of IT equipment (Blackberry devices, VoIP phones, PCs, laptops, servers, routers, etc.) must be coordinated through the FSS IT Equipment Custodian (ITEC) prior to the equipment leaving contractor control (i.e., being issued, installed or shipped). Contractor shall provide type of equipment, manufacturer, model, serial number and gaining point-of-contact information to the FSS ITEC when applicable. Contractor shall not accept any equipment from users other than for temporary troubleshooting and a Temporary Issue Receipt (AF Form 1297) shall be provided to the user. All faulty equipment must be returned to the user with instructions to contact their ITEC for proper disposition procedures.

4.0 SERVICE DELIVERY SUMMARY

Performance Objective	PWS Section	Performance Threshold
Contractor complies with Response and Resolution Times in Prioritization Matrix	3.1, IT Customer Support/Service Desk	No more than one infraction per month for Critical or High priorities. No more than ten total infractions per month.
Correct categorization of tickets IAW Prioritization Matrix	3.1, IT Customer Support/Service Desk	No more than one infraction per month for Critical or High priorities. No more than five total infractions per month.
NIPR, SIPR, JWICS, SAPnet Network Availability	3.2, IT Network Engineering and Operations Management	Core devices as defined by the Government must be available and functional enterprise-wide at least 99% of the time.
Documentation of Network	3.2, IT Network Engineering and Operations Management	Update of the Network documentation as changes to the network baseline occur in a centralized location within three business days of change.
Patches and Updates: Ensure all updates and patches are applied	3.2, 3.3, 3.4,	Working within 30 days of patch release. Any problems with patches shall be resolved within one business day.
Perform system administrative and maintenance functions for Domain Controllers (DC), Exchange, Internet/Intranet connectivity and functional systems/applications	3.3, IT Systems Engineering	Maintain availability of core servers (as defined by the Government) of 99% or higher.
NIPR, SIPR, JWICS, SAPnet Enterprise Server Availability	3.4, IT Systems Administration	Core devices** as defined by the Government must be available and functional enterprise-wide at least 99% of the time.

Performance Objective	PWS Section	Performance Threshold
Issue/Opportunity Discovery	3.5, IT Application Maintenance and Development	Within ten business days of discovery.
Application Metrics	3.5, IT Application Maintenance and Development	There shall be no more than two instances of failing to meet thresholds/requirements as defined in 3.5 and Appendix D for all applications
Software Update and Patch Push	3.5, IT Application Maintenance and Development	Tested/Executed: Within 30 days of release Create Solution: Within 30 days or next patch release
Daily monitoring of applications	3.5, IT Application Maintenance and Development	Application monitored daily. Issue reported to PM within same business day. Justification shall be required and approved for missed deadlines, with no more than two missed deadlines per month.
I2MS/CI2MS Specific Metrics - External Agency Data Exchange	3.5, IT Application Maintenance and Development	Accomplished 100% of the time
DIACAP	3.10, Information Assurance/Information Protection Support	No late submissions of DIACAP-supporting documents without approved waiver. No more than three DIACAP-supporting documents (artifacts) need to be reworked per month (or 5% whichever is greater).
IA Controls	3.10, Information Assurance/Information Protection Support	100% compliant and on time unless approved waiver obtained
Public Key Infrastructure (PKI)	3.10, Information Assurance/Information Protection Support	100% compliance with AF-PKI implementation within deadline/suspense, or within approved waiver or extension periods.
Command Cyber Readiness Inspection (CCRI)	3.10, Information Assurance/Information Protection Support	Score of 87 within the first six months of the contract and then achieve and maintain a score of 95 through completion of contract performance period.

Performance Objective	PWS Section	Performance Threshold
Website Availability	3.6, AFOSI Classified Website Presence	Websites shall be available to both internal and external users at least 95% of the time.
Websites shall be timely, current and comply with policy.	3.6, AFOSI Classified Website Presence	Within one week of content change requests. New products published daily until fully updated.
VTC Scheduled Upgrades/Scheduled Maintenance	3.2.5 Video Teleconference (VTC) Operations and Maintenance	Within 30 days of release.
VTC Conference Scheduling	3.2.5 Video Teleconference (VTC) Operations and Maintenance	Provide access within 24 hours for all users and within 2 hours for VIPs.

Specific metrics above may be waived/modified when the Government Contracting Officer or designee makes the determination that there are extenuating circumstances that are beyond the control of the contractor.
** Core devices - Servers that provide AD services (DNS, Exchange, DC, DHCP, file and print, web services that are utilized in support of command.)

5.0 Deliverables. The Contractor shall provide the following deliverables to the Contracting Officer or designee.

5.1 Monthly Status Report (MSR). The Contractor shall summarize its efforts on the contract over the previous month and address any issues. Reports shall be provided to the COR the fifth day of each month. The MSR shall be delivered in either the form of an updated page/site, or produced and delivered to the Government in a format compatible with (or exportable to) standard Microsoft applications for the Governments ease in reviewing or additional analysis. Reports shall include the following components:

- Current metrics with specified Key Performance Indicators (KPIs). The contractor shall report KPIs for the previous month to successfully communicate the status of contract performance metrics; (the KPI metrics are to be defined by the Government consistent with established PWS scope and deliverables; but are subject to change
- Summarize ticket statistics including number of requests received, number of trouble tickets submitted in each priority with a list of overdue high or critical tickets, average resolution time, listing of technical bulletins, information guides issued, and trend analysis information. The contactor shall also provide a break out of how many tickets are assigned to each Area Processing Center (APC) and how many tickets are resolved by each APC with the same statistics.
- Availability metrics for core servers, services and all networks. Contractor shall provide information on the general health of each network. Availability metrics shall be reported in MSR within 90 days after award. Contractor shall notate outages outside the contractor's ability to remediate.

- NTO, MTO, TCNO, NOTAM, TCTO, DCO shall be reported in MSR with completion or compliance statistics
- Project Summary - Summarize the number of Project Plans developed and number of Projects Opened/Completed. The contractor shall also provide the overall project status for each project (Green/Yellow/Red), overall percent complete, milestones completed and any unresolved technical/business issues.
- Provide a monthly list of completed RFC actions to the Configuration Control Board. List shall include details such as successes, failures and issues encountered with secondary systems as a result of the RFC action and problem areas.
- Any other information or statistics as deemed relevant by the contractor or government and requested at least five days in advance of the monthly report due date.
- Any requested changes to the proposed Staffing Matrix must be presented in the monthly report and approved by the Contracting Officer prior to being made.
- NOTE: Rolling metrics are required for all reports and consist of metrics from previous and current metrics.

5.2 Briefing materials, point papers, staff packages, reports, plans, and correspondence. As required upon request in support of meetings or projects

5.3 Meeting minutes and action items/deliverables. The contractor shall provide meeting minutes and action items/deliverables within five workdays when requested prior to meeting.

5.4 Trip report. The contractor shall submit a trip report for contractor employee(s) who complete official travel for the Government outside of the local Maryland/DC/Virginia area. If multiple contractor employees travel on the same trip, one consolidated trip report will satisfy the deliverable requirement. Trip reports shall be provided within five workdays after completion of travel.

5.5 Non-Disclosure Statements. The contractor shall submit a Standard Form 312, Non-Disclosure Statement, for the company and each contractor and/or subcontractor employee performing under this PWS no later than (NLT) the first day of performance to the COR. This shall also apply to any replacement personnel.

5.6 After Action Report (AAR). An AAR shall be completed and submitted to the Government within 24 hours of resolution of any unplanned outage documenting the start and finish time of the outage, logging the notification of the Government/customers, listing all affected systems, users or networks, cause of outage, troubleshooting steps, process improvements and any action items necessary. It shall also include input on what was done incorrectly, and a mitigation plan with suggestions for how to prevent recurrence. These recommendations/action items shall be input as tickets and corrected following the outage. AARs shall adhere to the ITSM best practices for incident management.

5.7 Authorized Service Interruption (ASI) Request and Execution Checklist. Contractor shall generate an ASI Request Form including the following information: Execution plan, planned actions, list of services affected, impact, estimated length of time, location, point of contract and ASI execution, contingency plan and any other information deemed relevant to ASI by the Government or contractor. The ASI Request shall be routed through appropriate coordination approvals. Once approved, the contractor shall follow the ASI execution plan during ASI window and complete an

ASI checklist afterward to ensure best-practices are used to avoid outages and identify issues quickly. ASI checklist shall include a functional check of all network services upon completion of the ASI. The ASI form and checklist shall be retained in a designated, centralized location within 24 hours of completion of ASI.

5.8 Equipment Tracking Report. The contractor shall create a baseline document exportable to Microsoft Excel of all network equipment within six months after award and shall be updated as changes occur. Once the baseline is captured, the contractor shall document all equipment that is installed, moved, added, changed or removed. The spreadsheet shall be retained in a designated, centralized location. The spreadsheet shall contain the following information: type of hardware (server, router, switch, etc.), hardware platform, Automated Data Processing Equipment ADPE Automated Military Justice Analysis & Management System (AMJAMS)account numbers, make and model, part number, serial number, location, purpose, warranty information, backup schedule (if relevant) and other relevant information.

5.9 Configuration Documentation. The contractor shall submit final/updated configuration documents to the COR within three months of contract award. Afterwards, the contractor must conduct two audits per year or upon request of the Government and submit updated/final documents every six months.

5.9.1 Baseline Network Configurations. Configuration templates shall be maintained for ease-of-use and quick deployment of network routers, switches, and servers. Templates shall be maintained for routers, switches, servers, VPN appliances, and other network devices as needed. If applicable, separate templates shall be maintained as required per router/switch codebase and/or platform limitations. Such templates shall provide an explanation as to the purpose and use of each configuration command. Templates shall be reviewed annually, or in conjunction with the issuance of an applicable STIGs or NTO that directs changes to router and/or switch configurations. In addition, codebase versions shall be maintained and documented for switching and routing platforms, and updated as required per IAM or Air Force Cyber / 24th AF components.

5.10 Network Baseline Documentation. The contractor shall develop and maintain current, "as-built" documentation on the configuration of the AFOSI networks. At a minimum, this shall include IP address allocation records (correlations of host addresses, subnets, network masks, and virtual local area network designations to equipment or geographical locations), rack elevations (visual depictions of location of equipment in a given rack as it is or as it will be installed), circuit diagrams (visual depictions of Open Systems Interconnection Layer 1 connectivity between network devices and end equipment), and network topology diagrams (visual depictions of AFOSI Layer 3 and 4 connectivity between network routing and switching devices supporting AFOSI connectivity). Such visual depictions/diagrams shall include as relevant information, categorical data or metadata such as site, building, floor, room, rack, and device/host name of each termination point, as well as other pertinent information as applicable such as port, host IP address, designated uplink and/or trunk port(s), protocols, management IP address, media, termination type, and any intermediate equipment such as media converters, line drivers, channel service units/data service units, or modems. The contractor shall be responsible for completing, updating and organizing documentation within six months after contract award and then kept current within three business days of change. Diagrams shall be created

using Microsoft Visio, but some data may be requested in an Excel compatible format and shall be retained in a designated, centralized location.

5.11 Standard Operating Procedures (SOP's). Include step-by-step instruction for typical, periodic tasks as requested by the Government in each major functional area. Revise/update as changes occur and submit to Government for approval. Include revision history. SOP's will be randomly inspected by the Government.

5.12 Back-up and Recovery Plan. Create back-up plan and schedule for vital data and offline tape documentation for all enclaves in a designated, centralized location. Provide a Recovery plan that illustrates recovery from catastrophic system failure utilizing data from back-ups. Additionally, provide history of past recoveries preformed whether from real world system failures or quarterly data recovery samples. Provide within six months after contract award and keep current every time plan changes.

5.13 Circuit Management Weekly Status Update. Contractor shall provide update on any pending circuit actions or circuit outages. Each item shall be separated by AFOSI unit and include the Command Communications Service Designator (CCSD), location and actions taken.

5.14 Compliance Reporting, Incident Response and Legal/Investigative Request Documentation. The contractor shall generate documents in response to incidents, orders, controls compliance and updates submitted to Defense Information Systems Agency (DISA) Vulnerability Management Systems (VMS) or the AF Compliance Tracker (ACT) or their successor systems. The contractor shall provide IA supporting documentation when requested for incident response, inquiries, or requests for information from external agencies. Format and timeline shall be dictated by order originator, policy, law and external agencies.

5.15 Project Plan. The Project Plan shall include all the following information: technical solution, timeline with breakdown of individual tasks and overall phases, level of effort, resource allocation, risk assessment and any other information deemed necessary by the PAB. Both the initial Project Plan and any subsequent changes to the Project Plan must be approved by the PAB or higher level approval authority as required. In limited cases, project plans may be requested for efforts that are not necessarily performed by the contractor. The contractor shall be responsible for meeting Government or industry regulations/standards that are applicable. The contractor shall develop project plans/work breakdown structures within seven duty days of project approval.

5.16 Weekly Project Status Reports. The contractor shall provide weekly status reports on AFOSI's top ten on-going projects as decided by the PAB. The report shall include the following: status on overall project and on individual tasks as listed in the Project Plan for each project, any new or changed risks, decision points or Government involvement required, schedule changes and other concerns or information as requested by the PAB.

5.17 Contractor's Quality Control Plan. The contractor shall develop a Quality Control Plan (QCP) which incorporates all aspects of the contract. The QCP shall be submitted to the COR within fifteen duty days after contract award and shall be kept up-to-date within five days of updates/changes.

5.18 Security Plan. The contractor shall submit a Security Implementation Plan within 30 duty days of award and must include the following minimum requirements:

- A complete list of Key Contractor Personnel to be notified in the event of a Classified Spillage as defined in DoDM 5200.01
- A list of safeguards and administrative, technical, and policy controls that will be implemented day to day by all contractor personnel
- A list outlining personnel's compliance with annual DoD Information Assurance training, including but not limited to DoD IA Cyber Awareness Challenge v 2.0, Information Protection, Force Protection, and Human Relations
- A list of all contractor personnel's current security clearance level and type of background investigation completed
- A list of contractor user roles / levels of access and a narrative or visual representation of separation of duties

5.19 Staffing Matrix. The offeror shall provide a list of staffing positions listing skills/expertise and clearances/certification that will meet all requirements with a matrix designating management hierarchy and cross functionality in their proposal. The Offeror will also demonstrate that appropriate personnel and skill levels will be positioned efficiently to carry out all requirements. The staffing matrix will be incorporated into the contract award and can only be changed via approval from the CO.

6.0 GENERAL REQUIREMENTS.

6.1 Compliance. The contractor shall comply with all Federal, State and local applicable laws, regulations, and any changes or revisions thereto. The contractor shall adhere to such laws and regulations including when they are changed or revised during the performance of this PWS. AFOSI is anticipating new Two Person Initiative (TPI) regulations which will apply to all contractors working on this effort. The contractor shall perform its own administrative services necessary to accomplish the work, i.e., internal payroll documents, internal administrative document handling, etc.

6.2 Certification Requirements. Contractors with access to DoD system must meet the certification requirements established in the DoD 8570.01-M for the category and level functions in which they are performing. All contractors must be certified in accordance with AFI 33-112. Certifications may be waived for up to 6 months at the discretion of the COR on a case by case basis.

Position category and levels as defined by the DoD 8570 as broken down by task:

- Customer Support/IT Service Desk: IAT II
- IT Network Engineering and Operations Management - Information Assurance Technical Level II
- Video Teleconference (VTC) O&M - Information Assurance Technical Level II
- IT Systems Engineering - Information Assurance Technical Level II
- IT Systems Administration - Information Assurance Technical Level II
- IT Application Maintenance and Development - At least one team member with an IAT III or IAM III qualification must directly oversee and approve all work performed by others. When this is the case, other Application Maintenance/Developers do not require more than IA

Awareness certification. Only IAT/IAM III qualified team member may perform Configuration Management duties

- Database Administration and Automation - At least one team member with an IAT III or IAM III qualification must directly oversee and approve all work performed by others. When this is the case, other Database Administrators do not require more than IA Awareness certification
- Circuit Management - Information Assurance Technical Level II
- Information Assurance/Information Protection Support - Information Assurance Technical Level III, or Computer Network Defense – Service Provider Manager
- Configuration Management - Information Assurance Management Level II, or Information Assurance Systems Architecture and Engineering Level II
- IT Plans and Projects. Project Manager - IA Awareness only.
- AFOSI Classified Website Presence - At least one team member with an IAT III or IAM III qualification must directly oversee and approve all work performed by others. When this is the case, other Web Presence Administrators do not require more than IA Awareness certification.

6.3 Security Requirements. The contractor shall comply with DD Form 254, Contract Security Classification Form and attachments, Department of Defense Contract Security Classification Specification, and DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), DoD Directive 8500.1, DoD Directive 5200.2, AFI 31-501 and AFI 33-202. The contractor shall ensure all contract personnel, three business days prior to on-site arrival, have the required security clearances and/or required background checks equal to or greater than the classified information to which they are granted access. The contractor shall work with the Information Security Program Manager (ISPM) on all security-related issues. The Contractor shall bear all costs associated with obtaining the required security clearances and/or required background investigations. All 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.

The Contractor shall implement and administer a security program to ensure that classified information and documentation are protected in accordance with the latest appropriate Security Classification Guide for each project identified in the Department of Defense Contract Security Classification Specification (DD Form 254, Attachment 1).

6.3.1 Security Requirements. All personnel shall have a minimum of a current and active TOP SECRET (TS) clearance at least three business days prior to beginning work. Service Desk in accordance with paragraph 3.1 personnel may request a temporary waiver (up to six months) from the Security Office as long as they are not exposed to material higher than SECRET level or requiring a successfully adjudicated Single Scope Background Investigation (SSBI) or equivalent during the time period of the waiver. Contractor personnel requiring access to the SAP network shall meet all SAP requirements including consenting to counterintelligence scope polygraph and be read-in as required to SAR materials. All contractors requiring access to law enforcement data requires a successfully adjudicated SSBI or equivalent. All contractors needing access to JWICS shall require TS with SCI eligibility. While not all contractor personnel shall need access to SAPnet and JWICS, the contractor shall ensure that cleared personnel are available to meet all requirements on SAPnet and JWICS.

6.3.2 Physical Security. The contractor shall be responsible for safeguarding all Government property provided for contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured.

6.3.3 Base and Building Access. The contractor shall obtain personnel identification for all employees and vehicle passes for all contractor and personal vehicles entering the Quantico Marine installation. The contractor must complete AF Form 75, Request for Visitor/Vehicle Pass and DD Form 1172, Application for Uniformed Services Identification Card and submit them to Security Forces, Pass and Registration. Vehicle registration, proof of insurance, and a valid driver's license must be presented for all vehicles to be registered. The contractor must submit a complete list of all employees performing on this contract through the Contracting Officer Representative to the Security Forces. Lost vehicle and entry passes shall be reported immediately to Security Police and the COR.

6.3.3.1 Key Control. The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Personnel no longer requiring access to locked or secure areas must turn keys into their Government COR.

6.3.3.2. In the event the provided keys are lost, the Contractor shall immediately report any occurrences of lost key cards to AFOSI Security Services Division immediately and take no further action. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the contractor's payment. In the event a master key is lost or duplicated by the contractor, all locks and keys for that system or facility shall be replaced by the Government and the total cost shall be deducted from the contractor's monthly payment.

6.3.3.3 The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's authorized employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

6.3.3.4 Lock Combinations. The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when their personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor's Quality Control Plan.

6.3.4 Retrieving Identification Media. Within 72 hours, the contractor shall retrieve all identification media, including vehicle passes from employees who depart for any reason before the contract expires; e.g., terminated for cause, retirement and provide them to the Acquisition Program Manager.

6.3.5 Contractor Identification. All contractor / subcontractor personnel shall wear company picture identification badges so as to distinguish themselves from Government employees. When conversing

with Government personnel during business meetings, over the telephone or via electronic mail, contractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractors occupying collocated space with their Government program customer shall identify their work space area with their name and company affiliation, or as a minimum, "Contractor" after name.

6.3.6 Access To Air Force Computer Systems. The contractor shall require access to Air Force computer systems (stand alone or networked); therefore, compliance with Air Force Instruction AFI 33-119 and Air Force Instruction AFI 33-202 is mandatory. Such access requires, at a minimum, a National Agency Check or Entrance National Agency Check in accordance with DoD 5200.2-R, Personnel Security Program. The offeror shall make themselves familiar with local procedures for processing such requirements, and be prepared to be in compliance on the first day of contract performance. Failure to comply with this requirement may be considered a failure to perform. Additionally, personnel with access as defined by DoD 8570.01-M shall meet applicable information assurance certification standards as established by DoD 8570.01-M.

6.3.7 Computer Security and Privacy Requirements. The contractor shall ensure all employees involved in the management, use, design, development, maintenance or operation of an application or automated information system, are informed of their security responsibilities based on their need-to-know and trained to fulfill them. Training content shall assure that all employees are versed in the rules and requirements pertaining to security of the respective Federal IT systems, which they access, operate, or manage. Training shall be consistent with guidance issued by the OMB and NIST Special Publication 800-16. New contractor employees shall be trained by the Contractor within 30 days of hire. Computer security awareness refresher training is required at least annually, or whenever there is a significant change in IT. Additional annual training is required and shall be tracked in LMS.

6.3.8 Public Law 99-474, Title 18, United States Code. Prohibits unauthorized access to United States Government Computer Systems and software. Public Law 99-474 and Chapter XXI, Section 1030 states that: Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conducts, obtains, alters, damages, destroys, or discloses information or prevents authorized use of (data or a computer owned by or operated for) Government of the United States shall be punished by a fine under this title or imprisonment for not more than ten years, or both.

6.3.9 Privacy. Performance on this contract requires that personnel have access to personal information protected under the Privacy Act. Contractor personnel are expected to observe rules and regulations regarding physical security and appropriate document handling, and adhere to the Privacy Act (5 U.S.C. Section 552a) and other applicable agency rules and regulations.

6.3.10 Right of Privacy. All activities on this system and network may be monitored, intercepted, recorded, read, copied or captured in any manner and disclosed in any manner, by authorized personnel. There is no right of privacy in this system**.** System personnel may give to law enforcement officials and potential evidence of crime found on USAF computer systems. Use of this system by any other user, authorized or unauthorized, constitutes consent to this monitoring,

interception, recording, reading, copying or capturing and disclosure. Report unauthorized use to an information systems security officer as designated by the Acquisition Program Manager.

6.3.11 System of Record. Contractors who by contract are required to operate or maintain a Privacy Act system of records must follow this Instruction. Such a Privacy Act system of record is considered to be maintained by the Air Force and is subject to AFI 33-133. System managers for offices who have contractors operating or maintaining Privacy Act system of records must identify the record system number and coordinate with the Government manager of the contract to ensure the contract contains the proper Privacy Act clauses, and as required by the Defense Acquisition Regulation and Chapter 8, AFI 33-332 5 JUNE 2013 Instruction. (See Federal Acquisition Regulation (FAR): https://www.acquisition.gov/far/current/pdf/FAR.pdf, Privacy Act Notification: 52.224-1 and Privacy Act and the Defense FAR: 52.224-2, Subpart 224.1., Protection of Individual Privacy).

6.4 Travel and Other Direct Costs (ODC). The Contractor will be required to travel Continental United States (CONUS), Outside Continental United States (OCONUS), and within the National Capital Region during the performance of this contract. The Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. All travel requires the COR approval/authorization prior to the purchase of travel tickets and hotels.

Additionally, there may be other direct cost associated with performing duties of this contract.

6.4.1 Local Travel. The contractor may be required to attend meetings or provide technical support to AFOSI field offices within the local area of assignment commuting vicinity. Local travel, such as this shall be considered a cost of doing business with the government and shall not be separately reimbursed. Local travel is considered within the 50 mile radius from the primary performance location.

6.4.2 Non-Local Travel. Contractor employees may be required to travel to various locations, both CONUS and/or OCONUS, in performance of this contract. For OCONUS travel, Contractor employees shall obtain passports, visas, and medical clearances for designated operations areas. Travel costs shall be reimbursed utilizing the Federal Travel Regulation, JTR and Standardized Regulations section 925 as applicable from FAR 31.205-46 for locality per diem rates. Contractor travel will not be reimbursed. Actual modes of transportation and costs shall be coordinated and agreed to in advance. Reimbursement shall be on a cost basis upon receipt of the invoice in Wide Area Work Flow and submission of all receipts to the COR for review. All air travel shall be booked on American-flagged carriers, unless otherwise directed by the COR.

The Contractor shall present official business travel requests for non-local travel in the form of a Travel Cost Estimate to the COR NLT five workdays prior to commencement of travel. Upon COR approval, the contractor may take the business trip. All travel reimbursement claims must be submitted no later than 30 business days after travel. No General & Administrative charges will be paid on these actual costs.

6.4.3 Other Direct Costs (ODC). This category includes equipment and training required to support the scope of this contract. The CO will submit an Equipment Purchase Request to the Contractor for

review and cost estimates. The Contractor shall submit three estimates and shall be compliant with Air Force mandated sources, such as Air Force Way (AFWay) and Network Centric Solutions-2 (NETCENTS-2). If the Contractor can obtain better value in terms of price, quality, time of delivery, and maintain all security requirements, the Contractor shall request a waiver from NETCENTS-2 Program Management Office. IT assets and materials purchased by the Contractor under this contract shall become GFE. Such purchases shall be governed by Air Force acquisition policies and regulations and requires prior CO approval. Upon CO's approval of the three estimates, the vendor shall purchase the requested items within a seven day time frame, and it shall not exceed the amount authorized by the CO.

6.5 Place of Performance. The customer base is worldwide with the primary place of performance at HQ AFOSI located at Russell-Knox Building, 27130 Telegraph Road, Quantico, Virginia 22134. Other work sites may include Joint Base Andrews, Maryland; Joint Base Anacostia-Bolling, Washington, DC; or other AFOSI approved Government worksites within a 50 mile radius from primary performance location.

6.6 Hours of Operations and Telework. The contractor is responsible for conducting business, between the hours of 0600 and 1800 Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons.

During closure, or work related issues, the COR may approve telework. All telework must be preapproved and a detailed work plan is required with all telework request.

6.6.1 Holidays. The Government office will be closed during the following holidays, except during times of emergencies in which the contractor should be available on call when needed.

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

6.7 Period of Performance. The period of performance shall be for one (1) Base Year of 12 months and four (4) 12-month option years. The Period of Performance reads as follows:

Base Year	30 June 2019 - 29 June 2020
Option Year I	30 June2020 - 29 June2021
Option Year II	30 June 2021 - 29 June 2022
Option Year III	30 June2022 - 29 June 2023
Option Year IV	30 June 2023 - 29 June 2024
-8 Clause	30 June 2024 – 29 December 2024

The Government reserves the right to extend the term of this contract in accordance with the terms and conditions contained in FAR clause 52.217-9 entitled, "Option to Extend the Term of the Contract." This is a firm fixed price contract with a period of performance of base plus four option periods inclusive of a 30 day transition period at start of the base period.

6.8 Quality Control Program. The Contractor shall establish a quality program that shall encompass all aspects of the contract. The Contractor's Quality Control Program is the means to assure that their work complies with the requirements of the contract. As a minimum, the contractor shall develop quality control procedures in a QCP that address the areas identified in the Services Delivery Summary set forth in paragraph 4.0. See also paragraph 6.3.3.4 for required content within the QCP regarding building access and key control. The QC records of inspections shall identify procedures, prevent and ensure non-recurrence of defective services being performed and the nature of corrective action taken as appropriate.

6.8.1 Quality Assurance. The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. The contractor's performance will be monitored on a continuous basis to ensure that the contractor has performed in accordance with the performance standards. Any recurrence or failure to meet the requirements outlined in this PWS will documented and reported as a failure to meet key performance measures.

6.9 Training Program. The contractor shall develop and execute a training program designed to ensure all Contractor personnel maintain currency with emerging technology and standards applicable to the tasks detailed in this PWS. In addition, contractor personnel shall be required to take mandatory annual and periodic AF directed, DISA and other DoD training, as provided by the government. Training shall include, but is not limited to: Cyber Awareness Challenge, Force Protection, Information Protection and Personally Identifiable Information (PII) Protection Training, and other training as required. As required, additional government provided training may be required and will be identified by the COR.

6.10 Contract Personnel/Staffing. The Contractor shall be responsible for employing qualified technical personnel proficient and current in their skill sets and able to perform all tasks identified in this contract. The Contractor shall manage and staff the contract with security-cleared and qualified personnel to allow their contractor personnel to perform the required tasks and maintain normal day-to-day operations. The contractor shall provide dedicated, qualified personnel to manage and execute all aspects of the PWS. Contractor shall staff personnel in a manner to avoid single points of failure.

The contractor shall:

- Present a professional appearance and maintain professional demeanor and conduct at all times.
- Conduct their work assignments IAW project schedules
- Function effectively and efficiently during extended periods of high pressure and stress.
- Function as an integral member of a team of highly trained professionals responsible for the safety and security of USAF personnel and resources.

When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential. Personnel must be available to support all areas defined within this PWS. At no time should contractor staffing affect the operations and support required.

6.11 Non-Personal Services. The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances will the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the CO immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government.

6.12 Phase In Transition. To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the 30 day phase in/ phase out periods. During phase-in, the contractor shall ensure all personnel, parts, equipment, subcontractor(s) and other efforts necessary, are on-site at and available to assume all the responsibilities to perform the requirements of this PWS at conclusion of the phase-in period. The Contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date.

6.13 Phase Out Transition. Upon notification of transition of services to a new service provider, the contractor shall cooperate and develop a plan in coordination with the new service providers plan, to provide full support for a smooth transition of the phase-out period. The contractor is fully responsible for the continued operation of all areas of effort covered by this contract during the phase out period of 30 days, unless released by the CO for such purposes of an incremental transition, the contractor shall provide sufficient experienced personnel during the phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency. Contractor shall provide all relevant documentation to the new service provider during phase out. Documentation shall include current versions of all on-going documentation listed in this PWS. In addition, contractor shall provide the status and findings of any O&M related initiatives that are in-progress including Approved Change Requests, pending Change Request actions and actual changes implemented in part, for respective initiatives.
During this period the successor contractor shall be allowed full access to all required facilities. Successor contractor personnel shall be permitted access to observe all operations and the contractor shall allow full and complete observation.

6.14 Government Furnished Equipment, Space and Information (GFI). The new contractor shall fully coordinate with the incumbent contractor and the Government to conduct and complete accountability of all Government Furnished Property/Equipment, the results of which shall be provided to the Government. The contractor shall work in a Government facility. The Government will furnish or make available an adequate number of working space, office furniture, office equipment, general office supplies, and network access. The contractor shall be provided with two

cell phones (one capable of receiving email) and laptops to conduct on-call support for after-hours issues.

GFI will include Network diagrams of all AFOSI sites, Ports and Protocols listing, Network equipment list for systems we use and maintain, Data Center rack elevations for network devices connected and maintained, SOPs and AFIs and policy guidelines for all functional areas, Architectural drawings, Change Management Plans - both AF and Navy. While AFOSI will provide many of the required deliverables, it is important to note that not all documents will be current or complete in accordance with the requirements of this PWS. These are living documents that are updated regularly but may require work and are subject to change.

6.15 Data Rights. The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the CO. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

6.16 Organizational Conflict of Interest. Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the CO and COR immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the CO to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the CO and in the event the CO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the CO may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

7.0 CONTRACTOR MANPOWER REPORTING. The Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided 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.

7.1 Reporting inputs will be for the labor executed during the period of performance for each Government Fiscal Year (FY), which runs 1 October through 30 September. While inputs may be reported 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 CMRA help desk.

7.2 Reporting Period: Contractors are required to input data by 31 October of each year.

7.3 Uses and Safeguarding of Information: Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct

labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data.

7.4 User Manuals: Data for Air Force service requirements must be input at the Air Force CMRA link. However, user manuals for government personnel and contractors are available at the Army CMRA link at http://www.ecmra.mil.

8.0 ASSOCIATE CONTRACTOR AGREEMENTS

8.1 The Contractor shall enter into Associate Contractor Agreements (ACA) for any portion of the contract requiring joint participation in the accomplishment of the Government's requirement. The agreements shall include the basis for sharing information, data, technical knowledge, expertise, and/or resources essential to the integration of efforts related to this PWS, which shall ensure the greatest degree of cooperation for the development of the program to meet the terms of the contract. Associate contractors will be identified near the start of the base year period of performance and, as necessary, during performance.

8.2 ACA's shall include the following general information:

(1) Identify the associate contractors and their relationships.
(2) Identify the program involved and the relevant Government contracts of the associate contractors.
(3) Describe the associate contractor interfaces by general subject matter.
(4) Specify the categories of information to be exchanged or support to be provided.
(5) Include the expiration date (or event) of the ACA.
(6) Identify potential conflicts between relevant Government contracts and the ACA; include agreements on protection of proprietary data and restrictions on employees.

8.3 A copy of such agreement shall be provided to the Contracting Officer for review before execution of the document by the cooperating contractors. The Contractor is not relieved of any contract requirements or entitled to any adjustments to the contract terms because of a failure to resolve a disagreement with an associate contractor. Liability for the improper disclosure of any proprietary data contained in or referenced by any agreement shall rest with the parties to the agreement, and not the Government. All costs associated with the agreements are included in the negotiated cost of this contract. Agreements may be amended as required by the Government during the performance of this contract. All ACAs shall be delivered to the Contracting Officer in accordance with PWS paragraph 7.2.

8.4 It is the intent of the Government to provide for an organized transition to ensure uninterrupted efforts throughout the assumption of responsibilities by the follow-on Contractor.

(1) When notified of contract award, the Contractor will be granted a 30-day transition. The Contractor shall execute an ACA, attend program reviews, participate in working groups, briefings, and on-site communications, and work closely with the departing contractor to assume functional responsibilities.

(2) When notified of contract completion, the Contractor shall work closely with the Government to develop a proposal to transition to either the Government or another contractor. The Government will provide the specifics, including the transition time period, of what the requirements will include at the time of the request for change. The Contractor shall execute an ACA, attend program reviews, participate in working groups, briefings, and on-site communications, and provide full disclosure of technical, cost, and programmatic information between Contractors/teams associated with meeting the various on-going requirements.

9.0 APPENDICES

Appendix A: Acronyms

AAR	After Action Report
AD	Active Directory
ADPE	Automated Data Processing Equipment
AF	Air Force
AF NOTAMS	Notice to Airmen
AFI	Air Force Instructions
AFNET	Air Force Network
AFOSI	Air Force Office of Special Investigations
AMJAMS	Automated Military Justice Analysis & Management System
APC	Area Processing Center
ASI	Authorized Service Interruption
BA	Business Analytics
BI	Business Intelligence
CAP	Connection Approval Process
CCB	Change Control Board
CCRI	Command Cyber Readiness Inspection
CI2MS	Classified Investigative Information Management System
CIO	Chief Information Officer
CM	Configuration Management
CO	Contracting Officer
CONUS	Continental United States
COR	Contracting Officer Representative
COTS	Commercial Off The Shelf
CPI	Continuous Process Improvement
DBMS	Database Management Systems
DC	Domain Controllers

DCO	Data Call Orders
D-Dex	Defense Law Enforcement Data Exchange
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIBRS	Defense Incident-based Reporting System
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoD	Department of Defense
DPS	DoD Person Search
DSAID	Defense Sexual Assault Incident Database
ECM	Enterprise Content Management
EMS	Evidence Management System
ESD	Enterprise Service Desk
FP	Functional Programing
FSS/SCO	Field Support Squadron/Computer Systems Operations
FTP	File Transfer Protocol
FY	Fiscal Year
GFI	Government Furnished Information
GIAP	Internet Approval Process
GIG	Global Information Grid
GPOs	Group Policy Objects
GVS	Global Video System
HQ	Headquarters
HTML	Hypertext Markup Language (and file extension)
I2MS	Investigative Information Management System
IA	Information Assurance
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Information Assurance Manager

IAW	In Accordance With
IBM	International Business Machines Corporation
ICD	Intelligence Community Directives
IP	Internet Protocol
ISD	Integrated Services Digital Network
IT	Information Technology
ITCSU	Information Technology Customer Support Unit
ITEM	IT Equipment Custodian
ITRG	IT Requirements Working Group
ITSM	Information Technology Service Management
JAFAN	Joint Air Force – Army – Navy
JCL	Job Control Language
JTR	Joint Travel Regulations
JWICS	Joint Worldwide Intelligence Communications System
KPIs	Key Performance Indicators
LMS	Learning Management System
MCBQ	Marine Corp Base Quantico
MOU/MOA	Memorandum of Agreement/Memorandum of Agreement
MS	Microsoft
MSR	Monthly Status Report
MTO	Maintenance Tasking Orders
NASA	National Security Agency
NCIC	National Criminal Information Center
N-Dex	National Law Enforcement Data Exchange
NIPRNET	Non-secure Internet Protocol Router Network
NLETS	National Law Enforcement Telecommunications System
NOTAM	Notice To Airmen
NTO	Network Tasking Order
O&M	Operations and Maintenance

OCI	Organizational Conflict of Interests
OCONU	Outside Continental United States
ODC	Other Direct Cost
OEM	Original Equipment Manufacturer
OL	Operating Location
PAB	Project Action Board
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestone
PWCS	Personal Wireless Communication Systems
PWRR	Project, Workflow, Requirements, and Resource
PWS	Performance Work Statement
QASP	Quality Control Plan
R&R	Review & Revalidation
RFC	Record Request for Change
SAM	Status of Acquisition Message
SAPnet	Special Access Program Network
SAR	Special Access Required
SFTP	Secured File Transfer Protocol
SIPRNET	Secure Internet Protocol Router Network
SLOC	Source Lines of Code
SNAP	System/Network Approval Process
SOP	Standard Operating Procedures
SQL	Structured Query Language
SSBI	Single Scope Background Investigation
STIGs	Security Technical Implementation Guides
TCNO	Time Compliance Network Orders
TCTO	Time Compliance Technical Order
TIC/DEV	Test Integration Center/Development
TSO	Telecommunications Service Order

TSR	Telecommunications Service Requests
TSR	Telecommunications Service Request
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video TeleConference
WO	Web Orders
XI	Warfighter Integration
XML	Extensible Markup Language

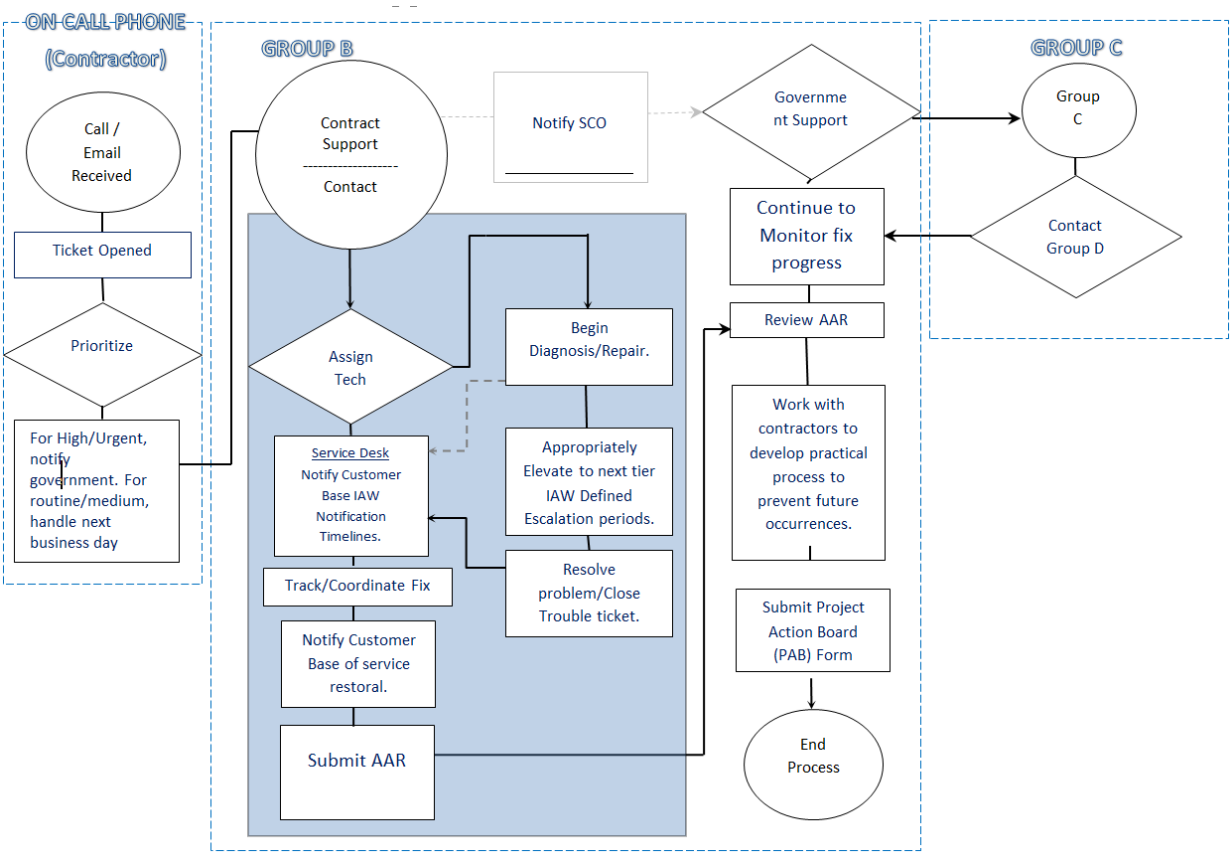
Appendix B: References

Name of Publication	Sections that Apply	Date of Publication and Changes	Title of Publication
AFI 33-152/ AFMAN 17-1201	Entire	1-Jun-12	User Responsibilities and Guidance for Information Systems
AFOSI 33-129 Sup 1	Entire	30-Jun-10	Web Management and Internet Use
AFI 17-130	Entire	19-Mar-18	Air Force Cybersecurity Program Management
AFMAN 17-1301	Entire	10-Feb-18	Computer Security (COMPUSEC)
AFI 33-322	Entire	17-Nov-16	Air Force Privacy and Civil Liberties Program
AFI 33-322 AFOSI Sup 1	Entire	13-Jan-09	Records Management Program
AFMAN 33-363	Entire	30-May-18	Management of Records
AFI 33-364	Entire	23-May-18	Records Disposition-Procedures and Responsibilities
Change Management Plan	Entire	17-Apr-12	AFOSI IT Change Management Plan (CMP)
DOD 5200.1-PH	Entire	Apr-07	DoD Guide to Marking Classified Documents
DoD 5200.2	Entire	3-Apr-17	Procedures for the DoD Personnel Security Program
DoD 8570.01-M	Entire	10-Nov-15	Information Assurance Workforce Improvement Program
JDCSISSS Rev 4	Entire	1-Jan-06	Joint DoD Intelligence Information System Cryptologic SCI Information System Security Standards
5 U.S.C. Section 552a	Entire	7-Jan-11	Privacy Act
NIST Special Publication 800-16	Entire	20-Mar-09	Information Technology Security Training Requirements

Name of Publication	Sections that Apply	Date of Publication and Changes	Title of Publication
Public Law 99-474	Title 18 and Chapter XII, Section 1030	26-Oct-01	Information Technology Systems: The Computer Fraud and Abuse Act
DoDI 8500.2	Entire	15-Jun-10	*Information Assurance (IA) Implementation*
DoDI 8551.1	Entire	28-May-14	*Ports, Protocols and Services Management*
AFI 17-203	Entire	7 Jan 2011	Information Technology (IT) Asset
1 (SPIN-1)	N/A	N/A	690th Network Support Group (690 NSG) Special Instruction
AFI 10-712	Entire	17-Dec-15	Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process
ICD 208	Entire	17-Dec-08	Write for Maximum
ICD 501	Entire	21-Jan-09	Discovery and Dissemination or Retrieval of Information within the
AFMAN 17-2101	Entire	22-May-18	Long-Haul Communications
DISAC 310-70-1	Entire	21-Apr-12	Methods and Procedures Global Information Grid
DISAC 310-130-1	Entire	4-Apr-00	Submission of Telecommunications Service Requests
TO 00-33A-1100	Entire	17-May-18	AFNET Operational Change Management
TO 00-33A-1112-WA-1	Entire	19-May-14	Methods Procedures – Air Force Network Enterprise Service Desk Service Incident Management
AFI 17-101	Entire	2-Feb-17	Risk Management Framework for AF IT
AFI 17-201	Entire	5-Mar-14	Command and Control for Cyberspace
AFMAN 17-1303	Entire	20-Mar-15	Cybersecurity Workforce
AFPD 17-2	Entire	12-Apr-16	Cyberspace Operations

Name of Publication	Sections that Apply	Date of Publication and Changes	Title of Publication
AFI 17-100	Entire	16-Sep-14	Air Force Information Technology (IT) Service Management
Joint Special Access Program Implementation Guide	Entire	11-Apr-16	Joint Special Access Program Implementation Guide

Appendix C: Notification Matrix



	Notify
Group A	FSS Operating Locations
Group B	Service Desk
	Contractor Support
	FSS-SCO
Gro	FSS-CC

	Notify
	AFOSI CIO
	Deputy CIO
Group D	AFOSI DS
	AFOSI CCE
	AFOSI CV
	AFOSI CC

- The Government reserves the right to change the notification matrix to reflect Government position or responsibility changes, as well as incorporate guidance from AFOSI, XI, or FSS leadership.

Appendix D: Custom Application Data

Investigative Information Management System (I2MS) – Web Based	
Factor	**Data**
Application Purpose and Background	The Investigative Information Management System (I2MS) is an incident-based application that allows the agent to document all investigative data and build digital case files. The web-based I2MS was launched in 2011 and approximately 5000 case files are opened annually.
Criticality of application	I2MS is the most critical application owned by AFOSI. AFOSI relies on I2MS to document all unclassified investigations, approve cases, conduct case assessments, and provide statistical reports. It is critical not to lose any capabilities or availability.
Network	NIPRnet
Security clearance requirement	SSBI investigation due to exposure to law enforcement data
Ownership of system	Government/AFOSI
Governance	I2MS configuration control, security, and IA are maintained by I2MS Program Manager (Government/AFOSI). The I2MS Program Manager chairs the monthly configuration control boards and is the final approval of any changes to the application. The Change Manager (contractor) tracks all change requests and software/database engineers maintain the data.
Code and data complexity	I2MS is an Oracle Application Express data base with approximately 200 online screens.
Stability	I2MS has an hourly repair time with minimal outside help required. The average in Functional Programing (FP) or Source Lines of Code (SLOC) is 40 - 50 modifications/improvements per quarter.
Number of concurrent users	Approximately 200 concurrent users and total of 2100 user accounts.
Application age	7.5 years

Function Points Inputs External Inputs	DEERS DoD Person Search (DPS) Web application. I2MS pulls the data from DPS when the I2MS user clicks a button. Contactor is responsible for maintenance of this automated feature.
External Outputs	The I2MS developers extract the required data from I2MS and transferred the data to the following applications via Secured File Transfer Protocol (SFTP): Defense Law Enforcement Data Exchange (D-Dex), National Law Enforcement Data Exchange (N-Dex), Defense Incident-based Reporting System (DIBRS), Defense Central Index of Investigations (DCII) and Defense Sexual Assault Incident Database (DSAID). The data pull for DCII and DSIAD occurs weekly and for the rest of applications occurs monthly. All reporting performed within I2MS is normally accomplished by SmartOSI based on data extracts from I2MS.
External Interfaces	I2MS exchange data between the following systems: Integrated Automated Fingerprint Identification System (IAFIS), Evidence Management System (EMS), and AMJAMS. Data exchange with IAFIS is automated via email file type transfers. EMS and AMJAMS are done manually where developers export and import data via SFTP.
Life expectancy	10 years/Unknown
Operating system	Server 2008, R2
Platform	Web I2MS is currently running on a VM platform using Windows Server 2012
Programming Languages	Oracle 11G (PL/SQL), Java Script J-Query
Programs	See row 1 above.
Database	See row 1 above.
COTS	N/A I2MS was custom built for AFOSI.
Average transactions per day	644 logins/day 3438 saves/day 134 deletes/day
Upgrades	Upgrades performed every 3 months. I2MS developers fix/modify the application once a quarter with approved change requests from the monthly configuration control boards.
Average help desk call volume	Tier 1: 50/month Tier 2 and 3: 120/month
Requirement/Tasks:	The contractor is expected to maintain databases, upgrade software, modify applications to meet constant change of policies and requirements, exchange data with other systems, and provide report deliverables as requested by AFOSI I2MS Program Manager. I2MS also has a training page that shall be maintained and updated as needed.
Metric: External Agency Data Exchange	Data exchange with external agencies shall be accomplished IAW external agency Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) and AFOSI policy at appropriate time intervals 100% of the time unless otherwise notified

I2MS - Legacy	
Factor	**Data**
Application Purpose and Background	The Investigative Information Management System (I2MS) is an incident-based application that allows the agent to document all investigative data and build digital case files. The Legacy I2MS is a client-based application which was launched in 2002 and approximately 4 on going cases are still maintained in this application.
Criticality of application	Mission critical. AFOSI relies on I2MS to document all unclassified investigations, approve cases, conduct case assessments, and provide statistical reports. It is critical not to lose any capabilities or availability.
Network	NIPRnet
Security clearance requirement	SSBI investigation due to exposure to law enforcement data
Ownership of system	Government/AFOSI
Governance	I2MS configuration control, security, and IA are maintained by I2MS Program Manager (Government/AFOSI). The I2MS Program Manager chairs the monthly configuration control boards and is the final approval of any changes to the application. The Change Manager (contractor) tracks all change requests and software/database engineers maintain the data.
Code and data complexity	I2MS is an Oracle Application Express data base. I2MS is primarily a Visual Basic 6 desktop application supported by an Oracle database on the server.
Stability	I2MS has an hourly repair time with minimal outside help required. Legacy I2MS is no longer modified
Number of concurrent users	Users no longer log into Legacy I2MS. A Legacy search page has been provided in Web I2MS to query existing data.
Application age	17 years
Function Points Inputs External Inputs	DEERS DPS Web application. The I2MS pulls the data from DPS when the I2MS user clicks a button. Contactor is responsible for maintenance of this automated feature.

External Outputs	All reporting performed within Legacy I2MS is normally accomplished by Defense Incident-based Reporting System, Defense Central Index of Investigations, and SmartOSI based on data extracts from I2MS. External outputs will be discontinued in the near future.
External Interfaces	I2MS exchange data with Integrated Automated Fingerprint Identification System. Data exchange with IAFIS is automated via email file type transfers.
Life expectancy	Unknown; however, no new cases created since September 2011. Upgrades and modifications are not required.
Operating system	Server 2008, R2
Platform	2008 HP standard rack-mounted server with 2TB storage
Programming Languages	Oracle 11G (PL/SQL), Java Script J-Query. The desktop application was written using Microsoft Visual Basic 6 (VB6)
Programs	See row 1 above.
Database	See row 1 above.
COTS	N/A I2MS was custom built for AFOSI.
Average transactions per day	3 logins/day 0 saves/day
Upgrades	N/A
Average help desk call volume	See Web I2MS. Call volumes were combined with Web I2MS.
Requirement/Tasks:	The contractor is expected to maintain databases, exchange data with other systems, and provide report deliverables as requested by AFOSI I2MS Program Manager.
Metric: External Agency Data Exchange	Data exchange with external agencies shall be accomplished IAW external agency MOU/MOA and AFOSI policy at appropriate time intervals 100% of the time unless otherwise notified

CI2MS – Web-Based	
Factor	**Data**
Application Purpose and Background	The Classified Investigative Information Management System (CI2MS) is an incident-based application that allows the agent to document all investigative data and build digital case files. The web-based CI2MS was launched in 2012.
Criticality of application	Mission Critical. AFOSI relies on CI2MS to document all classified investigations, approve cases, conduct case assessments, and provide statistical reports. It is critical to lose any capabilities or availability.
Network	SIPRNet
Security clearance requirement	Secret and SSBI investigation due to exposure to law enforcement data and classified information.
Ownership of system	Government/AFOSI
Governance	CI2MS configuration control, security, and IA are maintained by I2MS Program Manager (Government/AFOSI). The I2MS Program Manager chairs the monthly configuration control boards and is the final approval of any changes to the application. The Change Manager (contractor) tracks all change requests and software/database engineers maintain the data.
Code and data complexity	CI2MS is an Oracle Application Express data base with approximately 200 online screens.
Stability	CI2MS has an hourly repair time with minimal outside help required. The average (in FP or SLOC) is 40 to 50 modifications/improvements per quarter.
Number of concurrent users	Approximately 30 concurrent users and total of 1900 user accounts.
Application age	1 year
Function Points Inputs External Inputs	None
External Outputs	Reporting is normally accomplished by SmartOSI based on data extracts from Web CI2MS
External Interfaces	None
Life expectancy	10 years/Unknown

Operating system	Server 2008, R2
Platform	VM platform
Programming Languages	Oracle 11G (PL/SQL), Java Script J-Query
Programs	See row 1 above.
Database	See row 1 above.
COTS	N/A I2MS was custom built for AFOSI.
Average transactions per day	174 logins/day 1200 saves/day 27 deletes/day
Upgrades	Upgrades performed every 3 months. I2MS developers fix/modify the application once a quarter with approved change requests from the monthly configuration control boards.
Average help desk call volume	Tier 1: 70/month Tier 2 and 3: 25/month
Requirement/Tasks:	The contractor is expected to maintain databases, upgrade software, modify applications to meet constant change of policies and requirements, exchange data with other systems, and provide report deliverables as requested by AFOSI I2MS Program Manager.
Metric: External Agency Data Exchange	Data exchange with external agencies shall be accomplished IAW external agency MOU/MOA and AFOSI policy at appropriate time intervals 100% of the time unless otherwise notified

CI2MS – Legacy	
Factor	**Data**
Application Purpose and Background	The Classified Investigative Information Management System (CI2MS) is an incident-based application that allows the agent to document all investigative data and build digital case files. The Legacy CI2MS is a client-based application.
Criticality of application	Mission Critical. AFOSI relies on CI2MS to document all classified investigations, approve cases, conduct case assessments, and provide statistical reports. It is critical to lose any capabilities or availability.
Network	SIPRNet
Security clearance requirement	Secret and SSBI investigation due to exposure to law enforcement data and classified information.

Ownership of system	Government/AFOSI
Governance	CI2MS configuration control, security, and IA are maintained by I2MS Program Manager (Government/AFOSI). The I2MS Program Manager chairs the monthly configuration control boards and is the final approval of any changes to the application. The Change Manager (contractor) tracks all change requests and software/database engineers maintain the data.
Code and data complexity	CI2MS is an Oracle Application Express data base with approximately 200 online screens Legacy CI2MS uses a desktop application written primarily in VB6 supported by an Oracle database on the server.
Stability	CI2MS has an hourly repair time with minimal outside help required. Legacy CI2MS is no longer updated
Number of concurrent users	Active users of Legacy CI2MS is greatly reduced since it is no longer used to process new cases. Data is mainly accessed by HQ and Analysts for historic value.
Application age	17 years
Function Points Inputs External Inputs	None
External Outputs	Reporting is normally accomplished by SmartOSI based on data extracts from Legacy CI2MS
External Interfaces	None
Life expectancy	Unknown; however, no new cases created since June 2013. Upgrades and modifications are not required.
Operating system	Server 2008, R2
Platform	VM platform
Programming Languages	Legacy CI2MS uses a desktop application written primarily in VB6 supported by an Oracle database on the server.
Programs	See row 1 above.
Database	See row 1 above.
COTS	N/A I2MS was custom built for AFOSI.
Average transactions per day	Active users of Legacy CI2MS is greatly reduced since it is no longer used to process new cases. Data is mainly accessed by HQ and Analysts for historic value.
Upgrades	Upgrades performed every 3 months. I2MS developers fix/modify the application once a quarter with approved change requests from the monthly configuration control boards.
Average help desk call volume	See Web-CI2MS. Call volumes were combined with Web-CI2MS.

Requirement/Tasks:	The contractor is expected to maintain databases, exchange data with other systems, and provide report deliverables as requested by AFOSI I2MS Program Manager.
Metric: External Agency Data Exchange	Data exchange with external agencies shall be accomplished IAW external agency MOU/MOA and AFOSI policy at appropriate time intervals 100% of the time unless otherwise notified

Integrated Automated Fingerprint Identification System (IAFIS)	
Factor	**Data**
Application Purpose and Background	IAIFS is an FBI system that I2MS sends fingerprints with subject biographic and charges/citations.
Criticality of application	IAFIS is a critical piece of I2MS as OSI relies on it to index subjects in the FBI NCIC system. The system can also query the system to see if the users is currently in NCIC.
Network	NIPRnet
Security clearance requirement	SSBI investigation due to exposure to law enforcement data
Ownership of system	Government/AFOSI
Governance	IAFIS configuration control, security, and IA are maintained by I2MS Program Manager (Government/AFOSI). The I2MS Program Manager chairs the monthly configuration control boards and is the final approval of any changes to the application. The Change Manager (contractor) tracks all change requests and software/database engineers maintain the data.
Code and data complexity	The IAFIS system contains two programs that run as Windows services (one to send and one to receive) written in Microsoft Visual Basic 6.
Stability	IAFIS depends heavily on a network connection over the CJIS WAN to send/receive SMTP/POP3 emails to the FBI's server.
Number of concurrent users	Users do not access this application.
Application age	13 years
Function Points Inputs External Inputs	WebI2MS and Legacy I2MS have buttons that users press to send information. The IAFIS Send Service monitors the I2MS databases for data to send via SMTP. The IAFIS Response Service monitors via POP3 for return messages from IAFIS.
External Outputs	The IAFIS Send Service creates and EFT packet to send to IAFIS via SMTP.
External Interfaces	Integrated Automated Fingerprint Identification System (IAFIS).
Life expectancy	Unknown
Operating system	**1.** tvyx-as-001p - (VM - Windows Server 2008R2 Standard) - Runs IAFISReplies.exe and SendRequest.exe, connects to tvyx-as-002p to send/receive email.

Integrated Automated Fingerprint Identification System (IAFIS)	
Factor	**Data**
	2. tvyx-as-002p - Windows Server 2008R2 Standard) - Located in the DMZ runs the IPSwitch Imail Software and has a connection to the IAFIS server operated by the FBI.
Platform	2010 HP standard rack-mounted server with 2TB storage and HP Blades
Programming Languages	Microsoft Visual Basic 6
Programs	SendRequest.exe and IAFISReplies.exe
Database	Accesses the WebI2MS and Legacy I2MS Oracle Databases.
COTS	The IAFIS Send/Receive services were custom built for AFOSI.
	IPSwitch IMAIL is used on tvyxl-as-002p to send/receive email to IAFIS.
Average transactions per day	6.5 submissions per day/average 1540 submissions per year/average
Upgrades	This system is normally not touched unless absolutely needed.
Average help desk call volume	N/A N/A
Requirement/Tasks:	The contractor is expected to maintain databases, upgrade software, modify applications to meet constant change of policies and requirements, exchange data with other systems, and provide report deliverables as requested by AFOSI I2MS Program Manager.
Metric: External Agency Data Exchange	N/A

OSILink	
Factor	**Data**
Application Purpose and Background	OSILink is based on the Livelink Enterprise Information Management (EIM) System that incorporates collaborative capabilities for Document and Records Management. This EIM tool allows OSI to effectively manage documents and records using a structure environment. Users can create, manage, store, disseminate and share information across OSI. Additional capabilities of OSILink include; full text searching, audit trails and version control.
Criticality of application	Mission Essential
Network	NIPRnet, very limited on SIPRNet
Security clearance requirement	SSBI investigation due to exposure to law

OSILink	
Factor	**Data**
	enforcement data
Ownership of system -	AFOSI/XIL
Governance	Provide applications development and management support for all aspects relating to OSILink system. OSILink is developed using Livelink to manage AFOSI's Closed Case Investigation records. OSILink maintains over 1.25 million documents.
Code and data complexity	Oracle data using Open Text Enterprise Content Management (ECM) Suite software, Microsoft SQL Server and Access databases related to custom applications, provided basis. Shall require OpenText support.
Stability (I would say this is more 'Sustainability' than Stability).	OSI Link is a high availability/moderate mission critical application with a required meantime for legacy code modification and/or fix of <24 hours
Number of users	Approximately 2900 user accounts.
Application age	~ 12 years old
Initial Application initiation response time	Less than 5 seconds
Life expectancy	With SharePoint Services online, OSILink has minimal usage and Application owner will need to initiate discussion(s) on decommissioning.
Operating system	Windows 2008 R2
Platform	VMWare 6.5
Programming Languages	JAVA, O-Script, .net, etc.
Programs	Refer to programming languages
Database	Oracle
COTS	OpenText Livelink Version 9.7.1
External Data Interfaces	N/A
Internal Data Interfaces	N/A
Upgrades	Current version Livelink v 9.7.1. OSI has Livelink maintenance support.
Average help desk call volume	Approximately 300/month
Requirement/Tasks:	The contractor shall: Provide technical expertise for the successful - Maintenance and systems support of the OSILink application on the OpenText platform. - Provide service and support for any initiative to migrate official records or data content from OSI Link to another Content Management or any designated 5015.2-STD compliant records

OSILink	
Factor	**Data**
	management repository. - Provide the Government documentation of all relevant OSILink service delivery configuration technical specifications

CaseLink	
Factor	**Data**
Application Purpose and Background	CaseLink is developed to manage AFOSI's closed investigative records and track record locations within the File Room. Integrated with I2MS and an E-FOIA system, CaseLink maintains over 300,000 records utilizing OpenText Records Management technologies.
Criticality of application	Mission Essential
Network	NIPRnet
Security clearance requirement	SSBI investigation due to exposure to law enforcement data
Ownership of system -	AFOSI/XIL
Governance	Provide applications development and management support for all aspects relating to CaseLink system. CaseLink is developed using LiveLink to manage AFOSI's investigative records. Integrated with I2MS and an E-FOIA system, CaseLink maintains over 300,000 records.
Code and data complexity	Oracle data using OpenText ECM Suite software, Microsoft SQL Server and Access databases related to custom applications, provided by AFOSI. Shall require OpenText support.
Stability	99% uptime required
Number of concurrent users	20 concurrent users
Application age	11 years
Initial Application initiation response time	Less than 5 seconds
Life expectancy Operational Life	TBD – AFOSI requires support thru 2020
Operating system	Windows Server 2008 R2
Platform	VMWare 6.5
Programming Languages	OPENTEXT
Programs	Refer to programming languages

CaseLink	
Factor	**Data**
Database	Oracle
COTS	OpenText Livelink Version 9.7.1
Average transactions per day	Unknown
Interfaces	I2MS provides minimal data on archived files and participants to aid Caselink users with data entry. This is normally done bi-weekly via scripting.
External Peripheral devices	CaseLink has several barcode readers that interface I2MS records data.
Internal Data interfaces	JAVA and DOTNET
Upgrades	Current version Livelink v 9.7.1. AFOSI has Livelink support.
Average help desk call volume	15 – 30 tickets per month
Requirement/Tasks:	The contractor shall: Provide technical expertise for the successful: Maintenance and systems support of the CaseLink application on the OpenText platform. Provide service and support for the any OSI Case File document interface into CaseLink from I2MS and/or other official document repositories. Provide the Government documentation of all relevant CaseLink service delivery configuration technical specifications

CaseSync	
Factor	**Data**
Application Purpose and Background	CASESync is developed to manage AFOSI's closed investigative records and track record locations within the File Room. Integrated with CASELink, CASESync maintains over 300,000 records utilizing OpenText Records Management technologies.
Criticality of application	Mission Essential
Network	NIPRnet
Security clearance requirement	SSBI investigation due to exposure to law enforcement data
Ownership of system -	AFOSI/XIL
Governance	Provide applications development and management support for all aspects relating to CASESync system. CASESync is developed using Java to manage AFOSI's investigative records locations. Integrated with the CASELink system, CASESync maintains over 300,000 records.

CaseSync	
Factor	**Data**
Code and data complexity	CSV data is compiled from Barcode Scanners into 1 of 5 folders (each representing a specific reader) which is capable of being uploaded to CASELink as updates.
Stability	99% uptime required
Number of concurrent users	20 concurrent users
Application age	17
Initial Application initiation response time	Unknown
Life expectancy Operational Life	N/A
Operating system	Windows 7
Platform	Air Force Standard Desktop Configuration, v3.x
Programming Languages	Java, XML, Oracle
Programs	N/A
Database	N/A
COTS	N/A
Average transactions per day	Unknown
Interfaces	1Gb Ethernet
External Peripheral devices	Barcode Reader
Internal Data interfaces	JAVA and DOTNET
Upgrades	None
Average help desk call volume	Unknown
Requirement/Tasks:	

LMS	
Factor	**Data**
Application Purpose and Background	LMS is used for training, weapons compliance management, and additional duties assignment and management. It is mandatorily used

LMS	
Factor	**Data**
	by all employees of AFOSI.
Criticality of application	LMS is critical to the continuing operations of AFOSI. It houses training records provides training and tracks training without which AFOSI Special Agents may not arm with firearms.
Network	NIPRnet
Security clearance requirement	SSBI investigation due to exposure to law enforcement data
Ownership of system -	AFOSI/XIW
Governance	LMS configuration control, security, and IA are maintained by Raymond Lewis, the LMS Program Manager. Data is maintained by Raymond Lewis, with technical support from contracted senior software and database engineers.
Code and data complexity	Number of code modules by type (i.e. C, Java, JSP, PL/SQL, TCL/TK, C#, COBOL, 4GL, Pearl, etc.) • C# / VB.NET / ASP: 3003 code modules containing 354,967 lines of code • PHP: 4,863 code modules containing 662,732 lines of code • PLSQL: 44 Packages Number of reusable modules (i.e. COBOL copy book elements, C library modules, Java utility classes/libraries, Screen/HTML templates, XML modules, Job Control Language, Unix scripts, Screen resource elements, Stored Procedures, SOA web services, etc.) • PL SQL Stored Procedures: 1022 • PL SQL Functions: 26 • C# libraries: 103 • CSS files: 1,444 Number of online screens. • HTML: 626

LMS	
Factor	**Data**

	• ASP/ASPX: 1,516
	
	Number of report programs (if using COTS BI/Ad Hoc Reporting tools, provide the number and types of each module including database table views, joins, Cubes, etc.).
	
	• IBM Cognos:
	  o 7 tables
	  o 77 data elements
	  o 3 relationships (joins)
	  o 2 packages
	  o 27 reports
	
	Database definitions (i.e. number of tables, number of data elements, number of primary keys, foreign keys, number of table joins, etc.). This can be provided in the form of logical and physical data models.
	
	• Database Constraints : 1395
	• Data Elements: 4016
	• DB Link: 1
	• Foreign Keys: 238
	• Functions: 26
	• Indexes: 398
	• Objects: 10549
	• Packages: 44
	• Primary Keys: 324
	• Procedures: 1022
	• Roles: 55
	• Sequences: 141

LMS	
Factor	**Data**
	• Tables: 522 • Triggers: 139 • Types: 33 • Views: 28
Stability	The Mean Time to Repair on the legacy code: 12 hours Provide the defect density (the number of defects/DIREPS/SCRs average per Function Point or 1000 Lines of code). This is preferred by the type of code listed in the first row of this table. • This cannot be calculated unless it is specifically tracked and logged over time. The defect density is not collected for LMS. • The number of FP or SLOC modifications/improvements are not collected for LMS.
Number of concurrent users	This is not logged for LMS.
Application age	8 years
Function Points Inputs External Inputs	Function points have not been designated for LMS There are no direct external inputs. However, there shall be data uploads on a weekly basis submitted by the PM.
External Outputs	The ADOT sub-utility outputs data to a Livelink customized program called OSILINK – which utilizes an Oracle Database.
Logical Internal Files	There are no logical internal files.
External Interfaces	GUI web interface
External Inquiries	LMS outputs data to a Cognos data warehouse called SMART OSI using 12 views (predefined queries) in the LMS Oracle database.
Initial response time	The current application average response time for online applications and/or web services.

LMS	
Factor	**Data**
	• 2 seconds The expected/desired application response time for online applications and/or web services. • < 30 seconds
Life expectancy	There is no end-date identified for LMS.
Operating system	Provide a complete list of the OS and all COTS/GOTS utilities including Development Tools along with the version numbers of each. • Microsoft Windows Server 2008 Release 2 Service Pack 1 Using standard utilities provided with Windows
Platform	• HP X5650 2.67 (2 Processor) 64-Bit Server x 2 (production and testing) • 1.2TB disk space
Programming Languages	• Oracle 11g PL/SQL version 11.1.0.6 • C# version 4.0 • VB.NET version 10.0 • ASP version 3.0 • ASP.NET version 4.0.3 • PHP version 5.3.6 • HTML version 4.01 • IIS version 7
Programs	• Visual Studio 2010 version 10.0.3 • Visual SVN version 2.5.6 • Toad version 10.6

LMS	
Factor	**Data**
	• Oracle SQL Developer version 3.2.2
Database	• Oracle 11g version 11.2.0.1
COTS	• Moodle version 2.0 (Unlimited Licenses) • Meridian KSI 4.06 (5000 licenses) • Select Survey
Average transactions per day	• 400 average logins per day. • Transactions not logged for LMS
Interfaces	• Smart OSI uses Cognos to query a set of views in the LMS database on a nightly schedule. • LMS uses Open Text COTS software to connect to the OSI Link application upload, download and manage files and documents using the OSI Link Web Services API.
Upgrades	Planned as well as past history for both COTS and the applications. • LMS (Meridian KSI 4.06) has not been upgraded. • Oracle was updated from Oracle 9i to 11i • Moodle 2.0 will be upgraded to Moodle 2.6
Average help desk call volume	Provide by severity levels and the numbers that have passed from level 1 to 2 to 3. • LMS receives an average of 600 help desk requests per month, or 150 per week. o Low Severity: 598/month o Medium Severity: 1/month o High Severity: 0.5 / month o None of the tickets changed severity level.

LMS	
Factor	**Data**
LMS Courseware	LMS Contains approximately 600 courses assigned or available to AFOSI personnel for completion per policy and instruction. Courses may be assigned on a recurring basis or taken only once. The courses are taken on-line from LMS itself or from other providers, either on-line or in a classroom environment. All course completions are recorded in LMS. • SCORM 1.2 Courses – 81 o Courses created/maintained by contractor multimedia courseware developers and taken on-line via LMS. Courses are created in Trivantis Lectora and typically contain graphics and text but may contain video, audio and flash animation as well as quizzes and/or exams. Students take the courses as required; recurring courses are automatically scheduled in LMS according to a predefined interval. • Date Only Courses – 264 o Courses taken from a provider outside of LMS/AFOSI but required per policy/instruction. Students take the training in whatever format is required and upon completion upload course completion certificates and completion dates to LMS. Recurring courses are automatically scheduled in LMS according to a predefined interval. • Weapons Courses – 10 o Courses taken from certified weapons instructors on an annual or quarterly basis depending upon policy. Students enter course completion data themselves or data is imported via external data pulls which are uploaded to the LMS Oracle database and viewed via html transcripts • Classroom Courses – 284 o Courses taken in-residence from military or commercial providers.

LMS	
Factor	**Data**
	○ Designated instructors create class sections and rosters and monitor rosters for course completion/failure, etc.
Multimedia Course Developer Requirements	• Current Trivantis Lectora course creation / maintenance experience • Current Adobe Flash animation creation / maintenance experience • Current digital image creation / editing experience • Current digital audio creation / editing experience • Current digital video creation / editing experience • Current multimedia course creation/conversion experience ○ Assess customer training requirements ○ Create lesson plan ○ Create lesson story board ○ Create required imagery, audio (and narrator scripts as required), and animation to support lesson storyboard requirements ○ Author course in Trivantis Lectora ▪ Beta test course ▪ Revise as necessary ○ Provide to customer
Multimedia Developer Tasks	• Create new SCORM 1.2 courseware as required (approximately 3 times per year) • Maintain current SCORM 1.2 courseware as changed policy dictates training upgrades ○ Review and maintain approximately five courses

LMS	
Factor	**Data**
	monthly as prioritized by PM

U.S. Air Force Special Investigations Academy (USAFSIA) LMS Requirements. The U.S. Air Force Special Investigations Academy (USAFSIA) is located on the grounds of the Federal Law Enforcement Training Center (FLETC) in Glynco, Ga., where all new Air Force Office of Special Investigation recruits receive their entry-level investigative training. The Academy also conducts basic and advanced investigative courses at FLETC and several geographically separated sites. USAFSIA is accredited by the Federal Law Enforcement Training Accreditation Board (FLETA) as well as the Community College of the Air Force, a multi-campus, federally charted institution.

All course curricula documentation, student records, instructor credentials, in-residence course facilitation and instructor led on-line training is maintained via the AFOSI Command LMS utilizing a Moodle subsystem. The contractor shall upgrade and maintain the LMS Moodle subsystem together with the Meridian KSI 4.06. LMS is critical to the integrity and daily operation of USAFSIA.

SmartOSI	
Factor	**Data**
Application Purpose and Background	SMART-OSI provides important mission metrics to decision makers within the Command and outside of the Command. SMART-OSI offers a combination of analysis functions, reporting capabilities (standardized and ad hoc) and metrics (performance management) applications.
Criticality of application	SMART-OSI enhances the mission of AFOSI by providing a systematic process of delivering Air Force Criminal Data to customers at the highest levels of the Government. SMART-OSI alleviates the requirement to manually count statistical information required for various purposes. SMART-OSI's customer base often requests data with just a few hours suspense which makes delivery under the manual system within the requested timeframe impossible.
Network	NIPRnet
Security clearance requirement	A SSBI investigation or equivalent is required due to exposure to law enforcement data.
Ownership of system -	AFOSI owns the SMART-OSI program however Cognos is a COTS sold by IBM; all data included in SMART-OSI reports is owned by AFOSI.
Governance	Contractor maintains configurations control over Cognos. The data sources are pulled or have been pulled into the SMART-OSI data warehouse via the following interfaces:

SmartOSI	
Factor	**Data**
	• Web and Legacy I2MS • Learning Management System (LMS) • DSDS personnel files (UMD and Personnel data from Defense Civilian Personnel Data System and Military Personnel Data System) AFOSI maintains security/ IA control over SMART-OSI. A limited number of AFOSI leaders have access to certain standardized reports; however any report containing PII information must be requested through the SMART-OSI Program Manager.
Code and data complexity	Code and data complexity for SMART OSI is as follows: • Over 250 standardized reports • Approximately 1,048 other saved reports including user reports, developer reports and archived reports no longer in use • Approximately 6 Analysis Studio Cubes • Approximately 73 published data packages used in report building • Approximately 135 import layer tables used to create packages • Approximately 200 Oracle tables, containing more than 3,000 columns (production schema) • Approximately 122 Oracle tables, containing 2,025 columns (staging schema)
Stability	There are two situations when SMART-OSI has been/ will be down: 1. The two servers (database and application) require regular security patch installations/ updates. The servers have to be stopped and restarted. After the servers have been restarted, SMART-OSI automatically starts up. 2. Running updates from IBM; we anticipate a new install of the latest version of Cognos In the past year, SMART-OSI was down on several occasions when AFNET group policy was changed without notice and impacted users' ability to logon.

SmartOSI	
Factor	**Data**
Number of concurrent users	There are approximately 170 users per month utilizing reports within SMART-OSI. Many more customers request specific reports directly from the SMART-OSI team.
Application age	SMART-OSI has been in place since 2009. Prior to 2009, AFOSI had a similar capability using Cognos products dating back to the late 90's.
Inputs/ Outputs	Input: • SMART-OSI requests specific data from I2MS/DSDS/LMS based on the customer request. The information is pulled from I2MS and placed in the data warehouse for SMART-OSI access. Additionally, the SMART data warehouses contain information from sources reflected in the "governance" section. Output: • Products are created based on customer requests. Once created, the products are posted on the SMARTOSI portal for the customer to view or delivered via e-mail in a specified format.
Initial response time for customer product requests	After a request has been submitted to SMART-OSI Team (via email, in-person meeting, over the phone, etc.) the following general timeline is set as described in the priority listed below: • Product has been approved for creation and priority set (Status New) • Product is placed in development (Status changed to: In Development) • The report is completed, reviewed, and validated. PMO or peer review if necessary. • Product is returned to the customer; modifications completed if necessary (Status changed to: Customer Review) • Final product is disseminated to the customer and work order is closed (Status changed to: Development Complete) • PMO final review and approval (Status changed to: Closed) Requests for products are categorized as prioritized as follows: • Level 1 – Emergency (Same day but less than 24 hours) • Level 2 – Critical (48 hours or two business days) • Level 3 – High (5 business days) • Level 4 – Medium (12 business days) • Level 5 – Low (30 business days) *NOTE: SMART OSI receives complex reports that require in depth customer interaction. When the tickets are received, suspense's can and

SmartOSI	
Factor	**Data**
	will be adjusted accordingly so long as progress is being made on the requested product/report.
Life expectancy	The ATO for Cognos expires in 2019; in order to maintain the use of Cognos on AFOSI networks, a request must be completed.
Operating system	Current operating systems for Cognos is Microsoft Windows Server 2008 R2 Enterprise, version 6.1.7601 (Build 7601: Service Pack 1) COTS utilities - Development Tools for SMART-OSI: • IBM Cognos 10.2.1 Business Intelligence Data Manager, Version 10.2.1 • IBM Cognos 10.2.1 Business Intelligence Transformer, Version 10.2.1.13 • IBM Cognos 10.2.1 Business Intelligence Framework Manager, Version 10.2.1.13 • IBM Cognos 10.2.1 Business Intelligence Configuration, Version 10.2.1.13 However, Cognos 10.2.1 has reached its end of support, therefore an upgrade will occur to Cognos 11 in the near future. Version 10.2.1 is in a period of Continued Support if since OSI maintains an active service and support contract. 'Continued Support' offers support functions to help maintain the current Cognos install until the upgrade is completed.
Platform	Current platform utilized For the SMART-OSI process: Application server: hqcuismartapp • Windows Server 2008 R2 Standard • hqcuismartapp • Disk drives: VMware Virtual disk SCSI Disk Device • Disk (C): 61.4 GB free of 399 GB Database server: hqcuismartdb • Windows Server 2008 R2 Standard • hqcuismartdb • Disk drives: VMware Virtual disk SCSI Disk Device (2) • Disk (C): 191 GB free of 499 GB • Disk (E): 105 GB free of 309 GB
Programming Languages	The current programming language is COTS proprietary, Oracle 11G (PL/SQL).
Programs	Development Tools for SMART-OSI: (these are also listed in the Operating System block)

SmartOSI				
Factor	**Data**			
	• IBM Cognos 10.2.1 Business Intelligence Data Manager, Version 10.2.1 • IBM Cognos 10.2.1 Business Intelligence Transformer, Version 10.2.1.13 • IBM Cognos 10.2.1 Business Intelligence Framework Manager, Version 10.2.1.13 • IBM Cognos 10.2.1 Business Intelligence Configuration, Version 10.2.1.13			
Database	Three databases are currently in use and reside on the hqcuismartdb server: • Audit • SMARTCS • Xiiidwh2			
COTS	Cognos 10.2.1 has reached it's end of support, therefore an upgrade will occur to Cognos 11 in the near future. Version 10.2.1 is in a period of Continued Support if since OSI maintains an active service and support contract. 'Continued Support' offers support functions to help maintain the current Cognos install until the upgrade is completed.			
	Current licensing information:			
	IBM COGNOS BUSINESS INTELLIGENCE ADMINISTRATOR AUTHORIZED USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL	BI ADMINISTRATOR	AUTH USER ANNUAL SW S&S RENEWAL	3
	IBM COGNOS BUSINESS INTELLIGENCE ADVANCED BUSINESS AUTHOR AUTHORIZED USER LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	BI ADVANCED BUSINESS AUTHOR	AUTH USER LIC + 12 MOS S&S	3
	IBM COGNOS BUSINESS INTELLIGENCE ENHANCED CONSUMER AUTHORIZED USER LICENSE + SW SUBSCRIPTION &	BI ENHANCED CONSUMER	AUTH USER LIC + 12 MOS S&S	150

<table>
<tr><th colspan="5">SmartOSI</th></tr>
<tr><td>Factor</td><td colspan="4">Data</td></tr>
<tr><td></td><td>SUPPORT 12 MONTHS</td><td></td><td></td><td></td></tr>
<tr><td></td><td>IBM COGNOS DATA MANAGER DEVELOPER AUTHORIZED USER LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS</td><td>BI DATA MANAGER DEVELOPER</td><td>AUTH USER LIC + 12 MOS S&S</td><td>2</td></tr>
<tr><td>Average transactions per day</td><td colspan="4">According to the audit logs, SMART-OSI user ran an average of 212 reports per day during CY2017.

In addition, there are currently over 20 reports run on automated schedules (weekly, monthly or quarterly). These reports are run and saved, with links to the current version going out by email to over 50 recipients.

The following data refreshes are performed:
• Daily Case Updates (daily)
• LMS refresh (daily)
• Agent Applicant Weekly (daily)
• Monthly data refresh (completed by 8th day of each month - cube refreshes, etc., are valid to the last day of previous month)
• DSDS Personnel Data refresh (1st and 15th day of each month)

These reports and activities only include the already scheduled and tailored reports. Customer requested reports are built and ran on a requested basis.</td></tr>
<tr><td>Interfaces</td><td colspan="4">N/A</td></tr>
<tr><td>Upgrades</td><td colspan="4">Currently working on upgrade to Cognos 11.</td></tr>
<tr><td>Average help desk call volume</td><td colspan="4">Customer requests are entered into Remedy to track requests and urgency levels. The following levels apply:

• Level 1 – Emergency
• Level 2 – Critical
• Level 3 – High/Medium
• Level 4 – Medium
• Level 5 – Low

The following depicts the number of requests (230) submitted/completed and their respective levels assigned for the inclusive dates of 1 Jan 13 to 31 Dec 13:</td></tr>
</table>

SmartOSI	
Factor	**Data**
	• Level 1 – 17 • Level 2 – 70 • Level 3 – 53 • Level 4 – 53 • Level 5 – 36 • Training/briefing – 1 The above numbers do not account for customer requests that can be handled without opening a Remedy ticket (i.e. pointing the customer to the location of the standard reports for their utilization).
Requirement	Contractors are expected to maintain databases and conduct a data refresh on a monthly basis. Contractors shall create, provide and update report deliverables as requested by AFOSI users or external entities IAW the below metrics:
Metric: Response/Resolution time required for customer product requests:	After a product has been identified and a request has been submitted to the SMART-OSI team, the following general timeline shall apply: Requests for products are categorized as prioritized as follows: • Level 1 – Emergency (Same day but less than 24 hours) • Level 2 – Critical (48 hours or two business days) • Level 3 – High (5 business days) • Level 4 – Medium (12 business days) • Level 5 – Low (30 business days) *NOTE: SMART OSI receives complex reports that require in depth customer interaction. When the tickets are received, suspense's shall be adjusted accordingly so long as progress is being made on the requested product/report.
Metric – SMARTOSI data refresh requirement	The majority of the data is refreshed daily (WebI2MS and LMS). DSDS data is refreshed twice per month, and all investigative case data is refreshed monthly, by the 8th of every month.

Classified SmartOSI	
Factor	**Data**

Classified SmartOSI	
Factor	**Data**
Application Purpose and Background	CSMART provides important mission metrics to decision makers within the Command and outside of the Command. CSMART offers a combination of analysis functions, reporting capabilities (standardized and ad hoc) and metrics (performance management) applications.
Criticality of application	CSMART enhances the mission of AFOSI by providing a systematic process of delivering Air Force Counter Intelligence Data to customers at the highest levels of the Government. CSMART alleviates the requirement to manually count statistical information required for various purposes. CSMART's customer base often requests data with just a few hours suspense which makes delivery under the manual system within the requested timeframe impossible.
Network	SIPRnet
Security clearance requirement	A Secret clearance is required.
Ownership of system -	AFOSI owns the CSMART program however Cognos is a COTS sold by IBM; all data included in CSMART reports is owned by AFOSI.
Governance	Contractor maintains configurations control over Cognos. The data sources are pulled or have been pulled into the CSMART data warehouse via the following interfaces: • Web and Legacy CI2MS • ABRAXAS (ICON database) • DSS Referral Tracker (ICON database) • AFOSI Foreign Disclosure Management System (AFDMS) (ICON database) • Blue Line Production data Contractors do not directly distribute any reports from this system as this would require them to classify the data contained. Either the government PMO or the licensed users pull this data themselves.
Code and data complexity	Code and data complexity for SMART OSI is as follows: • Approximately 29 standardized reports • Approximately 18 published data packages used in report building • Approximately 38 import layer tables used to create packages • Approximately 45 Oracle tables (production schema) • Approximately 51 Oracle tables (staging schema) • Approximately 96 data extract builds (extract, transform

Classified SmartOSI	
Factor	**Data**
	and load processes)
Stability	There are two situations when CSMART has been/ will be down: 1. The two servers (database and application) require regular security patch installations/ updates. The servers have to be stopped and restarted. After the servers have been restarted, CSMART automatically starts up. 2. Running updates from IBM; we anticipate a new install of the latest version of Cognos. In the past year the system has been stable with no major issues or outages.
Number of concurrent users	There are 170 licensed users with access to reports within CSMART. Occasionally customers request specific reports directly from the CSMART team and delivered through the PMO.
Application age	CSMART has been in place since 2015. Prior to this implementation, AFOSI had a similar capability around 2005.
Inputs/ Outputs	Input: · CSMART requests specific data from legacy and WebCI2MS, and other ICON databases, based on the customer request. The information is pulled from these data sources and placed in the data warehouse for CSMART access. Output: • Products are created based on customer requests. Once created, the customer must logon to CSMART and pull the data themselves. Contractor staff cannot classify the data produced by these reports. If the user does not have a license, the CSMART government Project Manager will deliver the data.
Initial response time for customer product requests	After a product has been identified and a request has been submitted to the CSMART team, the following general timeline shall apply: • Product has been approved for creation and priority set (Status New) • Product is placed in development (Status changed to: In Development) • The report is completed, reviewed, and validated. PMO or peer review if necessary. • Product is returned to the customer; modifications completed if necessary (Status changed to: Customer Review) • Final product is disseminated to the customer and work

Classified SmartOSI	
Factor	**Data**
	order is closed (Status changed to: Development Complete) • PMO final review and approval (Status changed by PMO to: Closed) Requests for products are categorized as prioritized below and consist of each step and status from 'new' to 'development complete': • Level 1 – Emergency (Same day but less than 24 hours) • Level 2 – Critical (48 hours or two business days) • Level 3 – High (5 business days) • Level 4 – Medium (12 business days) • Level 5 – Low (30 business days) *NOTE: SMART OSI receives complex reports that require in depth customer interaction. When the tickets are received, suspense's can and will be adjusted accordingly so long as progress is being made on the requested product/report.
Life expectancy	The ATO for Cognos expires in 2019; in order to maintain the use of Cognos on AFOSI networks, a request must be completed.
Operating system	Current operating systems for Cognos is Microsoft Windows Server 2008 R2 Standard, version 6.1.7601 (Build 7601: Service Pack 1) COTS utilities - Development Tools for SMART-OSI: • IBM Cognos 8 Business Intelligence Data Manager, Version 10.2.1.13 • IBM Cognos 8 Business Intelligence Framework Manager, Version 10.2.1.13 • IBM Cognos 10.2.1 Business Intelligence Configuration, Version 10.2.1.13 However, Cognos 10.2.1 has reached its end of support, therefore an upgrade will occur to Cognos 11 in the near future. Version 10.2.1 is in a period of Continued Support if since OSI maintains an active service and support contract. 'Continued Support' offers support functions to help maintain the current Cognos install until the upgrade is completed.
Platform	Current platform utilized For the CSMART process:

<table>
<tr><th colspan="5">Classified SmartOSI</th></tr>
<tr><th>Factor</th><th colspan="4">Data</th></tr>
<tr><td></td><td colspan="4">Application server: hqsipsmartapp
• Windows Server 2016 Standard
• hqsipsmartapp
• Disk drives: VMware Virtual disk SCSI Disk Device
• Disk (C): 75.2 GB free of 249 GB

Database server: : hqsipsmartdb
• Windows Server 2016 Standard
• hqsipsmartdb
• Disk drives: VMware Virtual disk SCSI Disk Device (2)
• Disk (C): 191 GB free of 498 GB
</td></tr>
<tr><td>Programming Languages</td><td colspan="4">The current programming language is COTS proprietary, Oracle 11G (PL/SQL).</td></tr>
<tr><td>Programs</td><td colspan="4">Development Tools for CSMART: (these are also listed in the Operating System block)

• IBM Cognos 10.2.1 Business Intelligence Data Manager, Version 10.2.1
• IBM Cognos 10.2.1 Business Intelligence Framework Manager, Version 10.2.1.13
• IBM Cognos 10.2.1 Business Intelligence Configuration, Version 10.2.1.13</td></tr>
<tr><td>Database</td><td colspan="4">Three databases are currently in use and reside on the HQCUITABIS server:
• AUDIT
• SMARTCS
• XIIDWH2</td></tr>
<tr><td rowspan="3">COTS</td><td colspan="4">Cognos 10.2.1 has reached its end of support, therefore an upgrade will occur to Cognos 11 in the near future. Version 10.2.1 is in a period of Continued Support if since OSI maintains an active service and support contract. 'Continued Support' offers support functions to help maintain the current Cognos install until the upgrade is completed.</td></tr>
<tr><td colspan="4">Current licensing information:</td></tr>
<tr><td colspan="4"><table>
<tr><td>IBM COGNOS BUSINESS INTELLIGENCE ADMINISTRATOR</td><td>BI ADMINISTRATOR</td><td>AUTH USER ANNUAL SW S&S</td><td>3</td></tr>
</table></td></tr>
</table>

Classified SmartOSI				
Factor	**Data**			
	AUTHORIZED USER ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL		RENEWAL	
	IBM COGNOS BUSINESS INTELLIGENCE ADVANCED BUSINESS AUTHOR AUTHORIZED USER LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	BI ADVANCED BUSINESS AUTHOR	AUTH USER LIC + 12 MOS S&S	3
	IBM COGNOS BUSINESS INTELLIGENCE ENHANCED CONSUMER AUTHORIZED USER LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	BI ENHANCED CONSUMER	AUTH USER LIC + 12 MOS S&S	150
	IBM COGNOS DATA MANAGER DEVELOPER AUTHORIZED USER LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	BI DATA MANAGER DEVELOPER	AUTH USER LIC + 12 MOS S&S	2
Average transactions per day	According to the audit logs, CSMART users ran an average of between 9 and 15 reports per day during CY2017. Data Refreshes: • Daily Case Updates (WebCI2MS) • Daily ABRAXAS updates • Daily DSS Referral Tracker updates • Daily AFDMS updates • Daily Blue Line Production data			
Interfaces	N/A			
Upgrades	Planning upgrade to Cognos Analytics Version 11.			

Classified SmartOSI	
Factor	**Data**
Average help desk call volume	Customer requests are entered into Remedy to track requests and urgency levels. The following levels apply: • Level 1 – Emergency • Level 2 – Critical • Level 3 – High/Medium • Level 4 – Medium • Level 5 – Low The following depicts the number of requests (45) submitted/completed and their respective levels assigned for the inclusive dates of 1 Jan 17 to 31 Dec 17: • Level 1 – 7 • Level 2 – 3 • Level 3 – 13 • Level 4 – 5 • Level 5 – 17 The above numbers do not account for customer requests that can be handled without opening a Remedy ticket (i.e. pointing the customer to the location of the standard reports for their utilization).
Requirement	Contractors are expected to maintain databases and oversee daily data refreshes. Contractors shall create, provide and update report deliverables as requested by AFOSI users or external entities IAW the below metrics:
Metric: Response/Resolution time required for customer product requests:	After a product has been identified and a request has been submitted to the CSMART team, the following general timeline shall apply: • Product has been approved for creation and priority set (Status New) • Product is placed in development (Status changed to: In Development) • The report is completed, reviewed, and validated. PMO or peer review if necessary. • Product is returned to the customer; modifications completed if necessary (Status changed to: Customer Review) • Final product is disseminated to the customer and work order is closed (Status changed to: Development Complete) • PMO final review and approval (Status changed to: Closed)

Classified SmartOSI	
Factor	**Data**
	Requests for products are categorized as prioritized below and consist of each step and status from 'new' to 'development complete': • Level 1 – Emergency (Same day but less than 24 hours) • Level 2 – Critical (48 hours or two business days) • Level 3 – High (5 business days) • Level 4 – Medium (12 business days) • Level 5 – Low (30 business days) *NOTE: SMART OSI receives complex reports that require in depth customer interaction. When the tickets are received, suspense's shall be adjusted accordingly so long as progress is being made on the requested product/report.
Metric – SMARTOSI data refresh requirement	100% of table data is refreshed on a daily basis.

Appendix E – AFOSI Software/Equipment

AFOSI is currently utilizing the following (though this is not an all-inclusive list) in our environment. New or different software/equipment can be added at any time and shall also need to be supported by the contractor. The contractor shall provide expertise on common IT brands and equipment including those listed below:

- ActiveClient
- Adobe Captivate and Robohelp
- Adobe products to include Flash, CS suite, and Shockwave
- Analyst Notebook
- APC Power Distribution Units
- Barracuda Networks security appliances
- Brocade switches
- Cisco Multilayer network routers, switches, and security appliances such as ASA, ASR, and TACACS
- Cisco Telepresence (Video/Voice Communication) appliances and servers
- Codian switches
- Cognos (most current approved version)
- Dameware Mini Remote Control Tool
- Defense Enrollment Eligibility Reporting System (DEERS)
- Deliberate and Crisis Action Planning and Execution Segments (DCAPES)
- Dell rackmount servers
- eEye Retina
- eFOIA
- Eltek Valere voice devices
- Faces
- First Responder's Evidence Disk (FRED)
- GEM X Encryptor Manager
- GFI Events Manager
- Global Combat Support System (GCSS)
- Host Based System Security (HBSS)
- HP Blade servers/systems
- HP Insight
- HP rackmount servers
- HP Tape libraries
- IBM (was Qlabs) Qradar security appliances
- IBM 9131 Model 52A & IBM 8406 Model 70Y
- IBM rackmount and tower servers
- IBM server support for OpenFox (NCIC and NLETS)
- IBM Tape libraries
- Info Analyst
- InfoConnect
- IAFIS

- Investigative Information Management System (I2MS)
- Java
- Juniper security appliances
- KLAS satellite/security appliances
- Lantronix routers
- Lexmark Multi-Functional Devices (X792's deployed throughout command)
- Moodle
- McAfee Firewall Enterprise (Sidewinder Admin Console)
- McAfee Sidewinder security appliances
- Microsoft Desktop Optimization Pack
- Microsoft Exchange 2007/2010 or most current approved version
- Microsoft Forefront Identity Management (FIM)
- Microsoft ISA 2006 or currently approved version
- Microsoft Lync 2010 or currently approved version
- Microsoft Office Products
- Microsoft Operating Systems such as Windows 7 (32 and 64 bit), Windows Server 2003/2003 R2 (32 and 64 b and 64 bit)
- Microsoft SharePoint 2010 or currently approved version
- Microsoft SQL 2005/2008/2012
- Microsoft System Center Operations Manager (SCOM)
- Microsoft System Center Configuration Manager 2007 or current approved version (SCCM)
- Microsoft Windows Server Update Service (WSUS)
- Mozilla Firefox 26 or currently approved version
- NetApp Data ONTAP 7.X and newer
- NetApp Storage Area Network appliances
- NetQos security appliances
- OpenFox / NCIC / NLETS
- OpenText Livelink 9.7.x or currently approved version
- Oracle 11g or current certified version
- Oracle Sun servers
- Overland storage appliances
- PremiSys ID
- PWRR
- Promise storage appliances
- Quantum tape libraries
- Remedy 6/7 and ServiceNow ITSM Suites
- ScenePD Pro 5
- Server Technologies Inc. Power Distribution Units
- SIPRNET Tokens Trusted Agent (TA) and Local Registration Authority (LRA)
- SME-PED (Secure Mobile Environment - Portable Electronic Device)
- SnagIt 10 or currently approved version
- SnapManager (SQL and Exchange)
- SolarWinds
- SourceFire security appliances to include Defense Centers

- StarBoard
- Symantec Anti-virus client/server
- Symantec Back-up Exec 2010/2012
- Symantec BrightMail
- Task Management Tool (TMT)
- Titus Labs Classification tools
- Toad for Oracle
- Tumbleweed Desktop Validator
- Unisys Distributed Enterprise Print Controller (DEPCON)
- ViaSat security appliances
- Vmware ESXi 5.x or current approved version

Appendix F: Priority Response Matrix

Priority	Response/Ticket Opened	Resolution	Case Type Usage Examples (not all-inclusive)	Notification Timeline
1-Critical (Outage)	Immediately Upon Credible Report (I-UCR)	4 Hours	-More than 50 people lose access to a network, application or service -Mission critical – mission critical communications are not being received or sent and/or functional group experience mission degradation/loss -Issues can be designated as critical by the Field Support Squadron Commander, Chief of Network Operations or Chief Information Officer (CIO) as needed due to mission impact or management visibility	Initial notification IAW Notification Matrix (Appendix C) within 45 minutes. Affected users notified within 15 minutes of government direction. Provide updated status every 2 hours or as requested.
2-High (Outage)	I-UCR	8 Hours	-Business is interrupted –10-50 users cannot access services, systems or network -The user is an AFOSI Executive -The user supports a command-wide AFOSI functional area or service -Escalate high priority tickets to critical priority if unresolved after 2 duty days in high -Issues can be designated as high by the Field Support Squadron Commander, Chief of Network Operations or Chief Information Officer (CIO) as needed due to mission impact or management visibility	Initial notification IAW Notification Matrix (Appendix C) within 1 hour. Affected users notified within 15 minutes of government direction. Provide updated status every 4 hours or as requested.
3-Medium	30 Minutes	24 Hours	-Normal user requests due to issues causing business interruption affecting 6-10 people	Initial notification next business day, follow up within

Priority	Response/Ticket Opened	Resolution	Case Type Usage Examples (not all-inclusive)	Notification Timeline
			-Single detachment outage -Escalate medium ticket to high priority if unresolved after 5 duty days in medium	24 hours.
4-Low	60 Minutes	3 Duty Days	-Normal user requests that do not cause work stoppage -Complex issues that are not mission critical and that do not affect more than 5 users -Moderately complex issues -Escalate routine ticket to medium priority if unresolved after 7 duty days	N/A
5-Routine, quick	4 Hours	1 Duty Day	-Easy/quick resolutions, quick turnaround requests such as: -Account creation, password resets, profile updates, active directory updates, IT Configuration info, websites/moxies, answer customer questions, send guides, instructions and links	N/A

- The Government reserves the right to change Appendix F as necessary to reflect current or updated guidance from 24th AF, 624th OC, 690 NSS.
- Applies to all tickets.