

**PERFORMANCE-BASED STATEMENT OF WORK (PBSOW)
FOR DEVELOPMENT AND SUSTAINMENT OF
AIR FORCE DIRECTORY SERVICES (AFDS)**

01 APRIL 2005

1.0 INTRODUCTION. HQ OSSG has been directed by Air Staff to establish a Program Management Office to formally execute continued implementation of Air Force Directory Services. The AFDS program is designed to address enterprise IT challenges and to enhance AF mission performance through seamless integrated access to the right information, anywhere, anytime.

2.0 BACKGROUND. The AFDS consists of many commercial-off-the-shelf (COTS) products. When these products are configured to operate together, they provide a common set of resources consisting of application servers, web servers, security resources, and database facilities. AFDS is currently in three different life cycle phases; development, implementation and sustainment. In the development phase, the AFDS lab environment is operated on between 30 and 50 Intel based servers. Future capabilities include: technical analysis of alternatives, automated identity flow, automated account provisioning, user self service, access management, authorization service, and federated authentication service account provisioning. Implementation and operational services include: identity consolidation service, personal identity service, global address list distribution services on both the unclassified and classified network. The implementation environment is currently run on three different operating system platforms; Exchange 5.5, and MIIS. The operational network is run on approximately 13 Intel based servers. The COTS products and programming languages used to provide the services are Microsoft Identity Integration Server (MIIS), Netscape Directory Services, Visual Basic (VB.NET), C#, PERL, SQL, LDAP, Secure LDAP, Microsoft MIIS, MMS 2.2, Microsoft Exchange 5.5 and 2003, Active Directory, Networking, IPSEC, Z Script, C#. The Government team currently consists of a military program manager, deputy program manager, project lead, technical lead and operational lead.

3.0 APPLICABLE DOCUMENTS.

- a. HQ USAF/XI Memorandum AF Program Management Office for AF Directory Services dated 6 June 2003.
- b. Secretary of the Air Force Memorandum Air Force Information and Data Management Strategy Policy dated 3 March 2004.
- c. AFI 33-119
- d. AFI 33-201, 222, 225 and 229
- e. AFI 25-201
- f. Time Compliance Network orders
- g. DoD Directive 5000.1

4.0 OBJECTIVES.

4.1 Purpose. The purpose of this SOW is to describe systems engineering expertise needed for the HQ OSSG Air Force Directory Services Program support. The Contractor Team supporting this task is expected to compliment the Government team currently in place. The support these requirements in accordance with the taskings outlined in this SOW.

5.0 REQUIREMENTS/TASKS.

5.1 Task 1 – Enterprise Identity Data Management and Attribute Flow to Active Directory (AD). Provide common repository of role based identity data for war fighters that can be used by systems, applications, and devices with the capability to populate necessary attributes to support PK enablement of networks. This includes the population of Electronic Data Interchange/Personnel Identifier (EDI/PI) and Public Key Infrastructure (PKI) certificates in AD from Global Directory Services, Air Force Personnel Center, Defense Manpower Data System and other DoD directories. The Identity directory will hold authoritative AF identity data for exchange with varied data sources including the DoD GDS DMDS AFPC other various participating consumers and various applications. The identity directory will provide a flat namespace to support AF-wide applications to include the GCSS-AF integration framework/ AF Portal, AF Whitepages and eventually organizational “yellow pages. This capability will also provide data back to data sources for the process of creation of user certificates which will enable consistent match between data sources, enable single sign-on and provide email encryption certificates allowing individuals and systems access to authoritative data and updates non-authoritative systems with authoritative data.

- 5.1.1 Inputs: Data from authoritative sources such as DoD GDS, AFPC, DMDS, AF-GAL. Data request from an individual or system, existing program architecture diagrams and documents, COTs manuals, Memorandum of Agreement (MOA) for connection to AFDS Meta Directory database and Interface Requirement Agreement (IRA), AFI 25-201.
- 5.1.2 Outputs: Provide the war fighter and other DoD systems access to authoritative data stored AFDS Meta Directory database. Provide a stable, well managed, flat non-partitioned namespace for other directory enabled applications/directories. Provide the capability to distribute (push) updates to all non-authoritative data stores scheduled in FY06 (Contract Data Requirements List (CDRL) A001 Contractor’s Weekly Activity Report/Status), MOAs for connection to AFDS Meta Directory database (CDRL A002 – Memorandum of Agreements) and Interface Requirement Agreement IRAs, (CDRL A003 - Interface Requirement Agreements), Transition and Log Run files must be cleaned and archived weekly or on an as needed basis (CDRL A004 - Audit and tracking report) (CDRL A005 -Bandwidth Studies) Quarterly report addressing data quality within the system (CDRL A006 – Data Quality Report) and PIN Bi-Weekly Reports (CDRL A007 - PIN Bi-Weekly Report).
- 5.1.3 Skills/Experience Required (in order of importance): Microsoft MIIS, Active Directory, Netscape Directory Services , LDAP, Secure LDAP, Exchange 5.5 and 2003, Visual Basic (VB.NET), C#, PERL, SQL, Java Web services, Z Script, Networking, IPSEC,

- 5.1.4 Acceptance Criteria: Consistent data update to AD allowing AF to reconcile accounts with an increased match rate Air Force wide of 5 percentage points each contract year. A Meta-Directory database that is operational 99% of the time and provides a single source for accessing and distributing correlated identity information with current signed MOAs and IRAs that comply with AFI 25-201 for all AFDS connections.
- 5.2 **Task 2 – Virtual GAL.** Perform operational directory integration work, provide a Global Address List (GAL) that enables the war fighter to search and find contact information for AF and non-AF member (DoD/Federal members) on the classified and unclassified networks. User types in the name of the individual or organization for which they wish to find contact information. Provide this capability to search the AF GAL via LDAP and via web services. Provide a single standardized architecture throughout the AF enterprise network. Initial capability will only be accessible to AF-members full operational capability will provide referrals to non-AF DoD and government members that need access to AF Systems and applications. This capability will support NeCentric initiatives of the AF and DoD.
- 5.2.1 Inputs: MAJCOM NOSC servers, Global Directory Services, DMS-AF, and GCSS-AF, COTs software manuals, log files, help desk trouble tickets, TCNOs, current infrastructure documentation.
- 5.2.2 Outputs: With each key entered the Virtual GAL will close in on the desired name by moving to the first object in the store which matches all keystrokes entered so far until the user either selects the contact from the list or the criteria entered has no matches in the data store (CDRL A001 Contractor’s Weekly Activity Report/Status), transition and log runs archived and cleaned on a weekly or as needed basis (CDRL A004 - Audit and tracking report) Bandwidth studies (CDRL A005 – Bandwidth study, Test Reports for each new deployment (CDRL A008 – Test/Implementation Report) Trip reports for on-site support (CDRL A009– Trip Report), training manuals for any work that may be required by the base level Work Groups Mangers (WGMs) or System Administrators (SAs) (CDRL A010 – Training Manual).
- 5.2.3 Skills/Experience Required (in order of importance): Microsoft MIIS, , Exchange 5.5 and 2003, Active Directory, SQL, Networking, IPSEC, Visual Basic (VB.NET), Z Script, C#, java web services
- 5.2.4 Acceptance Criteria: Provide a single standardized documented architecture on the AF Enterprise network. Upgrade deployments will be based on the schedule stated in the current service level agreement. FY05 deployments include PACAF, AETC, and AFRC. AF-GAL will be available to the enterprise 99% of the time. Test Reports for each new deployment delivered 5 WD prior to implementation. Trip Reports due 8 working days upon return of contractor TDY. Program Manager approved training manuals delivered 30 work days prior to implementation of new technology or functionality.
- 5.3 **Task 3 – GAL Standardization.** Provide the AF a standard set of directives and instructions for the management of user accounts in the AF for the classified and unclassified networks. These directives and instructions will identify standard data elements. AFDS will provide the capability to identify inconsistencies in data, and develop/provide individual enhanced automated solution sets to pull MAJCOM GAL

authoritative attributes identity data (telephone number, office symbol, email address) into the AFDS master repository. The overall goal to create a single AF enterprise network identity for the war fighter and supporting applications.

- 5.3.1 Inputs: Current AF GAL contact information formats
 - 5.3.2 Outputs: Technical Guidance documentation concerning domain naming conventions (CDRL A011 – Active Directory Domain Naming Conventions Input) and recommendation updates to AFI 33-119 for standardization of AF GAL contact information (CDRL A012 – Technical recommendation for updates to AFI 33-119). Weekly reports generated for those accounts that are non-compliant with AF Standards one for NIPRNET and one for SIPRNET (CDRL A013 – NIPRNET Noncompliance Report and CDRL A014 SIPRNET – Noncompliance Report) delivery date and time are subject to change based upon requirements from Lead Command. Contractor will receive informal, via email, written notification of any change in schedule a minimum of 5 working days prior to change in delivery schedule.
 - 5.3.3 Skills/Experience Required (in order of importance): Microsoft MIIS, , Exchange 5.5 and 2003, Active Directory, SQL, Networking, IPSEC, Visual Basic (VB.NET), Z Script, C#, Java web services
 - 5.3.4 Acceptance Criteria: Non-compliance report delivered by COB the last working day of each week. Informal/formal written recommendations for changes in AFIs or guidance documentation on an as needed basis.
- 5.4 **Task 4 – GAL Synchronization.** Provide the AF a standard set of processes, tools and capabilities to synchronize the MAJCOM Active Directory and Exchange email systems on the classified and unclassified networks providing the war fighter a single address list. This capability will provide the AF the ability to more easily locate and communicate with war fighters. This capability will be maintained as AF networks are upgraded and modified to meet mission requirements.
- 5.4.1 Inputs: Data from the current sources of AF GAL information; AF-GAL, GDS, projected GAL information i.e.; DMS-AF, GCCS-AF, existing log files.
 - 5.4.2 Outputs: A single stable consolidated AF GAL directory that acts as the single source for contact information. (CDRL A001 - Contractor’s Weekly Activity Report/Status), NOTAMS for any scheduled/unscheduled work being performed which could impact the enterprise (CDRL A015 – Notice to Airmen (NOTAMs)).
 - 5.4.3 Skills/Experience Required (in order of importance): Microsoft MIIS, MMS 2.2, Exchange 5.5 and 2003, Active Directory, SQL, Networking, IPSEC, Visual Basic (VB.NET), Z Script, C#.
 - 5.4.4 Acceptance Criteria: A single AF enterprise network identity for the war fighter and supporting applications with less than 1% error rate and less than 1% interruption in services. Routine NOTAMs delivered to technical lead a minimum of 21 days prior to work being performed. Non routine NOTAMs delivered as directed by technical lead.
- 5.5 **Task 5 – Identity Data Consolidation.** Provide the capability for joining, synchronizing, and distributing authoritative data from authoritative sources. Data is currently pulled in from DoD GDS, DMDC, AF-GAL and AFPC. Other authoritative sources will be added in

the future to meet joint interoperability requirements i.e. Army, Navy, Coast Guard, DMS and NASA (projected FY07-FY12). Objective is to reduce errors in identity data by creating a single point of administration for multiple network identities. Automates process of identifying identity data origins and administrate processes to correct data. Provides foundation for provisioning services and automation of directory updates.

- 5.5.1 Inputs: Data from the authoritative data sources such as DoD GDS, AFPC, AF-GAL and DMDC.
- 5.5.2 Outputs: A single complete source for the network identity of individuals, (CDRL A001 - Contractor's Weekly Activity Report/status).
- 5.5.3 Skills/Experience required (in order of importance): Netscape Directory Services, Visual Basic (VB.NET), C#, PERL, SQL, LDAP, Secure LDAP, Microsoft MIIS.
- 5.5.4 Acceptance Criteria: Creation of a single AF Enterprise point of administration for network identities which possesses surge capability for additional sources of information.

5.6 **Task 6 – Automated Identity Data Attribute Flow.** New functionality currently projected during FY06-FY09. AFDS will explore and implement when directed, the means to update multiple directories and databases with authoritative data using dynamic and static business rules. Thus simplifying and automating the process of managing accounts across multiple systems in the AF.

- 5.6.1 Inputs: Data maintained within the AFDS meta-data directory, other authoritative data sources i.e. AFPC, DMDS and GDS.
- 5.6.2 Outputs: User accounts are created in appropriate systems. This will include modifications and deletions to data (CDRL A001 - Contractor's Weekly Activity Report/status), Technical Analysis of Alternatives (CDRL A016 – Technical Analysis of Alternatives).
- 5.6.3 Skills/Experience required (in order of importance): Netscape Directory Services, Visual Basic (VB.NET), C#, PERL, SQL, LDAP, Secure LDAP, Microsoft MIIS.
- 5.6.4 Acceptance Criteria: Provide a technical Analysis of Alternatives for automated Identity Data Attribute Flow; the capability to create, modify, and delete data based on personnel record changes, account information or requested processing based on current year SLA. Air Force enterprise implementation within 18 months of an Air Force accepted solution and tasking.

5.7 **Task 7 – Automated Workflow Provisioning.** This capability is currently projected to be implemented between FY06-FY09. Develop automated and semi-automated capability to change war fighter identity and access to enterprise data, devices and applications based on change in war fighter status, role, or attribute. Provide Audit and Tracking Reporting capability for the management of user accounts. Provide Delegated Administrator capabilities allowing dynamic management of accounts. Provide user self service capability to allow war fighters to update accounts. This capability will require development of training manuals providing clear guidance to network system administrators on how to manage accounts.

- 5.7.1 Inputs: Data maintained within the AFDS meta-directory.

- 5.7.2 Outputs: User access to a system change based on an update to data maintained in the meta-directory, MOAs for connection to AFDS Meta Directory database (CDRL A002 – Memorandum of Agreements) Interface Requirement Agreement (CDRL A003 - Interface Requirement Agreement), User Account Audit and Tracking Report (CDRL A004 – Audit and Tracking Report), and Analysis of Alternatives documentation. (CDRL A016 - Technical Analysis of Alternatives), Account Management training manuals for system administrators (CDRL A010 – Training Manual), Training plan – (CDRL A017 - Training Plan).
- 5.7.3 Skills/Experience required (in order of importance): Netscape Directory Services, Visual Basic (VB.NET), C#, PERL, SQL, LDAP, Secure LDAP, Microsoft MIIS.
- 5.7.4 Acceptance Criteria: The development and Air Force wide implementation of a tool that allows account updates to be accomplished automatically in systems based on changes to the user’s identity information. Appointed program manager approval of training plan/manual a minimum of thirty days prior to implementation of capability. Audit report reflecting less than 1% error rate delivered COB every Thursday.

- 5.8 **Task 8 – Role-Based Access Profile Distribution.** New functionality currently projected for implementation FY07 – FY11. This capability will provide data to systems based on roles with the enterprise. This capability will provide an automated authorization service to control access between USAF and DoD Systems. This will increase security, providing auditing capabilities, interoperability between systems and reducing administrative workload of attribute-based authorization. System Administrator training manuals/plans will need to be developed providing clear guidance to the SA on how to manage their mappings.
 - 5.8.1 Inputs: Data maintained within the AFDS meta-directory database. Account approval process and documentation.
 - 5.8.2 Outputs: User account profile used to manage enterprise access, Process documentation for procedures for creation of account profiles (CDRL A018 - Account Profile Creation Process Document, CDRL A019 - Account Profile Approval Forms), Audit and Tracking reports (CDRL A004 - Audit and Tracking Report), Training plans/manuals (CDRL A016 – Training plan) (CDRL A010 – Training manual).
 - 5.8.3 Skills/Experience required (in order of importance): Netscape Directory Services, Visual Basic (VB.NET), C#, PERL, SQL, LDAP, Secure LDAP, Microsoft MIIS.
 - 5.8.4 Acceptance Criteria: Documented process for creation of account profiles, Creation of account profiles within 5 working days from contractor receipt of all government approved documentation. Provide a capability to distribute verifiable/vettable/integrity profiles for users to the enterprise and provide a single point to manage access to enterprise data.

- 5.9 **Task 9 – Capability Review and Enhancement.** Periodically review what capabilities AFDS is providing and determine if an enhanced solution is viable based on the current technology.
 - 5.9.1 Inputs: Capabilities being provided by AFDS.

- 5.9.2 Outputs: Recommended enhancements to current architecture or service, (CDRL A020 - Architectural Design Documentation and Diagrams, CDRL A016 - Technical Analysis of Alternatives, CDRL A008 – Test/Implementation Report) Technology Refresh White Paper (CDRL A021 - Technology Refresh Plan).
 - 5.9.3 Skills/Experience Required (in order of importance): Netscape Directory Services , Microsoft MIIS , MMS 2.0, Exchange 5.5 and 2003, Visual Basic (VB.NET), SQL, LDAP, Secure LDAP, C#, Z Script.
 - 5.9.4 Acceptance Criteria: Documentation providing recommendations that will increase the level of support to the war fighter and ease the burden of management for the AFDS architecture and services on an as needed basis.
- 5.10 **Task 10 – Properly patched and upgraded framework.** Apply patches and functional component upgrades identified by configuration management (CM) to the AFDS Framework.
- 5.10.1 Inputs: An existing framework, patch/upgrade notice for the framework from CM, software patches from applicable application sources, COTS manuals and hardware installation guides.
 - 5.10.2 Outputs: Test Evaluation Master Plan (CDRL A022 – Test Evaluation Master Plan), Tested TCNO instructions (CDRL A008 – Test/Implementation Report), a correctly patched/upgraded framework and patch test report providing government personnel clear guidance on how the patch was applied to the laboratory framework and how to apply the patch to the operation field; to include any problems resulting from the patch. Updated architecture documentation (CDRL A020 - Architectural Design Documentation and Diagrams).
 - 5.10.3 Skills/Experience Required (in order of importance): Netscape Directory Services , Microsoft MIIS , MMS 2.2, Exchange 5.5 and 2003, Visual Basic (VB.NET), SQL, LDAP, Secure LDAP, C#, PERL, Z Script.
 - 5.10.4 Acceptance Criteria: Test Evaluation Master Plan updates delivered on the anniversary date of the existing approved document, Mandatory Software Patches properly applied to the framework one working day prior to the mandated install date specified on the TCNO. Optional software patches/upgrades applied to the framework within 10 working days of contractor tasking and receipt of patch from appointed government technical or operational lead. Updated Architecture documentation within 5 work days from date that the patch has been applied.
- 5.11 **Task 11 – Manage Meta-Directory Database.** Add, update, and manage users, groups, and roles following documented procedures.
- 5.11.1 Inputs: Existing database, documented procedures, request forms.
 - 5.11.2 Outputs: Users, groups, and roles correctly added to the framework (CDRL A001- Weekly Activity Report).
 - 5.11.3 Skills/Experience required (in order of importance): Netscape Directory Services, Visual Basic (VB.NET), C#, PERL, SQL, LDAP, Secure LDAP, Microsoft MIIS.
 - 5.11.4 Acceptance Criteria: A functioning AFDS framework with procedures to manage users, groups, and roles.

- 5.12 **Task 12 – Program Management Support.** The contractor shall provide program management support to efficiently execute taskings and report status of work performed under this task. This support will include coordination efforts in the development and implementation of AFDS architecture and services. Provide maintenance support for the AFDS website and Microsoft Sharepoint library. Assist with providing contractor peer review of contractor documentation. Provide assistance with planning, preparation, and conducting of AFDS meetings, conferences, and working group or technical meetings. Assist with development of project timeline and work break down structure. The contractor shall deliver a final work order status that chronologically summarizes work performed throughout the task period along with a final accounting of all delivered products.
- 5.12.1 Inputs: Existing program documentation, Requirements and regulations pertaining to the system in question, previously written AFDS documentation, COTS manuals, AFDS working group meetings, and technical interchange meetings. Existing website, change requests from Government lead, OSSG Templates.
- 5.12.2 Outputs: Technical inputs for the Capital Investment Report – (CDRL A023 – Technical inputs to Capital Investment Reports) Technical updates to the Capabilities Design Document (CDRL A024 - Updates to the Capability Development Document) Updates to the Privacy Impact Assessment and Federal System Notification (CDRL A025 – Privacy Impact Assessment, CDRL A026 – Federal System Notification) Memorandums of Agreement for AFDS connections (CDRL A002 – MOAs), Project Timeline/Work Breakdown Structure (CDRL A027 - Project timeline/WBS), consolidated contractor monthly status report (CDRL A028 – Monthly Status Report) and other program management related documentation on an as needed basis.
- 5.12.3 Skills/Experience required (in order of importance): Project control, Formal writing, Technical writing, MS Project, MS office Suite.
- 5.12.4 Acceptance Criteria: Completed documentation delivered in accordance with contractor taskings, Work Breakdown Structure completed in September for work to be performed in the next fiscal year, 90% of all contractor taskings completed and delivered on time.
- 5.13 **Task 13 – Trouble Ticket Resolution Management.** Troubleshoot and coordinate updates for Tier I and II help desk trouble tickets for AFDS. Analysis of submitted trouble tickets identifying any trends.
- 5.13.1 Inputs: Help Desk Trouble Tickets, COTS manuals, software patches, TCNOs.
- 5.13.2 Outputs: Remedy resolution input with recommendation on status, Trouble Ticket Report and trend analysis (CDRL A029 – Trouble ticket metrics/status/mgmt report, CDRL A030 - Trouble Ticket Trend Analysis Report).
- 5.13.3 Skills/Experience Required (in order of importance): Netscape Directory Services , Microsoft MIIS , MMS 2.0, Exchange 5.5 and 2003, Visual Studio (VB.NET), SQL, LDAP, Secure LDAP, C#, Z Script, Remedy, Technical writing.
- 5.13.4 Acceptance Criteria: AFDS PM appointed government lead acceptance of recommended solution provided within 72 working hours (3 work days) of tasking by help desk (ticket passed by help desk), Trouble ticket metrics/status/mgmt report delivered COB every

Tuesday, Trend analysis/metrics reports generated and forwarded to the program manager on the last work day of each month, trouble tickets updated every 72 hours until the Trouble Ticket is closed.

5.14 **Task 14 – Configuration Management of AFDS Framework.** Provide overall configuration Management support in the development and implementation of AFDS architecture and services.

5.14.1 Inputs: Existing program documentation, architecture documentation, TCNOs, software patches, and written government requests, SEP documentation, COTS software.

5.14.2 Outputs: Configuration Management Plan (CDRL A031 – Configuration Management Plan), properly archived program coding, (CDRL A001 Weekly Activity/Status Report), informal; written authorization to load all software patches, upgrades and TCNOs (CDRL A032 – Software Upgrade/TCNO authorization to load).

5.14.3 Skills/Experience required (in order of importance): Configuration Management, Formal writing, Technical writing, PVCS.

5.14.4 Acceptance Criteria: Compliance with HQ OSSG SEP standards for configuration control of program coding. Initial Configuration Management Plan delivered to government by 8 July 2005 annual review and updates to the existing plan delivered by COB on the anniversary date of initial plan. Minimum SEP audit rating of yellow with marked improvements for each consecutive audit.

5.15 **Task 15 – Security Management of AFDS Framework.** Provide overall security management support in the development and implementation of AFDS architecture and services. Complete all requirements to properly certify and accredit the system.

5.15.1 Inputs: Existing SSAA, NetRA, CON, IATO, applicable AFIs and SEP documentation.

5.15.2 Outputs: Completed approved Command, Control, Communications, Computer and Intelligence Support Plan (C4ISP) for AFDS (CDRL A033 – C4ISP), System Security Accreditation Agreement (CDRL A034 – System Security Accreditation Agreement), Interim Authority to Operate (IATO) and/or Authority to Operate (ATO) (CDRL A035- Interim Authority to Operate and/or Authority to Operate), Certificate of Networthiness (CDRL A036 - Certificate of Networthiness) and the Network Risk Assessment (CDRL A037 - Forms for Network Risk Assessment).

5.15.3 Skills/Experience required (in order of importance): Knowledge concerning current Security AFIs, Formal writing, Technical writing.

5.15.4 Acceptance Criteria: Compliance with all security regulations. Approved CON, IATO and/or ATO delivered no later than the expiration date of the existing documentation. SSAA and C4ISP delivered based upon ENQ's recommended schedule.

6.0 DELIVERABLES.

In addition to the deliverables required for each task, a monthly Contractor Progress Status and Management Report (CDRL A001) shall include all activities completed during each month to include appropriate cost reporting.

| SOW Par. Task # | Deliverable | CDRL # | Delivery Schedule |
|---|--|---------------|---|
| 5.1.2, 5.2.2, 5.4.2, 5.6.2, 5.11.2, 5.14.2 | Weekly Activity Report | CDRL A001 | Due COB every Thursday |
| 5.1.2, 5.7.2, 5.12.2 | Memorandum of Agreement (MOA) for connection to AFDS Meta Directory database | CDRL A002 | New MOAs for connection to AFDS Meta Directory database on an as needed basis. Existing MOAs for connection to AFDS Meta Directory database annual within one month prior to the anniversary date for accuracy and updates |
| 5.1.2, 5.7.2, 5.12.2 | Interface requirement agreement (IRA) | CDRL A003 | New MOAs for connection to AFDS Meta Directory database on an as needed basis. Existing MOAs for connection to AFDS Meta Directory database annual within one month prior to the anniversary date |
| 5.1.2, 5.2.2, 5.7.2, 5.8.2 | Audit and Tracking Report | CDRL A004 | Due COB every Thursday |
| 5.1.2 | Bandwidth studies | CDRL A005 | Upon request by Government Quality Assurance Personnel (QAP) |
| 5.1.2 | Data Quality Report | CDRL A006 | 08 July 05, 07 Oct 05, 07 Jan 06, 08 Apr 06, 06 Jul 06, 06 Oct 06, 05 Jan 07, 06 Apr 07, 06 Jul 07, 05 Oct 07, 04 Jan 08, 04 Apr 08, 11 Jul 08, 10 Oct 08, 09 Jan 09, 10 Apr 09, 10 Jul 09, and 09 Oct 09 |
| 5.1.2 | PIN Bi-Weekly Report | CDRL A007 | 03:00PM CST – every other Thursday |
| 5.12.2 | Test/Implementation Report | CDRL A008 | Mandatory Time Compliance Network Order (TCNO) - COB of date mandated date noted on the TCNO, Optional Patches and upgrades COB 10 Working days from receipt of patch from government appointed technical or operational lead and contractor tasking from appointed government QAP. |
| 5.2.2 | Trip Reports for all travel performed by the contractor | CDRL A009 | Within 8 WD from completion of travel |

| | | | |
|---------------------------|---|--------------|---|
| 5.2.2 | Training Manual | CDRL A010 | Delivered 30 work days prior to implementation of new technology or functionality |
| 5.3.2 | Active Directory Domain Naming Conventions Input | CDRL A011 | On an as needed basis |
| 5.3.2 | Technical recommendations for updates to AFI-33-119 | CDRL A012 | On an as needed basis |
| 5.3.2 | NIPRNET Noncompliance Report | CDRL A013 | Non-compliance report delivered by COB the last working day of each week |
| 5.3.2 | SIPRNET Noncompliance Report | CDRL A014 | Non-compliance report delivered by COB the last working day of each week |
| 5.4.2 | Draft NOTAMs | CDRL A015 | Routine draft NOTAMs 21 days prior to programmed implementation, maintenance of upgrade. Non-routine NOTAMs as directed by appointed Government Technical lead |
| 5.6.2, 5.7.2, 5.9.2 | Technical Analysis of Alternatives | CDRL A016 | As noted in current year Program Execution Addendum of Service Level Agreement provided to the contractor, currently projected for FY06, FY07. |
| 5.7.2 | Training Plan | CDRL A017 | 30 days prior to implementation of capability. |
| 5.8.2 | Account Profile Approval Document | CDRL A018 | Currently projected 31 October 07 any change in schedule will be communicated through the QAP. |
| 5.8.2 | Account Profile Approval Forms | CDRL A019 | Currently projected 31 October 07 any change in schedule will be communicated through the QAP. |
| 5.9.2, 5.10.2 | Architectural Design Documentation and Diagrams | CDRL A020 | Initial documentation delivered within 90 days of the contract year. Updates to existing documentation will be provided the last working day of Mar, Jun, Sep, and Dec. |
| 5.9.2 | Technology Refresh Plan | CDRL A021 | Currently projected 30 Nov 06 any change in schedule will be communicated through the QAP. |
| 5.10.2 | Test Evaluation Master Plan | CDRL A022 | Updates delivered on the anniversary date of the existing approved document |
| 5.16.2 | Documented inputs to the Capital Investment Report | CDRL A023 | 03 Jun 05, 01 Dec 05, 02 Jun 06, 01 Dec 06, 01 Jun 07, 07 Dec 07, 06 Jun 08, 05 Dec 08, 05 Jun 09, 04 Dec 09. |
| 5.12.2 | Technical inputs to the Capabilities Development | CDRL A024 | Updates to existing documentation on an as needed basis. |

| | | | |
|---------|---|-----------|--|
| | Document | | |
| 5.12.2 | Updates to PIA | CDRL A025 | Projected requirement with Provisioning upgrade in FY06 Update required 30 days from the date of contractor tasking |
| 5.12.2 | Federal System Notification | CDRL A026 | Projected requirement with Provisioning upgrade in FY06 Update required 30 days from the date of contractor tasking |
| 5.12.2 | Project timeline/WBS | CDRL A027 | Work Breakdown Structure completed in September for work to be performed in the next fiscal year and on an as needed basis |
| 5.12.2. | Monthly Status Reports | CDRL A028 | COB 2 nd Monday of the month following the reporting month |
| 5.13.2 | Trouble ticket metrics/status/mgmt report | CDRL A029 | COB Tuesday every week |
| 5.13.2 | Trouble Ticket Trend Analysis | CDRL A030 | COB Last working day of each month |
| 5.14.2 | Configuration Management Plan | CDRL A031 | 29 Jul 05 with updates on an as needed basis. |
| 5.14.2 | Software Upgrade/TCNO authorization to load | CDRL A032 | On an as needed basis |
| 5.15.2 | Command, Control, Communication, Computer and Intelligence Support Plan (C4ISP) | CDRL A033 | Completed and approved two months prior to expiration of each existing document |
| 5.15.2 | System Security Accreditation Agreement | CDRL A034 | Annual Review with signed updated documentation delivered on the expiration date of the previous version. |
| 5.15.2 | Interim Authority to Operate and/or Authority to Operate | CDRL A035 | Annual Review with signed updated documentation delivered on the expiration date of the previous version |
| 5.15.2 | Certificate of Networthiness | CDRL A036 | Annual Review with signed updated documentation delivered on the expiration date of the previous version |
| 5.15.2 | Network Risk Assessment | CDRL A037 | Annual Review with signed updated documentation delivered on the expiration date of the previous version |

7.0 TECHNICAL MEETINGS

7.1 Post Award. The contractor shall meet with Government representatives within 10 workdays after the contract award to reach a common understanding of task order requirements, deliverables, and Government expectations.

7.2 Technical Interchange Meetings. The Contractor shall provide technical expertise for all technical reviews and meetings.

8.0 SERVICE DELIVERY SUMMARY.

8.1 Performance Based Support: The HQ OSSG/DONE AFDS Objectives and Performance Thresholds are reflected in the table below. In support of this Performance-Based Task, the Contractor shall be responsible for achieving the established thresholds for each objective. The AFDS Quality Assurance Personnel (QAP) will be responsible for ensuring HQ OSSG/DONE furnish the Contractor all necessary documents, access, and support needed for timely performance-based activity.

| SOW Par. | Performance Objectives | Performance Threshold | Disincentive for Failure to meet standards | Method of Surveillance |
|-----------------|---|--|---|---|
| 5.1 | Develop and maintain identity data Meta Directory which provides a single source for accessing and distributing correlated identity information | Increased EDI-PI match rate Air Force wide of 5 percentage points each contract year. Meta-Directory Database that is accessible and operational 99% of the time | .5% reduction in annual billing for periods of non compliance | Validated via contractor provided reports and periodic government surveillance |
| 5.2 | Provide a fully synchronized AF GAL to the enterprise | System is synchronized and operational 99% of the time | 1% reduction in monthly billing for periods of non-compliance | Validated via periodic government surveillance |
| 5.6 | Provide for automated Identity Data Attribute Flow capability | Enterprise implementation 18 months from implementation tasking. | 1% reduction in monthly billing each month after the period of non Compliance carried through until task is completed | Validation of implementation via contractor provided reports and periodic government surveillance |
| 5.8 | Provide a documented capability to distribute verifiable/vettable/integrity profiles for users to the enterprise and provide a single point to manage access to enterprise data | Enterprise implementation 18 months from implementation tasking. 92% of all account profiles created 5 WD from contractor receipt of | 1% reduction in monthly billing each month after the period of non Compliance carried through until task is | Validation of implementation via contractor provided reports and periodic government surveillance. Account profiles validated through |

| | | | | |
|------|---|--|--|--|
| | | all government approved documentation | completed | random sampling and customer complaints |
| 5.10 | Properly patched and upgraded framework. | Contractor apply 100% of mandatory TCNOs to the system NLT the stated TCNO suspense date. Optional Patches and upgrades applied within 10 WD of contractor tasking 92% of the time | .5% reduction in monthly billing for periods of non-compliance | Validation of TCNO compliance through random sampling by Information Assurance Office. Optional Patches through Periodic Surveillance by PMO |
| 5.15 | Compliance with all security regulations. Approved CON, IATO and/or ATO, SSAA and C4ISP | 95% on time delivery of all security documentation. 100% compliance of security regulations | .5% reduction in monthly billing for periods of non-compliance | Validation of compliance by third party assessments (HQ OSSG/EN and AFCA) |
| 9.8 | Surge Capability. Provide surge support for unanticipated requirements as identified by the Government. Contractor shall identify qualified personnel within 10 WD or less to meet the requirement. | Contractor able to support surge request with qualified personnel within 10 WD window 92% of the time. | .5% reduction in monthly billing for periods of non-compliance | Validation of additional support and adequacy by the contracting office and program office |

9.0 ADDITIONAL/SPECIAL REQUIREMENTS:

9.1 Hours of Work. The Contractor shall be allowed access to Government facilities during normal business hours 07:00AM-05:00PM CST, Monday through Friday, excluding Federal Government holidays. For new implementations, and upgrades to the unclassified system work will be performed during non-peak traffic hours and can be performed from a remote location other than Maxwell AFB – Gunter Annex via virtual private network. All upgrades and new implementations to the classified network will be performed during non-peak duty hours and within the confines of a government controlled classified area in accordance with DoD Directive 5000.1. The Contractor shall coordinate any work hours outside of this period with the Government QAP before work is scheduled. Contractor shall provide one person to be on-call 24 hours a day, 7 days a week, 365 days a year, including holidays, to respond to issues pertinent to the operational network. On call work for the unclassified network being performed outside of normal business hours may be

performed from a remote location other than Maxwell AFB – Gunter Annex via virtual private network with the approval of the appointed program manager and quality assurance personnel. Contractors shall be given at least 48 hours notice if a schedule change is necessary.

9.2 Travel. Travel anticipated in support of new implementations, operational issues and to participate in Active Directory Working Group, and Technical Interchange Meetings. Travel for this effort, shall be in accordance with Government Joint Travel Regulation (JTR). No profit or fee shall be added. Quality Assurance Personnel (QAP) will be responsible for obtaining the Contracting Officer’s written approval for travel prior to contractor traveling. Reimbursement will include full travel costs, per diem reimbursement consistent with the Joint/ Federal Travel Regulation (JFTR), and reimbursement of general and administration expenses, as appropriate. Estimated travel locations and frequencies are listed in the following table. These travel estimates are subject to change based on Government requirements. Estimated travel is as follows:

| Origins | Destination | # of Trips | # of Days | # of Travelers |
|----------------|---|-------------------|------------------|-----------------------|
| Montgomery AL | Technical Interchange Meeting – Washington D.C. | 4 | 5 each | 2 each |
| Montgomery AL | Identity Mgmt Working Group | 4 | 3 each | 1 each |
| Montgomery AL | Software/Hardware Deployments Various MAJCOMs | 3 | 5 each | 2 each |
| Montgomery AL | PKI Conf | 1 | 3 each | 1 each |
| Montgomery AL | GCSS-AF Conf | 1 | 2 each | 1 each |
| Montgomery AL | Identity Mgmt Conference | 2 | 1 each | 1 each |

9.3 Location. The contractor shall be co-located in Government furnished facilities located at MAFB-Gunter Annex, AL. Space and computer equipment shall be provided for Contractor personnel on Maxwell AFB, Gunter Annex. The Government shall furnish all typical office equipment to support this requirement. This equipment shall include a PC, desk, chair, phone, and access to copiers and the Internet. If contractor is required to perform work off site via VPN, contractor will provide any equipment required to support this endeavor. All work performed on the SIPRNET will be completed within the confines of an area which has been approved for classified processing at Maxwell AFB-Gunter Annex.

9.4 Documentation. The Government shall provide the Contractor access to all required documents, specifications, and other applicable data within ten working days of the start of this task.

9.5 Timekeeping. The Contractor may be required to enter their hours of work into the Earned Value Management Tracking System. The data will solely be utilized for tracking internal earned value project information.

10. PERIOD OF PERFORMANCE.

10.1 Period of Performance. The initial period of performance for this effort shall be for seven months. Four twelve-month option periods shall also be priced and included in the task order.

| | | |
|--------------------|-----------------------|-----------|
| Base Year: | 01 Apr 05 – 31 Oct 05 | 7 Months |
| Option Year One: | 01 Nov 05 – 31 Oct 06 | 12 Months |
| Option Year Two: | 01 Nov 06 – 31 Oct 07 | 12 Months |
| Option Year Three: | 01 Nov 07 – 31 Oct 08 | 12 Months |
| Option Year Four: | 01 Nov 08 – 31 Oct 09 | 12 Months |

10.2 Skill Requirements. The contractor will assign sufficient resources and technically qualified, well trained contractor personnel to accomplish the tasks outlined in the SOW. The contractor shall assign qualified contractor personnel to accomplish these tasks while operating in an effective, efficient and timely manner.

11.0 SECURITY REQUIREMENTS.

During the performance of these taskings, contractor personnel may be required to use or come in contact with proprietary government information. The contractor shall not use such information for any purpose other than the performance of the work required in this SOW, in accordance with AFMC FAR 5352.209-9002 – ORGANIZATIONAL CONFLICT OF INTEREST (JULY 1997). In accordance with AFMC FAR 5352.209-9002 – ORGANIZATIONAL CONFLICT OF INTEREST (JULY 1997), Alternate III, the contractor agrees to enter into company-to company agreements to (1) protect another company’s information from unauthorized use or disclosure for as long as it is considered proprietary by the other company and (2) to refrain from using this information for any purpose other than that for which it was furnished. For information purposes, the contractor shall furnish copies of these agreements to the Contracting Officer. These agreements are not intended to protect information, which is available to the Government or to the contractor from other sources and furnished voluntarily without restriction. Non-disclosure agreements shall be accomplished and provided to the Contracting Officer prior to any access to competitive-sensitive or proprietary data, information or documents. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. If either the Government or the contractor discovers new or unanticipated threats or hazards, or if existing safeguards

have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

12.0 SECURITY REQUIREMENTS FOR UNCLASSIFIED SERVICES

12.1 Contractor Notification Responsibilities. The contractor shall notify the 42 SFS/ SFAI within 30 days before on-base performance of the service. The notification shall include:

- a. Name, address, and telephone number of contractor representatives.
- b. The contract number and contracting agency.
- c. The reason for the service (i.e., work to be performed).
- d. The location(s) of service performance and future performance, if known.
- e. The date service performance begins.
- f. Any change to information previously provided under this paragraph.

12.2 Security Manager Appointment. The contractor shall appoint a security manager for on-base service performance. The security manager may be a full-time position or an additional duty position. The security manager shall provide employees with training required by DoD 5200.1-R, *Information Security Program Regulation*, and AFI 31-401, *Information Security Program Management*. The contractor will provide 42 SFS/SFAI with name and telephone number of the security manager.

12.3 Visit Authorization Letters. The contractor will provide to the program manager, 42 SFS/SFAI, and HQ OSSG/DPS a Visit Authorization Letter identifying all employees performing the contract and required access to Maxwell AFB/Gunter Annex. The Visit Authorization Letter shall be validated and signed by the company Facility Security Officer (FSO) or company owner or president and provided to the program manager, 42 SFS/SFAI, and HQ OSSG/DPS prior the contract start date. A new VAL shall be provided when an employee's status or information changes. The Visit Authorization Letter will include following information:

- a. Contractor's company name, address, and telephone number.
- b. Name, date and place of birth, and citizenship of the employee(s).
- c. Certification of the employees' personnel security clearance and any special access authorizations required for the visit.
- d. Name of person(s), telephone, and unit identification to be visited

e. Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit.

f. Date or period during which the VAL is to be valid. **(Can be up to 12 months)**

12.4 Suitability Investigations. Contractor personnel shall successfully complete, as a minimum, a *National Agency Check (NAC)*, before operating **government furnished** workstations that have access to **Air Force** e-mail systems. These investigations shall be submitted by the government at no additional cost to the contractor. The contractor shall comply with the DoD 5200.2-R, *Personnel Security Program*, and AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, requirements.

12.5 Obtaining and Retrieving Identification Media. As prescribed by the AFFAR 5352.242-9000, *Contractor access to Air Force installations*, the contractor shall comply with the following requirements:

- a. The contractor shall obtain base identification and vehicle passes for all contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished identification badges while visiting or performing work on the installation.
- b. The contractor shall submit a written request on company letterhead to the contracting officer listing the following: contract number, location of work site, start and stop dates, and names of contractor employees needing access to the base. The letter will also specify the contractor individual(s) authorized to sign requests for base identification credentials or vehicle passes. The contracting officer will endorse the request and forward it to the issuing base pass and registration office or security forces for processing. When reporting to the pass and registration office for issue of a vehicle pass, contractor individual(s) shall provide a valid driver's license, current vehicle registration, and valid vehicle insurance certificate. When reporting to the pass and registration office for issue of military issue identification credentials for access to the installation, contractor individual(s) will need a valid state or federal issued picture identification.
- c. During performance of the service, the contractor shall be responsible for obtaining required identification for newly assigned personnel and for prompt return of credentials and vehicle passes for any employee who no longer requires access to the work site.
- d. Upon completion or termination of the service or expiration of the identification passes, the contractor shall ensure that all base identification passes issued to contractor employees are returned to the issuing office. The issuing office will verify all base identification passes have been returned and/or accounted for. The issuing office will forward a memorandum to the contractor individual authorized to sign request for base identification credentials indicating the badges and vehicle passes have been turned in. The DD Form 577 (signature card) for the contractor authorized requestor will be

destroyed and the individual will not long be authorized to sign DD Form 1172 (Application for Uniform Services Identification Cards).

e. Failure to comply with these requirements may result in withholding of final payment.

12.6 Pass and Identification Items. The service shall ensure the following pass and identification items required for service performance are obtained for employees and non-government owned vehicles:

a. DD Form 1172, *Application for Uniformed Services Identification Card* (AFI 36-3026, *Identification Cards For Members of The Uniformed Services, Their Family Members, and Other Eligible Personnel*, and AETC Instruction 36-3001, *Issue and Control of AETC Civilian Identification (ID) Cards*).

b. AETC Form 58, *Civilian Identification Card* (AETCI 36-3001).

c. AF Form 2219 (series), *Registered Vehicle Expiration Tab* (AFI 31-204, *Air Force Motor Vehicle Traffic Supervision*).

d. DD Form 2220, *DoD Registered Vehicle and Installation Tab* (AFI 31-204).

e. AF Form 1199, *USAF Restricted Area Badge*, or locally developed badge.

f. AF Form 75, *Visitor/Vehicle Pass* (AFI 31-204).

g. DoD Common Access Card (CAC), (AFI 36-3026).

12.7 Entry Procedures For HQ OSSG Facilities. Contractor employees required a HQ OSSG Contractor Access badge for unescorted entry into HQ OSSG facilities. To obtain a HQ OSSG Contractor Access badge the contractor's Facility Security Officer must send a Visit Authorization Letter (VAL) to HQ OSSG/DPS Security Office. The HQ OSSG/DPS Security Office must have a VAL on file prior to issuance of an HQ OSSG Contractor Access badge. Contractor personnel must bring a completed AF Form 2586, *Unescorted Entry Authorization Certificate*, and a letter signed by the HQ OSSG Staff Director's office (IL, SW, DI, etc.) to the HQ OSSG/DPS Security Office. The AF Form 2583, *Request for Personnel Security Action*, must include in Section III the task order number, period of performance, facility number and be signed by the Quality Assurance Personnel (QAP) associated with the assigned contract. Contractor personnel are required to wear their company's identification badge and HQ OSSG Contractor Access badge while in HQ OSSG facilities.

12.8 Unescorted Entry to Restricted Areas. When work under this contract requires unescorted entry to controlled or restricted areas, the contractor shall comply with AFI 31-101, Volume 1, *The Air Force Installation Security Program*, DoD 5200.2-R, and AFI 31-501, *Personnel Security Program Management*, as applicable. Contractor personnel shall be the subject of a favorably completed NAC investigation to qualify for unescorted entry

to a restricted area. In addition, the Air Force shall submit NAC investigations for contractor employees at no additional cost to the contractor. The contractor shall provide initial and follow-on training to contractor personnel who work in Air Force controlled/restricted areas. Air Force restricted and controlled areas are explained in AFI 31-101.

12.9 Entry Procedures to Controlled/Restricted Areas. The contractor shall comply and implement local base procedures for entry to Air Force controlled and restricted areas.

12.10 Freedom Of Information Act Program (FOIA). The contractor shall comply with DoD Regulation 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program*, requirements. The regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding *For Official Use Only (FOUO)* material. The contractor shall comply with AFI 33-332, *Air Force Privacy Act Program*, when collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. The contractor shall remove or destroy official records only in accordance with AFMAN 37-139, *Disposition of Records—Standards*, or other directives authorized in AFI 37-138, *Records Disposition—Procedures and Responsibilities*.

12.11 Reporting Requirements. The contractor shall comply with AFI 71-101, Volume- 1, *Criminal Investigations*, and Volume-2, *Protective Service Matters*, requirements. Contractor personnel shall report to 42 SFS, any information or circumstances of which they are aware may pose a threat to the security of DoD personnel, contractor personnel, resources, and classified or unclassified defense information. Contractor employees shall be briefed by their immediate supervisor upon initial on-base assignment and as required thereafter.

12.12 Additional Security Requirements. In accordance with DoD 5200.1-R and AFI 31-401, the contractor shall comply with AFI 33-202, *Computer Security*; AFI 33-203, *Emission Security (EMSEC) Program*; AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*; applicable AFKAGs, AFIs, and AFSSIs for Communication Security (COMSEC); and AFI 10-1101, *Operations Security (OPSEC) Instructions*.

12.13 Physical Security. Areas controlled by contractor employees shall comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) and local search/identification requirements. The contractor shall safeguard all government property, including controlled forms, provided for contractor use. At the close of each work period, government training equipment, ground aerospace vehicles, facilities, support equipment, and other valuable materials shall be secured.

12.14 Internal Operating Instructions. The contractor shall develop an Operating Instruction (OI) for internal circulation control, protection of resources, and to regulate entry into Air Force controlled areas during normal, simulated, and actual emergency operations. The OI shall be written in accordance with AFI 31-101, the local base Operations Plan usually

referred to as an OPLAN, and AFI 10-245, *Air Force Antiterrorism (AT) Standards*, and coordinated through the 42 SFS/SFAI.

12.15 Key Control. The contractor shall establish and implement key control procedures in the Quality Control Plan to ensure keys issued to the contractor by the government are properly safeguarded and not used by unauthorized personnel. The contractor shall not duplicate keys issued by the government.

12.16 Lost Keys. Lost keys shall be reported immediately to the contracting officer. The government replaces lost keys or performs re-keying. The total cost of lost keys, re-keying or lock replacement shall be deducted from the monthly payment due the contractor.

12.17 Access Lock Combinations. Access lock combinations are “For Official Use Only” and will be protected from unauthorized personnel. The contractor shall establish procedures in local OIs ensuring lock combinations are not revealed to unauthorized persons and ensure the procedures are implemented. The contractor is not authorized to record lock combinations without written approval by the government functional director.

12.18 Security Alarm Access Codes. Security alarm access codes are “For Official Use Only” and will be protected from unauthorized personnel. Security alarm access codes will be given contractors employees who required entry into areas with security alarms. Contractor employees will properly safeguard alarm access codes to prevent unauthorized disclosure. Contractor will not record alarm access codes without written approval by the government functional director.

12.19 Government Authorization. The contractor shall ensure its employees do not allow government issued keys to be used by personnel other than current authorized contractor employees. Contractor employees shall not use keys to open work areas for personnel other than contractor employees engaged in performance of their duties, unless authorized by the government functional area chief.

12.20 Lock Combinations. The contractor shall establish procedures in local OIs ensuring lock combinations are not revealed to unauthorized persons and ensure the procedures are implemented.

12.21 Traffic Laws. The contractor and their employees shall comply with base traffic regulations.

12.22 Healthcare. Healthcare provided at the local military treatment facility on an emergency reimbursable basis only.

13.0 EVALUATION CRITERIA.

The “Best Value” evaluation criteria identified below will be used to evaluate each offeror’s proposal. These criteria are listed in the order of importance determined to provide the “Best Value” to the Government.

13.1 Technical Expertise: The contractor will be evaluated on their demonstrated knowledge and capability to utilize Active Directory, Microsoft MIIS, Netscape Directory Services, LDAP, Secure LDAP, Exchange 5.5 and 2003, Visual Basic (VB.NET), C#, PERL, SQL, Java Web Services, Z Script, Networking, IPSEC and MMS 2.2, AFDS framework development requirements. The contractor will also be evaluated on their understanding of industry standard Information Technology best practices as it pertains to these software tools.

13.2 Past Performance: Contractor will be evaluated on past performance records from at least two projects of similar technical requirements at the Air Force enterprise level as those outlined in this SOW. Offerors should provide the contract numbers, description of the work and how it directly relates to the tasks identified in Section 5, and Government POCs (references) with current e-mail addresses and phone numbers.

13.3 Management Approach: Contractor will be evaluated on the understanding of the task, ability to bring the appropriate expertise/experience to the tasks when required, their management approach providing stability of workforce; maintaining those skills and key personnel for the life of the project. The requirements of this SOW and the resulting task order may change.

13.4 Surge Capability: Contractors should describe their company’s ability to bring additional skills to bear on unforeseen problems such as level of effort changes, security, and architecture and surge functionalities. Contractor should provide written plans for how they would address the requirement to increase their labor force/labor hours to match potential increases in the scope of the program as required by AFCA. Plan needs to include technical expertise, location of work force and estimated time frames required to meet the increased needs.

13.5 Cost: Contractor will be evaluated on overall cost and appropriate labor categories proposed for the management and technical approach/strategy. The cost/price areas will be evaluated based upon the total proposed prices and the degree of which the contractor’s proposed costs/prices indicate a clear understanding of a sound approach to meeting the requirements of the SOW and any discounts available off the published rates.