NETCENTS-2 SOLUTIONS

Application Services Full and Open

Performance Work Statement (PWS)

29 Apr 2010

1. NETCENTS-2 INTRODUCTION

1.1 Organization

AFLCMC/HICI – Enterprise Services Directorate

1.1.1 Identification

AFLCMC/HICK ATTN: Linda R. Lowmiller, NETCENTS-2 Application Services PCO
501 East Moore Drive, Bldg 884, Room 1400
MAFB-Gunter Annex, AL 36114

1.2 NETCENTS-2 Goal

The goal of the overall NETCENTS-2 program is to support missions that require voice, data, and video communications, information services, solutions, and products to deliver the right information, in the right format, to the right place, at the right time – efficient in peace, effective in war, and ensuring success across the spectrum of operations. NETCENTS-2 supports the IT lifecycle to include legacy operational and sustainment activities, re-engineering of legacy capabilities into target architectures and environments, and future service-oriented capabilities. NETCENTS-2 is an enabler to meet Air Force IT transformation goals to allow for innovation with the ability to more rapidly provision and field capabilities. NETCENTS-2 enables the ability to segregate aspects of full system lifecycles into more granular components that can be composed into integrated capabilities for the warfighter. Furthermore, NETCENTS-2 enables different solution providers to participate over the course of the program lifecycle. For example, the solution providers for development may be different from those that accomplish deployment, operation, and support.

1.3 NETCENTS-2 Scope

The NETCENTS-2 ID/IQ contracts will provide a wide range of IT Network-centric and Telephony products, services and solutions covering the full spectrum of netcentric operations and missions, including existing legacy infrastructure, networks, systems and operations, as well as emerging requirements based on the AF Chief Information Officer's (CIO's) SOA construct. These contracts will provide Network-Centric Information Technology, Networking, and Security, Voice, Video and Data Communications, system solutions and services to satisfy the Combat Support (CS), Command and Control (C2), and Intelligence Reconnaissance and Surveillance (ISR) Air Force and Department of Defense (DoD) requirements worldwide. These contracts will provide users the capabilities to find, access, collaborate, fuse, display, manage, and store information on the Department of Defense (DoD) Global Information Grid (GIG). AF sites may include commercial-off-the-shelf (COTS) National Security Systems (NSS), intelligence data handling equipment, C2 equipment, Local Area Networks (LAN), Wide Area Networks (WAN), secure and non-secure video, voice and data systems, and/or mission equipment. The equipment processes information of varying security classifications and may include sites that are Sensitive Compartmented Information Facilities (SCIFs).

All efforts supported under this contract shall be provided in accordance with Department of Defense, United States Air Force, or DoD Intelligence Information Systems (DoDIIS), and National Security Agency standards as applicable to the task order. Efforts under this contract will support industry best practices when not proscribed by aforementioned standards.

1.4 NETCENTS-2 Acquisition Strategy

NETCENTS-2 consists of various related IDIQ contracts in an effort to meet the above-stated goals. There are functions where performance on one task order may limit, because of dependencies or type of activity (e.g., support to the Government), work on other task orders. Total solutions will potentially be composed of combinations of subsets of the contract. NETCENTS-2 comprises the following suite of contracts:

1. Netcentric Products - COTS products to support the network

2. NetOps and Infrastructure Solutions - Solutions to support network operations, core enterprise services, and infrastructure development and operations

3. Application Services - Services to sustain, migrate, integrate, re-engineer, and expose Mission Applications for secure access by authorized users, by establishing web and netcentric services, to include help desk, testing and operational support, in legacy and netcentric enterprise environments

4. Enterprise Integration and Service Management (A&AS) - Enterprise level integration/portfolio management activities

5. IT Professional Support and Engineering Services Advisory and Assistance Services (A&AS)

The NETCENTS-2 contracts enable the delivery of products, services and solutions that adhere to the AF Enterprise Architecture (AF EA) and complement each other as depicted in Figure 1.

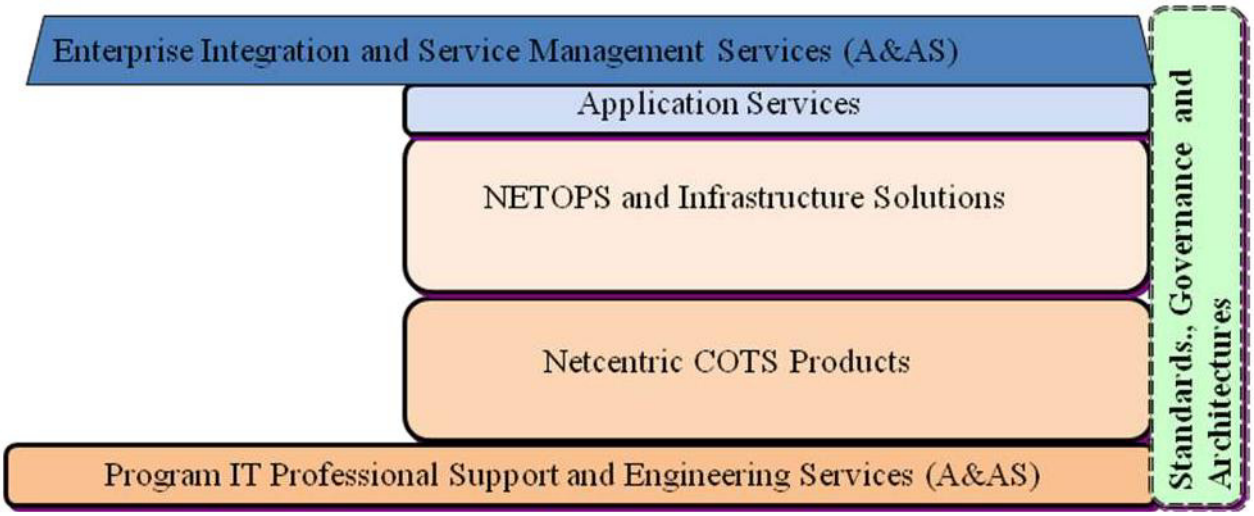

Figure 1. Relationship of Contract Areas

1.5 Air Force IT Challenge

Currently, the Air Force has multiple, disparate and sub-optimized collections of computing and communications resources. Each set of resources is managed independently, resulting in costly and inefficient redundancy. Different networks, multiple computing centers, and stove-pipe systems all make it difficult for end users to access consistent and relevant information in a timely manner, allocate resources to respond to demand, and consequently make timely and informed decisions.

1.6 NETCENTS-2 Solution

NETCENTS-2 is a vehicle enabling the IT lifecycle to include legacy operational and sustainment activities, migration of legacy systems, and future service-oriented capabilities. NETCENTS-2 provides a streamlined, enterprise-supported contract vehicle that enables the consolidation of many existing base-level contracts for Operations and Maintenance (O&M) activities. In addition, NETCENTS-2 supports the re-engineering and modernization of legacy systems through the rapid, incremental delivery of solutions, enabling improved day-to-day operations and warfighting mission execution. NETCENTS-2 provides a contract vehicle for the acquisition of the components, such as infrastructure, services, resources and activities, required to implement service-oriented capabilities.

To support the re-engineering of legacy systems and future service-oriented capabilities, the AF has created a set of information sharing business rules called the Singularly-Managed Infrastructure (SMI) and Enterprise Level Security (ELS) (SMI-ELS). SMI-ELS is not a technical solution or specific product, instead it guides a business model informed by governance and architecture that affects all aspects of a Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) solution for the effective implementation of a secure Net-Centric Data Strategy (NCDS). SMI-ELS gives form to processes such as architecture and acquisition; technical solutions such as networks, vocabulary-based web services, applications, data repositories, and computing infrastructures; and force transformation, to drive Air Force systems and users into higher degrees of information and knowledge-based operations.

The NETCENTS-2 scope of work directly supports SMI-ELS objectives, as follows:

1. SMI: The Singularly Managed Infrastructure will place AF core service computing and communications resources under a single enterprise-wide management construct. This does not mean consolidating resources into a single physical location for management purposes. Many high-end computing platforms, like those used to run simulations, may have internal management constructs as their resources are not shared across the enterprise. However, any interaction between these localized collections and any other computing resources will fall under the SMI construct. Likewise, not all communications (i.e., Military Strategic Tactical Relay (MILSTAR) satellites) may be individually managed under the SMI concept, but the overall capability delivered by these resources will adhere to SMI concepts. The SMI will operate over existing physical locations, with some adaptation of those physical locations based on business case analyses, to manage all computing resources from the enterprise perspective. Existing data centers, such as the MAJCOM Computing Centers, will be integrated into the SMI and the management of the resources within those Centers will be subject to the SMI processes and procedures.

2. ELS: The Enterprise Level Security will enable authorized users to locate, access, and utilize information from authoritative sources regardless of the location of the data as long as information security guidelines stipulated are met.

NETCENTS-2 also provides the contract vehicle to support the development of vocabulary-based web services, content delivery and presentation services, and new mission applications that operate in netcentric enterprise environments and exploit SOA infrastructures.

This contract provides the services management support required by SMI-ELS. Service Management (SM) ensures that: (1) agreed upon services are delivered when and where they are supposed to be delivered and (2) services operate as agreed upon. Using NETCENTS-2 contract vehicles, portfolio managers implement SM with a focus on risk mitigation and policies that require built-in closed-loop governance mechanisms.

1.7 Governance

The services and solutions delivered under NETCENTS-2 in support of Air Force operations will be subject to the oversight of an Air Force enterprise level governance structure and set of processes. The governance processes will employ systems engineering fundamentals, ensure adherence to the Air Force Enterprise Architecture, and be implemented along with the normal reviews in the acquisition process. The governance structure has three tiers, strategic, operational, and tactical, where policy will be set at the strategic level, reviews for compliance and technical rigor will be done at the operational level, and contract mechanics will be handled at the tactical level. Further explanation of the governance structure is explained in the User's Guide.

2. APPLICATION SERVICES SCOPE

The NETCENTS-2 Application Services acquisition provides a vehicle for customers to access a wide range of services such as sustainment, migration, integration, training, help desk support, testing and operational support. Other services include, but are not limited to, exposing data from Authoritative Data Sources (ADS) to support web-services or Service Oriented Architecture (SOA) constructs in AF enterprise environments. Through this vehicle, the contractor shall develop content delivery and presentation services and new mission applications that operate in netcentric enterprise environments that exploit SOA infrastructures. This contract shall support legacy system sustainment, migration and the development of new mission capabilities and applications. The focus of this contract is to provide application services support to mission areas, as overseen by portfolio managers, Communities of Interest (COIs), project offices, and program offices.

2.1 Application Services Relationship to Other NETCENTS-2 Contracts

The implementation and operation of SMI-ELS will be provided through the NETCENTS-2 Air Force Network Operations (NetOps)/Infrastructure Services and Solutions contract.

2.2 Netcentric Strategies, Standards, and the Use of This Contract by Other Agencies and Departments

Specific standards, guidance, and applicable documents within this contract are written with the intent of accomplishing Air Force and IC netcentric strategies. These strategies will evolve over time and, when appropriate, the AF will revise and replace standards accordingly. The contractor shall conform to Air Force strategies and visions and adhere to associated standards. If used by other agencies and departments for the same purpose, they may specify and substitute other standards, guidance, and applicable documents within their task orders that are appropriate to provide solutions tailored to meet their netcentric strategies.
Use of the Application Services contract may be available to DoD and Other Federal Agencies when any of the following criteria exists:

- is related to requirements for interoperability with Air Force capabilities;
- supports Air Force IT infrastructure, applications, or operations;
- supports host-tenant arrangements involving Air Force units; or
- supports joint operations or solutions.

The Air Force reserves the right to restrict use of this contract and to disallow DoD and other Federal Agencies from using this contract.

3. TECHNICAL REQUIREMENTS

The contractor shall provide application services that support sustainment, development, migration and integration, as well as web services and netcentric data services for legacy systems, content delivery and presentation services, and new mission applications that operate in netcentric enterprise environments and exploit AF infrastructures.

3.1 Systems Sustainment

The contractor shall support system sustainment activities to include maintaining existing legacy systems and environments IAW disciplined engineering practices and to sustain applications, databases, and interfaces. The contractor shall provide application services to support, maintain, and operate systems or services which are compliant with the DoD Information Assurance Certification and Accreditation Process (DIACAP) and DoDI 8500.2, Information Assurance Implementation or Intelligence Community Directive (ICD) 503 as applicable in the task order.

3.2 Systems Development, Migration, and Integration

The contractor shall provide services including, but not limited to, software development, software security, web services development, web services testing, smart phone or other IT devices applications and testing, security layer integration, database clean-up, data wrapping, and data conversion. The contractor shall provide system performance tuning, system re-hosting, and integration services. The contractor shall provide systems migration and integration support services to migrate legacy systems to an Enterprise Resource Planning System (ERP) or an existing standard infrastructure such as the Global Combat Support System (GCSS) or DoD Enterprise Computing Center (DECC). The contractor shall use only Government-Off-The-Shelf (GOTS) tools or approved Commercial-Off-The-Shelf (COTS) tools for systems design and development, or incorporation in system solutions, in accordance with AF Instruction 33-114, Software Management, and AF Policy Directive 33-2, Information Assurance (IA) Program, and the Air Force 33-200 series publications. Task orders for classified and mission-system networks will follow guidance and standards as identified in the task order.

3.3 Information Services

Task orders for classified and mission-system networks will follow guidance and standards as identified in the task order. The contractor shall provide application and content presentation services that identify and exploit existing services, create new SOA applications and data services, create presentation services, define, align and register vocabularies, expose the information assets for discovery in the Metadata Environment (MDE) for Communities of Interest (COIs), provide wrapping services, and provide data layer connectivity as described in the paragraphs that follow.

3.3.1 Development of New SOA Applications and Data Services

The contractor shall develop new information capabilities, as defined by a COI or other applicable Government organization. The contractor shall expose authoritative data as defined by the re-engineering of a business process, identifying the sources for the authoritative data, and establishing user roles and permissions for the information access as directed by Communities of Interest. The contractor shall support lifecycle management of new SOA-based applications that encapsulate business logic to provide new functional/ operational mission capabilities.

3.3.2 Create Aggregation Services

The contractor shall create aggregation services that deliver capabilities by coupling multiple core data services with business processes or sets of business rules to construct new information assets, utilizing enterprise services delivered through the NETOPS PWS in accordance with the enterprise architecture. The contractor shall make every effort to avoid duplication of data which is available from another authoritative source in the enterprise unless performance issues dictate a local cache or copy of the data. The contractor shall invoke appropriate enclave security services to address security issues that arise from the aggregation of information taken from multiple ADSs. The contractor shall create aggregation service specifications for review and approval. The contractor shall implement and deploy aggregation services.

The contractor shall provide aggregation services that apply business rules, as specified by applicable Government organizations, or through Enterprise Architecture analysis of business process models, to transform authoritative data into new information assets. The contractor shall create repositories for new authoritative data which are generated by aggregation services.

The contractor shall provide services through which content can be creatively combined, searched, and/or correlated in mashups web applications that combine data from more than one source into a single integrated tool for presentation to meet user requirements, such as dashboards.

3.3.3 Create Presentation Services

The contractor shall create presentation services, not already provided as enterprise services and available for reuse, that are required to display information unique to a specific set of users and to deliver specific mission capabilities. The contractor shall develop user presentation services, including, but not limited to, mashups, lightweight composite content, dashboards, portals, portlets, Rich Internet Applications (RIA), transformation and enrichment layers, and functionality source content to meet specific mission capability requirements. The contractor shall develop these presentation services to be available from the SOA infrastructure to provide content on-demand to meet specific mission capability requirements.

3.3.4 Specify Information Assets for Exposure

The contractor shall generate specification for exposing authoritative data as information asset payloads according to schemas or other guidance provided by the responsible Government organization, utilizing enterprise services delivered through the NETOPS PWS in accordance with the enterprise architecture The contractor shall provide semi-automated services that enable the specification of information asset by editing, sorting, filtering, and translating. The contractor shall utilize the data definitions and standards (vocabularies, ontologies, access rules, etc.) in specifying the information asset that will be exposed by the ADS owner. The contractor shall create schemas, documentation, or other supporting designs, for the ADS owners, COI or other Government organizations, to register for use throughout the DoD enterprise. The contractor shall establish access rules consistent with DoD Directive 8320.2 Net Centric Data Sharing and its implementation guide and/or Intelligence Community Information Sharing Steering Committee guidance.

3.3.5 Registering Services

The contractor shall support the registration of ADS exposure services, aggregation services, and presentation services in the MDE Service Registry, along with schemas for discovery purposes. The contractor shall support the registration of ADS exposure services for Top Secret and Intelligence, Surveillance, and Reconnaissance (ISR) mission systems per task order specifications.

3.3.6 Web Services

The contractor shall create and maintain web services using standards as defined within the Enterprise Architecture to include but not be limited to, Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and Universal Description, Discovery and Integration (UDDI) to enable sharing of data across different applications in an enterprise. These interfaces shall enable sharing of business logic, data and processes across a network, to specific functionality end-users.

3.3.7 Service Lifecycle Management

The contractor shall generate necessary design and implementation artifacts that will support lifecycle management of each service developed, defined as service development, testing, certification, registration, sustainment, and evolution aligned with defined requirements. These artifacts will include the metadata needed for service lifecycle management IAW the current version of the DoD Discovery Metadata Specification (DDMS). The design and implementation artifacts for Top Secret network systems and applications, as well as ISR mission systems, are owned by the Government and provided to the Government representative prior to the end of the task order at no additional cost to the Government unless otherwise stated in the task order.

3.3.8 Vocabulary Management

The contractor shall support the development of vocabularies to include developing schemas (e.g., use of Universal Core), semantic models, logical data models from structured repositories, and vocabularies that describe content in unstructured or semi-structured information assets. The contractor shall create and maintain Web Ontology Language (OWL) vocabularies and schemas to represent metadata that will enable service and data discovery using semantic web technologies. The contractor shall verify that vocabularies do not overlap or contradict other ADS vocabularies and resolve any discrepancies and eliminate redundancies before the vocabularies are registered.

Tasks may include the administration of COI-defined or other applicable Government organization vocabularies, in accordance with approved templates. The contractor shall create indexes that will be used to discover information in the vocabularies for mission assurance. The contractor shall translate information from one context to another, from a logistics perspective to a mission planning and execution perspective.

3.3.9 Register Vocabularies

The contractor shall support alignment, articulation and registration of vocabulary artifacts in the MDE for use during discovery and information access across the DoD and Air Force registries Model in accordance with NetOps infrastructure layer processes or Intelligence Community (IC) processes.

3.3.10 Data Stores

The contractor shall create or maintain data stores when a requirement for a new authoritative source of information is determined by the COI. The contractor shall make every effort to avoid duplication of data which is available from another authoritative source in the enterprise. The contractor shall provide services such as data cleansing, redundancy resolution, and business rule validation for those data stores. These data stores shall provide standard functionality and Continuity of Operations (COOP), and shall not degrade user operations, nor introduce critical points of failure. The contractor shall monitor and maintain these data stores to ensure data availability, accuracy, precision, and responsiveness.

3.3.11 Information Exposure Services

The contractor shall provide application services to expose specified information. The contractor shall prepare data to be retrieved by manipulating legacy information sources to be compatible with defined standards. Any modifications to the existing legacy system shall not have any adverse effects on the functioning of the legacy application. The contractor shall modify the information source, its interface, its data, and/or its behavior so that it is accessible using standards in accordance with the enterprise architecture. The contractor shall transform communication interfaces, data structures and program semantic alignment to allow exposure. At the direction of the Government, the contractor shall be responsible for configuration management of existing legacy baseline code and data exposure code.

3.3.11.1 Communication Wrappers

The contractor shall provide communication wrapping services by transforming the calling interface between two or more programs, managing event traffic between the information source and other services, and transforming method and function calls between the information source and other services. Any modifications to the existing legacy system shall not have any adverse effects on the functioning of the legacy application.

3.3.11.2 Program Wrapping

The contractor shall provide application program modifications, which may involve wrapping internal modules within an application for exposure in a SOA environment.

3.3.11.3 Data Language Translation

The contractor shall provide data language transformation by translating between different data manipulation languages, such as incompatible Structured Query Languages (SQL's). Transformations must not have any adverse effects on the functioning of the data retrieval or the legacy application.

3.3.11.4 Wrapping Standardization Processes

The contractor shall employ enterprise-wide processes for wrapping the information to be provided in accordance with the enterprise architecture, to eliminate redundant efforts and develop reusable libraries of information sources.

3.3.11.5 Reuse

The contractor shall make the wrapped data re-usable, providing common interfaces to information sources that follow widely accepted standards, allowing wrapped sources to be accessible to a wide class of coordination and mediation services.

3.4 Systems Operations

The contractor shall provide operational support services including, but not limited to, database administration, systems administration, to include system performance monitoring and tuning, customer training, and help desk support in support of legacy applications and systems or in support of new systems that are developed in compliance with the target enterprise architecture.

3.4.1 Database Administration

The contractor shall provide database administration support for logical and physical database designs. The contractor shall create and test backups of data, provide data cleansing services, verify data integrity, implement access controls to the data, ensuring maximum availability and performance. The contractor shall assist developers of data exposure services to efficiently and effectively use the database.

3.4.2 Systems Administration

The contractor shall provide a wide range of system administration services which may include, but not be limited to, installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems. The contractor shall quickly and correctly diagnose software and hardware failures to resolution. The contractor shall assist in the prevention of computer hacking and other security problems by implementing preventive measures in compliance with AF or IC enterprise architecture. The contractor shall ensure all firewalls and intrusion detection or other information assurance systems are fully functioning as intended and are kept current. The contractor shall monitor the performance of the system and resolve any issues related to the efficient and effective use of the system in general.

3.4.3 Customer Training

The contractor shall provide on-site training at Government and contractor locations, tailored to the specific requirement. The contractor shall allow the Government to videotape on-site training so the Government can use the tapes to conduct follow-on training of newly assigned personnel at that site. For training that is developed by the contractor at the contractor's expense, videotaping and reproduction by the Government will not be permitted unless terms/conditions/costs are incorporated in the task order. Training may be classified as initial or recurring. When a task order stipulates a requirement for training, the contractor shall submit, for Government approval, a training plan and lesson plan. The Government will specify the scheduling and location of the training course(s). Under certain conditions, prototype lab site configurations shall be setup at the contractor's facility and used not only for verification and validation but also as a training site for selected users. The contractor shall develop, maintain and/or update student and instructor training materials. This may include computer-based training (CBT), lesson plans and handouts, manuals, train-the-trainer material, textbooks, workbooks, manuals, evaluation forms and other documentation. This may include delivering copies of these materials to the extent specified in the task order. For training development that is provided under a task order, the contractor shall allow the Government to reproduce and distribute contractor customized training materials, at no additional cost to the Government. The contractor shall allow that follow-on training for newly assigned Government personnel may be conducted by Government trainers. The Government owns all rights to the current and future training materials developed by the contractor at Government expense. Examples of training requirements may include a combination of CBTs, classroom lecture, demonstration, hands-on experience, and manual/documentation familiarization for each student. The contractor shall ensure training stays current with the services offered throughout the life of the contract. The training shall not contain proprietary information and may be augmented/altered by the Government after delivery.

3.4.4 Help Desk Support

The contractor shall provide Help Desk Tier 1, Tier 2, and Tier 3 support for technical assistance, order processing, support of multiple software versions, training, warranty, and maintenance, 24-hours a day, 7-days a week, 365 days a year. This tasking may be a stand-alone tasking or as support of an existing Government help desk operation. The contractor shall provide customer assistance and information on warranty service, configuration, installation/implementation, systems administration, database administration, back-up/contingency planning, systems management, facilities management, operation of the contractor-provided software and hardware, and assistance to isolate, identify, and repair failures. The contractor shall provide trained technicians and shall provide technical assistance to users at worldwide installations. The contractor shall provide toll-free telephone access for obtaining technical assistance from worldwide locations. The contractor's technical assistance support shall be available 24-hours a day, 7-days a week, 365 days a year, worldwide.

Definitions:

Tier 1: Provides basic application software and/or hardware support to callers.
Tier 2: Provides more complex support on application software and/or hardware and is usually an escalation of the call from Tier 1.
Tier 3: Provides support on complex hardware and operating system software and usually involves subject matter experts.

4. GENERAL REQUIREMENTS

The contractor shall accomplish the following disciplined activities in support of tasks under this contract. These services shall include, but are not limited to, systems engineering, architecture and system design, information assurance, security, testing, technology refresh, and the provision of COTS manuals and supplemental data as described in the paragraphs that follow.

4.1 Contractors Use of NETCENTS-2 Products Contract

The contractor shall obtain all products and associated peripheral equipment required by each individual task order from the NETCENTS-2 Products contract.

4.2 Systems Engineering

The contractor shall employ disciplined systems engineering processes in accomplishing contract taskings, using commercial best practices in accordance with of AFI 63-1201, Life Cycle Systems Engineering or applicable ISR guidance, for systems engineering processes in planning, architecting, requirements development and management, design, technical management and control, technical reviews, technical measurements, integrated risk management, configuration management, data management, interface management, decision analysis, and test and evaluation, verification and validation. Task orders may further refine the systems engineering processes according to MAJCOM policies and practices. The contractor shall employ the principles of open technology development described in the DoD Open Technology Development Guidebook (http://www.acq.osd.mil/jctd/articles/OTDRoadmapFinal.pdf) and in Net-Centric Enterprise Solutions for Interoperability (NESI) body of knowledge (see http://nesipublic.spawar.navy.mil/) and systems engineering activities used in developing contractor solutions shall adhere to open architecture designs for hardware and software, and employ a modular open systems architecture approach. The contractor's systems engineering planning and design activities shall also adhere to the DoD's Information Sharing and Net Centric Strategies published by the DoD CIO (see http://www.defenselink.mil/cio-nii/) and the engineering body of knowledge and lesson's- learned accumulated in NESI.

All services provided under this contract shall be in compliance with the Federal Desktop Core Configuration (FDCC), Information Assurance guidelines, and Security Technical Implementation Guides

(STIGS) for collateral networks and systems. Services for Top Secret and SCI networks, systems and applications will be in compliance with standards, policies and guidelines identified in the task order.

4.3 Configuration Management

The contractor shall accomplish Configuration Management (CM) activities as described in the task order. CM activities include baseline identification, change control, status accounting, and auditing.

4.4 Architecture and System Design

The contractor shall support the design and development of systems and associated enterprise architectures. The contractor shall provide all required architectural documentation in compliance with Department of Defense Architectural Framework (DoDAF) Enterprise Architecture guidance or other frameworks as identified in the task order.

4.5 Information Assurance (IA)

The contractor shall ensure that all application deliverables meet the requirements of the DoD Information Assurance Certification and Accreditation Process (DIACAP) and DoDI 8500.2, ICD 503, or the most current standards and guidance that are applicable. This includes Certification and Accreditation (C&A) activities. The contractor shall provide applications services that are in compliance with and support DoD and USAF Public Key Infrastructure (PKI) policies or IC PKI policies as applicable. The contractor shall support activities to make applications PK-enabled (PKE) in order to achieve standardized, PKI-supported capabilities for digital signatures, encryption, identification and authentication. The contractor shall assist in defining user and registration requirements to Local Registration Authorities (LRAs). The contractor shall provide solutions that meet confidentiality, data integrity, authentication, and non-repudiation requirements. Contractor solutions shall comply with National Institute for Standards and Technologies (NIST) and Federal Information Processing Standards (FIPS) standards or IC standards as applicable.

4.6 Security

The contractor shall provide security and information assurance support, protecting information and information systems, and ensuring confidentiality, integrity, authentication, availability and non-repudiation. The contractor shall provide application services support for Certification and Accreditation (C&A) processes, DIACAP processes, SISSU processes, Enterprise Information Technology Data Repository (EITDR) certification or ICD 503.

4.7 Testing

The contractor shall conduct rapid testing and deployment of Core Data Services and Aggregation and Presentation Layer Services using distributed testing environments. The contractor shall develop dynamic testing environments to support C&A and functional testing. For mission systems and Top Secret networks, the contractor shall perform testing IAW standards, policies and guidelines identified in the task order.

4.7.1 Test Lab

When requested and specified in the task order, the contractor shall establish and maintain a system integrated test lab that is capable of supporting a full range of integration test activities for both the currently fielded system as well as maintenance/modernization releases. The currently fielded system includes the most current version and up to three previous versions for products that have not yet been declared ‘end of life.’ The contractor shall support test activities in areas which include, but are not limited to, product testing (regression testing and new capability testing), operational scenarios (real world simulation testing considering system topology and concept of operation, disaster recovery, clustering, and load balancing), stress and longevity (throughput, speed of service, and duration), interoperability, security (VPN, Firewall, security configuration of products and operating systems, and CAC Middleware testing), usability, transition (upgrade paths), and packaging/installation.

4.7.2 Product/System Integration Testing

The contractor shall perform testing and inspections of all system services to ensure the technical adequacy and accuracy of all work, including reports and other documents required in support of that work. The contractor shall conduct on-site testing when requested. When specified by the Government, the contractor shall participate with the Government in testing the complete communications system which may include premise equipment, distribution systems or any additional telecommunications equipment or operating support systems identified in the task order. After appropriate corrective action has been taken, all tests including those previously completed related to the failed test and the corrective action shall be repeated and successfully completed prior to Government acceptance. Pre-cutover audits will consist of verification of all testing completed by the contractor such that the system is deemed ready for functional cutover. As part of this audit, any engineered changes or approved waivers applicable to the installation will be reviewed and agreed upon between the contractor and the Government. Post-cutover audits will verify that all post-cutover acceptance testing has been performed satisfactorily IAW the standard practices and identify those tests, if any, which have not been successfully completed and must be re-tested prior to acceptance. Testing shall be performed in two steps: operational testing, then system acceptance testing. The contractor shall provide a logical test process that minimizes interruptions and avoids sustained downtime and presents a contingency procedure to be implemented in the event of systems failure during testing.

4.7.3 Simulated Operational Testing

The contractor shall conduct testing ranging from data entry and display at the user level combined with system loading to represent a fully operational system. The contractor shall accomplish operational testing IAW the Government-approved test plan as specified in the task order. The plan shall consist of a program of tests, inspections and demonstrations to verify compliance with the requirements of this contract. The contractor shall document test results in the test report(s). The contractor shall furnish all test equipment and personnel required to conduct operational testing. During the installation/test phase, the Government reserves the right to perform any of the contractor performed inspections and tests to assure solutions conform to prescribed requirements. The contractor shall be responsible for documenting deficiencies and tracking them until they are resolved. The Government will not be expensed for correcting deficiencies that were the direct result of the contractor's mistakes.

4.7.4 Acceptance Testing

The contractor shall provide on-site support during the acceptance-testing period. Acceptance testing shall be initiated upon acceptance of the operational test report and approval of the acceptance test plan. If a phased installation concept is approved in the Systems Installation Specification Plan (SIP), acceptance shall be based on the increments installed IAW the SIP. This on-site support shall be identified in the acceptance test plan.

4.7.5 System Performance Testing

The contractor shall provide system performance testing. The acceptance test will end when the system has maintained the site-specific availability rate specified in the task order. In the event the system does not meet the availability rate, the acceptance testing shall continue on a day-by-day basis until the availability rate is met. In the event the system has not met the availability rate after 60 calendar days, the Government reserves the right to require replacement of the component(s) adversely affecting the availability rate at no additional cost.

4.8 Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017, the Contractor shall disclose to the ordering Contracting Officer and ordering office in any proposal for a task order, or after award of a task order if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the task order. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the Contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the task order and its CDRL requirements and any cost/price associated with delivery. This disclosure requirement also applies to segregable routines of non-commercial software that may be developed exclusively at Government expense to integrate Commercial Software components or applications provided under a commercial software license or developed to enable Commercial Software to meet requirements of the Task Order. This disclosure obligation shall apply to technical data and non-commercial computer software developed exclusively at Government expense by subcontractors under any Task Order. Performance of this disclosure requirement shall be considered a material performance requirement of any task order under which such technical data or non-commercial computer software is developed exclusively at Government expense.

4.9 COTS Manuals and Supplemental Data

The contractor shall provide documentation for all systems services delivered under this contract. The contractor shall provide COTS manuals, supplemental data for COTS manuals, and documentation IAW best commercial practices (i.e. CD-ROM, etc.). This documentation shall include users' manuals, operators' manuals, maintenance manuals, and network and application interfaces if specified in the task order.

4.10 Enterprise Software Initiative

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular task order, the contractor shall first use available existing enterprise licenses, then products obtained via the DoD's Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs), and then the NETCENTS-2 products contract. The updated listing of COTS software available from DoD ESI sources can be viewed on the web at http://www.esi.mil. The NETCENTS-2 Application Services full and open task order Contracting Officer will authorize the contractor to use existing enterprise licenses or ESI vehicles for task orders issued under this contract. For mission systems and Top Secret networks, the contractor shall perform in accordance with and as specified in the task order.

4.11 Software License Management

When required at the task order level, the contractor shall provide maintenance and support to control the entire asset life-cycle, from procurement to retirement, which includes applications, license agreements as well as software upgrades. The contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The contractor shall support common practices for ordering assets, tracking orders and assets, and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, sustainment and configuration control, to include the procurement of supporting software licenses.

4.12 Transition and Decommissioning Plans

The contractor shall create transition and decommissioning plans that accommodate all of the non-authoritative data sources (non-ADS) interfaces and ensure that necessary capabilities are delivered using approved ADSs.

4.13 Prototypes

The contractor shall develop prototypes as required in task orders. The contractor shall operate and maintain prototype applications, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process. The contractor shall develop schedules and implementation plans with definable deliverables, including parallel operations where required, identification of technical approaches, and a description of anticipated prototype results

5. CONTRACT REQUIREMENTS

The following contract requirements are applicable to all Task Orders.

5.1 Performance Reporting

The contractor's performance will be monitored by the Government and reported in Contractor Performance Assessment Reporting (CPARs). Performance standards shall include the contractor's ability to provide or satisfy the following:

1. Provide quality products, incidentals, and customer support
2. Meet customer's agreed-upon timelines for scheduled delivery of items, warranty, and/or incidental services: Emergency/critical, Maintenance/Warranty – 24 x 7 x 365, and remote OCONUS, OCONUS vs. CONUS response times
3. Timely and accurate reports
4. Responsive proposals
5. Configuration assistance as identified in each delivery order

5.2 Program Management

The contractor shall identify a Program Manager who shall be the primary representative responsible for all work awarded under this contract, participating in Program Management Reviews and ensuring all standards referenced herein are adhered to.

5.2.1 Services Delivery Summary

The contractor's performance at the contract level will be assessed quarterly by a process that measures success towards achieving defined performance objectives. The Services Delivery Summary will be in

accordance with AFI 63-124, Performance Based Services Acquisition and FAR Subpart 37.6, Performance-Based Acquisition. Service Level Agreements (SLAs) will be defined in each task order.

Desired Outcome		Performance Objective	Performance Threshold	
Overall Outcome	Specific Outcomes		Target	Tolerance
Compliance w/ Application Services support requirements (delivery, quality)	Ensure compliance w/ Application Services deliverables requirements	Deliver the Application Services w/ predetermined outcomes and on time	Documentation submitted IAW CDRL A001 verifies task order was completed on time	98% of the time.
	Ensure compliance w/ Application Services Customer Support requirements	Customer Support: Availability for Application Services provided under contract	24x7 Live Customer Support assistance is provided if required by task order	98% of the time
	Ensure completed task orders are invoiced and submitted to the Government in a timely manner.	Invoices are received by the Government from the contractor within 30 calendar days of completion of task order.	Documentation submitted IAW CDRL A001 verifies invoices were submitted on time	99% of the time.
	Ensure delivery of all CDRLs by the contractor within the timeframe identified	Completed on time or ahead of schedule	CDRLs are delivered as identified	98% of the time.
	Ensure adherence to quality requirements of all CDRLs by the contractor	Quality CDRLs (conforming to design, specification or requirements) are delivered according to performance parameters	CDRLS are delivered as identified	98% of the time.
Compliance with Application Services Requirements	Ensure Application Services provided by the contractor are fulfilled within the timeframe identified by the task order.	Task orders are completed on time or ahead of schedule	Documentation submitted IAW CDRL A001 verifies task order was completed on time	98% of the time.

Compliance with Small Business Subcontracting Requirements	Contractor meets small business requirements	SB requirements listed in clause H133, or in the Subcontracting Plan, whichever is greater, are met	Documentation submitted IAW CDRL A006 verifies SB requirements were met	All requirements are met

Table 1. Minimum Required Performance Metrics

5.2.2 Task Order Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/task order manager who will oversee all aspects of the task order. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and solutions, support management and decision-making and facilitate communications. The contractor shall identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance shall be tracked, and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature, and continuously improving processes for administering all contract and task/delivery order efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness, and consistently high-quality delivery. The contractor shall provide transition plans as required.

5.2.3 Documentation and Data Management

The contractor shall establish, maintain, and administer an integrated data management system for collection, control, publishing, and delivery of all program documents. The data management system shall include but not be limited to the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters, and Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports.

5.2.4 Records, Files, and Documents

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition - Procedures and Responsibilities; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or the contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this PWS or the Application Services contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

5.2.5 Security

Individuals performing work under these task orders shall comply with applicable program security requirements as stated in the task order. NETCENTS-2 will support the following levels of security: Unclassified; Unclassified, But Sensitive; Secret (S); Secret Sensitive Compartmented Information (S/SCI); Top Secret (TS); and Top Secret Sensitive Compartmented Information (TS/SCI)

Certain task orders may require personnel security clearances up to and including Top Secret, and certain task orders may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed task order. The task orders may also require access to sensitive compartmented information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the task order. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and task order level and will encompass all security requirements. All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants, and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

The types of Personnel Security Investigations (PSI) required for the contractor vary in scope of investigative effort depending upon requirements of the Government and/or conditions of the contract/task order. In cases where access to systems such as e-mail is a requirement of the Government, application/cost for the PSI shall be the responsibility of the Government. In cases where access to systems is as a condition of the contract/task order, application/cost for the appropriate PSI shall be the responsibility of the contractor. In such instances, the contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work any active task order. Acquisition planning must consider antiterrorism (AT) measures when the effort to be contracted could affect the security of operating forces (particularly in-transit forces), information systems and communications systems IAW DoD Instructions 2000.16 Anti Terrorism Standards.

5.2.5.1 Transmission of Classified Material

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in the Task/Delivery Order.

5.2.5.2 Protection of System Data

Unless otherwise stated in the task order, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DOD Regulations 5400.7-R and 5200.1-R to include latest changes, and applicable service/agency/ combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or userid/password-based access controls. In either case, the certificates used by the Contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

5.2.6 Travel

The contractor shall coordinate specific travel arrangements with the individual Contracting Officer or Contracting Officer's Representative to obtain advance, written approval for the travel about to be conducted. The contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel in accordance with the basic contract clause H047.

If any travel arrangements cause additional costs to the task order that exceed those previously negotiated, written approval by CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use the tourist class, economy class, or similar accommodations to the extent they are available and commensurate with the mission requirements. Travel will be reimbursed on a cost reimbursable basis; no profit or fee will be paid.

5.2.7 Other Direct Cost (ODC)

The contractor shall identify ODC and miscellaneous items as specified in each task order. No profit or fee will be added; however, DCAA approved burden rates are authorized.

5.3 Contractor Manpower Reporting

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for Application Services via a secure data collection site. The contractor is required to completely fill in all required data fields at http://www.ecmra.mil.

Reporting inputs will be for 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 at contractormanpower@hqda.army.mil.

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

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.

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.

6. DATA DELIVERABLES

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the Government will result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness, or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall

formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers, and other data for which the Government shall treat as deliverable.

The contractor shall provide reports identified below. The format for each can be found in Section J, Exhibit A and B.

CDRL A001: Delivery/Task Order Status Report
CDRL A002: Fiscal Year Order & Financial Status
CDRL A003: Annual Review
CDRL A004: Contractor Performance Report
CDRL A005: Small Business Requirements
CDRL A006: Contractor Manpower Reporting

Exhibit B

CDRL B001: Small Business Participation

7. ELECTRONIC ORDERING AND PROCESSES

The vast majority of NETCENTS-2 products, services, or solutions will be procured using Requests for Quotes (RFQs) and Requests for Proposals (RFPs). The contractor shall establish a web site that is interoperable (electronically and procedurally) with the NETCENTS Portal, its follow-on (e.g., AFWAY II), or equivalent, within 30 working days after contract award to manage, report, and provide indicative data/status on all delivery orders, RFQs, and RFPs. The contractor shall maintain an operable interface with the current Government system and any future replacement system or changes to the existing system. While the plan is for AFWAY II to be available before NETCENTS-2 contract award, current Government capabilities may initially require NETCENTS-2 customers to follow a link on the legacy AFWAY system to get to the legacy NETCENTS Portal which will provide links to contractors' NETCENTS-2 web sites. Within 40 work days of NETCENTS-2 Contracting Officer announcement of the availability of AFWAY II, the contractor shall establish a working business-to-business (B2B) or Global Exchange (GEX) service interface through DISA with associated secure communications protocols and certificates or key-based authentication as required to communicate securely with NETCENTS-2 via AFWAY II. As the Government anticipates improving the web-based NETCENTS reporting capabilities and processes in the future, NETCENTS-2 contractors shall adjust and comply with Government efforts to standardize and modernize Government e-commerce capabilities in order to establish and improve interactive solicitation (pre and post award) processes and reporting. General policies and procedures will be established and published by the NETCENTS-2 PMO and shall be followed by the Contractor when transmitting, receiving, and processing NETCENTS-2 business documents.

8. QUALITY PROCESSES

As a minimum, the contractor shall be appraised at Level 3 or higher for Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI), or CMMI Development using the Software Engineering Institute's (SEI) Standard CMMI Appraisal Method for Process Improvement (SCAMPI) (Method A) by an SEI-authorized lead appraiser for the entire performance period of the contract, inclusive of options. This certification must be held at the prime offeror's organizational level performing the contract.

9. REFERENCE DOCUMENTS

The following certifications, specifications, standards, policies and procedures in Table 2 represent documents and standards that may be placed on individual contract task orders. Individual task orders may impose additional standards to those required at the contract level. The list below is not all-inclusive and the most current version of the document at the time of task order issuance will take precedence. Other documents required for execution of tasks issued under NETCENTS-2 will be cited in the relevant Task Order. Web links are provided wherever possible.

1. AF Enterprise Architecture (EA) Data Reference Model (DRM) https://wwwd.my.af.mil/afknprod/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-EA-AF-SE-2-5&Filter=OO-EA-AF-SE	2. AFI 33-210, AF Certification and Accreditation (C&A) Program (AFCAP), http://www.e-publishing.af.mil/shared/media/epubs/AFI33-210.pdf
3. AFI 33-200, Information Assurance, http://www.e-publishing.af.mil/shared/media/epubs/AFI33-200.pdf	4. Air Force IT Lean Reengineering and SISSU Guidebook v5.0, 7 June 2007 https://wwwd.my.af.mil/afknprod/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-SC-AF-47-1&Filter=OO-SC-AF-47

5. AFI 63-1201, Life Cycle Systems Engineering http://www.e-publishing.af.mil/shared/media/epubs/AFI63-1201.pdf	6. AFI 33-364, Records Disposition - Procedures and Responsibilities, http://www.e-publishing.af.mil/shared/media/epubs/AFI33-364.pdf
7. AFMAN 33-363, Management of Records, http://www.e-publishing.af.mil/shared/media/epubs/AFMAN33-363.pdf	8. Air Force Metadata Environment Concept https://www.gcss-af.com/noosphere/exec/version?name=USAF+Guidance+Documents&version=13
9. Air Force Policy Directive 33-3, Information Management, http://www.fas.org/irp/doddir/usaf/afpd33-3.pdf	10. Air Force Policy Directive 33-4, Enterprise Architecting
11. Air Force Instruction 33-401, Implementing Air Force Architectures, March 2007	12. American National Standards Institute (ANSI) Documents. http://www.ansi.org/
13. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C	14. CJCSI 6211.02c - DISN Policy and Responsibilities http://www.dtic.mil/cjcsdirectives/cdata/unlimit/621102.pdf
15. CMMI® for Development (CMMI-DEV), Version 1.2 (August 2006), http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html	16. COI Primer, 30 October 2006
17. Code of Federal Regulations (CFRs). http://www.access.gpo.gov/nara/cfr/	18. Data Interchange Standards Community (E-Business) http://www.disa.org/
19. Department of Defense Architecture Framework (DoDAF) Version 2.0 Volumes 1,2, and 3, dtd 28 May, 2009	20. DoDI 5200.40 - DoD Information Assurance Certification and Accreditation Process (DIACAP) http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf
21. DoD IPv6 Memorandum, June 9, 2003, and DoD CIO IPv6 Memorandum, 29 September 2003	22. DoD IPv6 Generic Test Plan, Version 3
23. DoD Discovery Metadata Specification (DDMS Version 1.4.1; http://metadata.dod.mil/mdr/irs/DDMS/documents/Documentindex.html	24. DoD Net-Centric Data Strategy dated May 9, 2003. http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf
25. DoD 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 06	26. SMI-ELS Strategic Concept Document, 1 September 2009
27. DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 2 https://www.opengroup.org/gesforum/ipv6/uploads/40/14291/DISRIPv6ProductProfilev2.0final15Jun07.pdf	28. DOD Guidance 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing" http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf

29. DoDD 8500.1 - Information Assurance (IA) http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf	30. DODI 8500.2, Information Assurance (IA) Implementation, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf
31. DoDI 8510.01, Information Assurance Certification and Accreditation Process (DIACAP), http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf	32. DoD IT Standards Registry (DISR) https://disronline.disa.mil/a/DISR/index.jsp
33. DoD Open Technology Development Guidebook (http://www.acq.osd.mil/jctd/articles/OTDRoadmapFinal.pdf)	34. Engineering for System Assurance, Version 1.0 (October 2008), http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct2008.pdf
35. Federal Desktop Core Configuration (FDCC), http://nvd.nist.gov/fdcc/index.cfm	36. Global Information Grid (GIG) https://www.jtfgno.mil/misc/mission.htm
37. Info-structure Technology Reference Model (i-TRM) https://itrm.hq.af.mil/itrm/Welcome.php	38. Institute of Electrical and Electronics Engineers (IEEE) Standards. Institute of Electrical and Electronics Engineers http://www.ieee.org/
39. ISO/IEC 15288: Systems and Software Engineering–Systems Life Cycle Processes, http://www.iso.org/iso/isocatalogue/catalogueics/catalogueetailics.htm?csnumber=43564	40. ISO/IEC 12207: Systems and Software Engineering–Software Life Cycle Processes, http://www.iso.org/iso/isocatalogue/cataloguetc/cataloguedetail.htm?csnumber=43447
41. International Committee for Information Technology Standards http://www.ncits.org/	42. ISO/IEC 26702: Systems Engineering–Application and Management of the SE Process, http://www.iso.org/iso/isocatalogue/cataloguetc/cataloguedetail.htm?csnumber=43693
43. International Standards Organization (ISO) Documents. http://www.iso.ch/iso/en/ISOOnline.openerpage	44. JTF-GNOP WARNORD 07-37, Public Key Infrastructure Implementation Phase 2
45. Joint Interoperability Test Command (JITC) Requirements http://jitc.fhu.disa.mil/	46. National Institute for Standards and Technology (NIST) (formerly National Bureau of Standards, NBS) Documents. http://www.nist.gov/
47. National Computer Security Center (NCSC) Documents. http://www.radium.ncsc.mil/	48. National Security Agency Guidelines http://www.niap-ccevs.org/
49. National Security Agency Rainbow Series http://www.fas.org/irp/nsa/rainbow.htm	50. Organization for the Advancement of Structured Information (Oasis) Standards http://www.oasis-open.org/home/index.php
51. Netcentric Enterprise Solutions for Interoperability (NESI), http://nesipublic.spawar.navy.mil/	52. Security Technical Implementation Guides (STIGS) http://iase.disa.mil/stigs/index.html
53. The Common Criteria Evaluation and Validation Scheme http://www.niap-ccevs.org/cc-scheme/	54. Singularly Managed Infrastructure - Enterprise Level Services Concept Document, September 2009
55. Systems Engineering Guide for Systems of Systems, Version 1.0 (August 2008), http://www.acq.osd.mil/sse/docs/SE-Guide-for-SoS.pdf	56. USAF Deficiency Reporting, Investigation and Resolution, TO 00-35D-54, http://www.tinker.af.mil/shared/media/document/AFD-070517-037.PDF

57. World Wide Web Consortium (W3C) Glossary http://www.w3.org/TR/ws-gloss/	58. Joint Vision 2020 http://www.fs.fed.us/fire/doctrine/genesisande volution/sourcematerials/jointvision2020.pdf
59. FAR Subpart 37.6, Performance-Based Acquisition. http://farsite.hill.af.mil/vffara.htm	60. Intelligence Community Directive 503, IT Systems Security, Risk Management, Certification and Accreditation 15 Sep 08, http://www.dni.gov/electronicreadingroom/ICD 503.pdf
61. Joint Capabilities Integration and Development System (JCIDS), CJCSI 3170.01G, 1 March 2009, http://www.dtic.mil/cjcsdirectives/cdata/unlimit/3170 01.pdf	62. Interoperability and Supportability of Information Technology and National Security Systems, CJCSI 6212.01E, 15 December 2008, http://www.dtic.mil/cjcsdirectives/cdata/unlimit/6 21201.pdf
63. Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), DoDI 4630.8, 30 Jun 04, http://www.dtic.mil/whs/directives/corres/pdf/463008p. pdf	64. Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), DODD4630.05, 23 April 2007, http://www.dtic.mil/whs/directives/corres/pdf/463 005p.pdf
65. Operation of the Joint Capabilities Integration and Development System, CJCSM 3170.01C, 1 May 2007, http://www.dtic.mil/cjcsdirectives/cdata/unlimit/m317 001.pdf	66. DoD CIO Department of Defense Net-Centric Data Strategy, 9 May 2003, http://www.defenselink.mil/cio-nii/docs/Net- Centric-Data-Strategy-2003-05-092.pdf
67. OASD Net-Centric Checklist, Ver. 2.1.3, 12 May 2004, https://acc.dau.mil/CommunityBrowser.aspx?id=2220 3	68. Net-Centric Operations & Warfare Reference Model, https://acc.dau.mil/CommunityBrowser.aspx?id= 28986&lang=en-US
69. Industry Best Practices in Achieving Service Oriented Architecture (SOA), 22 April 2005, http://www.sei.cmu.edu/library/assets/soabest.pdf	70. Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG), DODD 8100.2, [Date], http://www.dtic.mil/dticasd/sbir/sbir041/srch/n076 .pdf
71. Global Information Grid (GIG) Overarching Policy, DODD 8100.1, 21 November 2003, http://www.acq.osd.mil/ie/bei/pm/ref- library/dodd/d81001p.pdf	72.

Table 2. Applicable Documents and Standards

OPR: ESC DET 1/CCQ1
Mr. Mark
Jozwiak
***AFLCMC BES*Ph: 334-416-4820**

SECURITY REQUIREMENTS FOR CONTRACTORS REQUIRING ACCESS TO CLASSIFIED INFORMATION

1. ***Security Facility Clearance Requirements:*** The contractor must possess or obtain an appropriate facility security clearance as identified below prior to performing work on a classified government contract. **(Please check one):**

_____Top Secret

_____Secret

_____ Confidential

If the contractor does not possess a facility clearance the government will request one. The contractor shall notify the 42d Air Base Wing Information Protection Office (42 ABW/IP) before on-base performance of the service. The notification shall include:

a. Name, address, and telephone number of company representatives.

b. The contract number and contracting agency.

c. The highest level of classified information which contractor employees require access to.

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.

2. ***Personnel Security Clearance Requirements:*** Personnel will require a security clearance as identified below to perform this contract. **(Please check one):**

_____ Top Secret

_____ Secret

The government assumes costs and conducts security investigations for Top Secret, Secret, and Confidential security clearances. The contractor shall request security clearances for personnel requiring access to classified information within 15 days after receiving a facility clearance or, if the contractor is already cleared, within 15 days after service award. Due to costs involved with security investigations, requests for contractor

security clearances shall be kept to an absolute minimum necessary to perform service requirements.

3. Security Manager Appointment: The contractor shall appoint a security manager for the on base long-term visitor group. The security manager may be a full-time position or an additional duty position. The security manager shall provide contractor employees with training required by DoD 5200.1-R, *Information Security Program Regulation,* Chapter 10, AFPD 31-4, *Information Security,* and AFI 31-401, *Information Security Program Management*. The contractor security manager 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, *Integrated Defense.*

4. Visit Request: Contractors participating in the National Industrial Security Program are authorized to use Joint Personnel Adjudication System (JPAS) in lieu of sending Visitor Authorization Letters (VALs) for classified visit to Department of Defense facilities and military installations. VALs are only required if the contractor isn't using JPAS or if contractor personnel whom access level and affiliation are not accurately reflected in JPAS. However, some agencies may still require VALs to be submitted for access to their facilities.

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:

g. The contractor shall obtain base identification 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.

h. 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. The contracting officer will endorse the request and forward it to the issuing base pass and registration office for processing. When reporting to the base pass and registration office for issue of military identification credentials for access to the installation, contractor individual(s) will need a valid state or federal issued picture identification. To operate a vehicle on base contractor individual(s) will need to provide a valid driver's license, current vehicle registration, and a valid vehicle insurance certificate.

i. During performance of the service, the contractor shall be responsible for obtaining required identification for newly assigned personnel and for prompt return

of credentials for any employee who no longer requires access to the work site.

j. 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 have been turned in. The DD Form 577 (signature card) for the contractor authorized requestor will be destroyed and the individual will no longer be authorized to sign DD Form 1172 (Application for Uniform Services Identification Cards).

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

6. *Pass and Identification Items:* The contractor shall ensure the following pass and identification items as required for contract performance are obtained for employees:

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. AF Form 1199, *USAF Restricted Area Badge,* or a locally developed badge, if required.

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

7. *Entry Procedures For AFLCMC BES Facilities*: Contractor employees require an AFLCMC BES access badge for unescorted entry into AFLCMC BES facilities. To obtain an AFLCMC BES access badge contractor personnel must be in JPAS or have a VAL on file with AFLCMC BES /Gunter Security Office. Contractors requiring an access badge will bring a completed AF Form 2586, Unescorted Entry Authorization Certificate to the AFLCMC BES /Gunter Security Office. The AF Form 2586 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 while in AFLCMC BES facilities. When the FPCON level is higher than ALPHA contractors must wear the AFLCMC BES badge in addition to wearing their company's badge.

8. *Visitor Group Security Agreement (VGSA):* The contractor shall enter into a long-term visitor group security agreement for contract performance on base. This agreement shall outline how the contractor integrates security requirements for contract operations

with the Air Force to ensure effective and economical operation on the installation. The agreement shall include:

a. Security support provided by the Air Force to the contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations and the use of security forms and conducting inspections required by DoD 5220.22-R, *Industrial Security Regulation,* Air Force Policy Directive 31-6, *Industrial Security,* Air Force Instruction 31-601, *Industrial Security Program Management,* DoD 5200.1-R, *Information Security Program,* and AFI 31-401, *Information Security Program Management.*

b. Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.

c. On base, the long-term visitor group security agreement may take the place of a *Standard Practice Procedure* (SPP).

***9. Unescorted Entry to Restricted Areas*:** Contractor personnel requiring unescorted entry to restricted areas designated by the installation commander shall comply with base access requirements; AFI 31-101, *Integrated Defense*, DoD 5200.2-R, and AFI 31-501, *Personnel Security Program Management*, as applicable. Contractor personnel shall be the subject of a favorably completed NACI investigation to qualify for unescorted entry to a restricted area. The Air Force shall submit NACI investigations for contractor employees at no additional cost to the contractor. Contractor personnel must contact the unit security manager to obtain the required paperwork for NACI and restricted area badges.

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

11. Computer and Network Access Requirements: Contractor personnel working on this contract must be designed in one of the below AIS positions and complete the required security investigation to obtain the required security clearance. This must be accomplished before operating ***government furnished*** computer workstations or systems that have access to ***Air Force*** e-mail systems or computer systems that access classified information. The government at no additional cost to the contractor shall submit these investigations. The contractor shall comply with the DoD 5200.2-R, *Personnel Security Program* and AFI 33-119, *Air Force Messaging*, requirements. **(Please check one): (Please check one):**

____ **AIS-I Position - Critical-Sensitive Positions. Security Clearance: TOP SECRET based SSBI**. Responsible for the planning, direction, and

implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

AIS-II Position - Noncritical-Sensitive Positions. Security Clearance: SECRET based on a NACLC/ANACI. Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the AIS-I category, includes, but is not limited to; access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts.

AIS-III Position - Nonsensitive Positions. No security clearance required but is a Trusted Position based on NACI. All other positions involved in U.S. Government computer activities.

12. 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 an appropriate authority 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.

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.

14. Wireless Electronic Devices: No cell phones, camera cell phones, cordless telephones, or wireless microphones, keyboards, or mice, wireless or Infrared Local Area Networks (LANs), or devices are allowed in areas where classified information is discussed, briefed, or processed. ***"Area"*** refers to a room and/or to a space the size of a 3-meter radius sphere, centering on the classified source. In areas where classified information is discussed, briefed, or processed, wireless pointer/ mice devices are allowed for presentations only. This is an acceptable EMSEC risk. All other Personal Electronic Devices, PEDs. All other wireless PEDs not specifically addressed above, that are used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted.

15. Operating Instructions: The contractor will adhere to the Air Force activity Operating Instructions for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations.

16. Key Control: The contractor will adhere to the Air Force activity Operating Instructions control procedures 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. All government issued keys will be turned at the end of employment or contract. Lost keys shall be reported immediately to the Air Force activity that issued the keys. 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 to the contractor.

17. 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 duties, unless authorized by the government functional director.

18. Access Lock Combinations: Access lock combinations are "For Official Use Only" and will be protected from unauthorized personnel. The contractor will adhere to the Air Force activity operating instructions 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.

19. Security Combinations: Combinations to security containers, secure rooms, or vaults are classified information and must be properly safeguarded. Only contractor employees, who have the proper security clearance and the need-to-know, will be given combinations to security containers, secure rooms, or vaults. Contractor employees are responsible for properly safeguarding combinations. Contractor employees will not record security containers, secure rooms, or vaults combinations without written approval by the government functional director. Contractors will not change combinations to security containers, secure rooms, or vaults without written approval by the security officer and the government functional director.

20. 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 adhere to the Air Force activity operating instructions and 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.

21. 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 maintain records in accordance Air Force manual (AFMAN) 33-363, Management of Records; and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/.

***22. Traffic Laws*:** The contractor and their employees shall comply with base traffic regulations.

23. Cellular Phone Operation Policy: The use of cellular phones while operating a motorized vehicle is prohibited on Maxwell-Gunter. Although discouraged, drivers are authorized to use devices, i.e. ear bud or ear boom, which allows their cellular phone to be operated hands-free. The device must not cover both ears. This policy applies to everyone driving on Maxwell-Gunter AFB.

24. Security Education and Training: The contractor will be required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system.

26. *Healthcare:* Healthcare provided at the local military treatment facility on an emergency reimbursable basis only.

SECURITY REQUIREMENTS FOR UNCLASSIFIED SERVICES

1. *Contractor Notification Responsibilities:* The contractor shall notify the 42d Air Base Wing Information Protection Office 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.

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 42d Air Base Wing Information Protection Office with name and telephone number of the security manager.

3. *Visit Request:* Contractors participating in the National Industrial Security Program are authorized to use Joint Personnel Adjudication System (JPAS) in lieu of sending Visitor Authorization Letters (VALs) for classified visit to Department of Defense facilities and military installations. VALs are only required if the contractor isn't using JPAS or if contractor personnel whom access level and affiliation are not accurately reflected in JPAS. However, some agencies may still require VALs to be submitted for access to their facilities.

4. *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 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. The contracting officer will endorse the request and forward it to the issuing base pass and registration office for processing. When reporting to the base pass and registration office for issue of military identification credentials for access to the installation, contractor individual(s) will need a valid state or federal issued picture identification. To operate a vehicle on base contractor individual(s) will need to provide a valid driver's license, current vehicle registration, and a valid vehicle insurance certificate.

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 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 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.

5. *Pass and Identification Items:* The service shall ensure the following pass and identification items required for service performance are obtained for employees:

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

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

6. ***Entry Procedures for AFLCMC BES Facilities:*** Contractor employees require an AFLCMC BES access badge for unescorted entry into AFLCMC BES facilities. To obtain an AFLCMC BES access badge contractor personnel must be in JPAS or have a VAL on file with AFLCMC BES /Gunter Security Office. Contractors requiring an access badge will bring a completed AF Form 2586, Unescorted Entry Authorization Certificate to the AFLCMC BES /Gunter Security Office. The AF Form 2586 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 while in AFLCMC BES facilities. When the FPCON level is higher than ALPHA contractors must wear the AFLCMC BES badge in addition to wearing their company's badge.

7. Computer and Network Access Requirements: Contractor personnel that required access to unclassified government computers and operations systems (Automated Information Systems – AIS) will be designated as **AIS-III - Nonsensitive Positions.** Contractor personnel must submit a *National Agency Check with Inquiries (NACI)* and the NACI be favorability adjudicated before operating ***government furnished*** computer workstations or systems 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, *Air Force Messaging*, requirements.

8. Unescorted Entry to Restricted Areas: Contractor personnel requiring unescorted entry to restricted areas designated by the installation commander shall comply with base access requirements; AFI 31-101, *Integrated Defense*, DoD 5200.2-R, and AFI 31-501, *Personnel Security Program Management*, as applicable. Contractor personnel shall be the subject of a favorably adjudicated *National Agency Check with Inquiries (NACI)* investigation to qualify for unescorted entry to a restricted area. The Air Force shall submit NACI investigations for contractor employees at no additional cost to the contractor. Contractor personnel must contact the unit security manager to obtain the required paperwork for NACI and restricted area badges.

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.

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 maintain records in accordance Air Force manual (AFMAN) 33-363, Management of Records; and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/.

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 42d Air Base Wing Information Protection Office, 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. 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.

13. Internal Operating Instructions: The contractor will adhere to the Air Force activity operating instructions (OI) for internal circulation control, protection of resources, and to regulate entry into Air Force controlled areas during normal, simulated, and actual emergency operations.

14. Key Control: The contractor will adhere to the Air Force activity operating instructions control procedures 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. All government issued keys will be turned at the end of employment or contract. Lost keys shall be reported immediately to the Air Force activity that issued the keys. 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.

15. 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.

16. Access Lock Combinations: Access lock combinations are "For Official Use Only"

and will be protected from unauthorized personnel. The contractor will adhere to the Air Force activity operating instruction (OI) for 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.

17. 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 adhere to the Air Force activity operating instructions and 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.

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

19. C***ellular Phone Operation Policy:*** The use of cellular phones while operating a motorized vehicle is prohibited on Maxwell-Gunter. Although discouraged, drivers are authorized to use devices, i.e. ear bud or ear boom, which allows their cellular phone to be operated hands-free. The device must not cover both ears. This policy applies to everyone driving on Maxwell-Gunter AFB.

***20. Security Education and Training*:** The contractor will be required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system.

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

PERFORMANCE PLAN

FOR

NETWORK CENTRIC SOLUTIONS-2 (NETCENTS-2)

APPLICATION SERVICES
(FULL & OPEN)

1.0 Introduction

1.1. Objective. The goal of this NETCENTS-2 Application Services contract is to provide access to a wide range of services such as sustainment, migration, integration, training, help desk support, testing and operational support. Other services include, but are not limited to, exposing data from Authoritative Data Sources (ADS) to support web-services or Service Oriented Architecture (SOA) constructs in AF enterprise environments. NETCENTS-2 will support United States Air Force, Department of Defense (DoD), and other U.S. federal agency customers that work in transitory, static, and deployed locations throughout the world.

Use of the, Application Services contracts are available to DoD and Other Federal Agencies when any of the following criteria exists:

- be related to requirements for interoperability with Air Force capabilities;
- supports Air Force IT infrastructure, applications, or operations;
- supports host-tenant arrangements involving Air Force units; or
- support of joint operations or solutions.

The focus of this contract is to provide application services support to mission areas, as overseen by portfolio managers, Communities of Interest (COIs), project offices, and program offices. This contract will also help the DoD achieve information superiority as called for in Joint Vision 2020 and will support adherence to the Systems Engineering Process (SEP) as specified in the DoD 5000-series.

1.2. Contract Result. The intended result of the performance-based acquisition used in this contract is to benefit both the government and the contractor and allow them to join together as a seamless team to support and achieve the objectives stated above. This partnership will be based on trust, cooperation, and mutual respect. This performance plan sets forth a business strategy to accomplish these results built on the following precepts:

- The contract and source selection process should focus on communicating the outcomes the contractor is expected to achieve
- The contractor takes the primary lead in collecting performance data in an "open book" relationship with the government
- The government will seek to gain visibility into the performance of the contractor and reduce oversight whenever possible
- By focusing on outcomes instead of the "how to" process, the government will enable the contractor to improve their support processes, reduce costs, and enhance performance
- The relationship between the contractor and the government will be a partnership committed to the mutual success of each party
- The contractor will be rewarded based on performance achieved against outcomes

communicated in the Performance Work Statement (PWS) and Service Delivery Summary (SDS).

1.3. Compliance With Policy. The business strategy used in this contract complies with Air Force Instruction 63-124, Performance Based Services Acquisition. It revolves around a Management Oversight Team (MOT) to perform the functions of a centralized performance management office. This Performance Plan (PP) replaces the Quality Assurance Surveillance Plan (QASP) required by AFI 63-124. Unlike a QASP, the PP becomes a part of the contract. The Government reserves all rights regarding inspection of services provided by the clauses of the contract.

2.0 Performance Management Strategy

2.1. Performance Management Approach. Performance management refers to the approach taken to monitor, manage, and take action on contractor performance against expected outcomes communicated in the PWS. Performance management rests upon developing a capability to review and analyze information generated through performance measures. The ability to make decisions based on performance data analysis is the cornerstone of performance management. The data generated in a performance management approach provides information that indicates whether or not expected outcomes are being achieved adequately by the contractor. Performance measures used in performance management will focus on desired outcomes and not on interim process steps. The interim process performance measures and controls are the responsibility of the contractor who will be responsible for managing the processes and practices used to achieve contract outcomes. An effective system and process that generates well-defined performance data is central to performance management.

2.2. Focus On Service Delivery Summary (SDS) Outcomes. Performance management also represents a significant shift from the more traditional Quality Assurance concepts in several ways. Performance management only focuses on assessing whether or not SDS outcomes are being achieved and migrates away from scrutiny on the process and practices used to achieve the outcomes. The only exceptions to process reviews are those required by law and compelling business situations such as safety, security and resource protection. An outcome focus provides the contractor with the flexibility to continuously improve and innovate over the course of the contract as long as the critical SDS outcomes expected are being achieved at the desired levels of performance. By focusing on the desired outcomes rather than processes, performance based sourcing relationships unlock the contractor's potential for innovation and performance improvement.

2.3. Strategy Precepts. An established management oversight team and a dedicated quality assurance team will monitor the Contractor's performance. The post award teams will be actively involved with both vendors and customers through CDRLs, CPARs and PMRs at both the contract and individual task order levels. The AFLCMC EIS/HIJK NETCENTS-2 Post Award Team will:

- Administer the basic contracts

- Provide a Management Oversight Team that will accomplish the following:
  - Surveillance of decentralized orders
  - Coordinate on D&Fs and close monitoring of all Labor Hour orders
  - Implement Lessons Learned from NETCENTS

- Conduct Performance Management Reviews
- Technology Governance Team
- Customer Support
- Provide On-Site Training for Contract Ordering Process
- Dedicated Customer Support Team
- Provide and update Ordering Guide
- On-going communication via NETCENTS-2 Web site/phone or other media
- The government will identify the performance measures it requires to be tracked to determine whether the outcomes are being achieved at the appropriate levels of performance
- The government will define each performance measure and the data requirements for calculating the value of each over the appropriate time period.
- The contractor may use additional performance indicators for managing their processes and operations or for supplementing government's performance measures.
- The contractor will provide the information collection and analysis tools to capture the data required by the performance measures identified by the government.
- The contractor will be responsible for making the required changes in processes and practices to ensure performance is managed effectively.

3.0 Roles and Responsibilities

3.1. Team Member Roles and Responsibilities. The roles and responsibilities necessary to the success of the contract are distributed as follows:

3.1.1. Senior Contracting Official
- Serves as senior advisor to Management Oversight Team (MOT).
- Provides support to the MOT to ensure its personnel can accomplish their performance management role

3.1.2. Contracting Officer/Contract Specialist (CO)
- Ensures open communication is maintained between all parties, pre- and post-award.
- Reviews contractor performance documentation on a regular basis to ensure performance is compatible with contract and mission objectives.
- Informs the contractor of the names, duties, and limitations of authority for all QAP assigned to the contract.
- Manages contractor performance assessment data, including submitting Contractor Performance Assessment Reporting System (CPARS) reports.
- Issues contract modifications as necessary.
- Takes appropriate action should unacceptable contract performance occur.
- Certifies acceptance of services.

3.1.3. Management Oversight Team
- Develops technical requirements and independent cost/Government estimates for contract

services.

- Assesses and documents the contractor's performance in accordance with the procedures set forth in this performance plan.
- Immediately notifies the CO of any significant performance deficiencies.
- Maintains assessment documentation throughout the life of the contract.

3.1.4. Quality Assurance Program Coordinator (QAPC)
- Coordinates all aspects of the quality assurance program
- Provides training for the MOT personnel.

3.1.5. Contractor
- Complies fully with the terms and conditions of the contract.
- Maintains and implements a Quality Control Plan (QCP) that conforms with the performance plan.
- Ensures that non-conforming contract services are identified and corrected and the QCP is revised to prevent recurrences.
- Provides services that conform to contract requirements to the Government for acceptance.
- Recommends changes to the contract that will provide more effective operations or eliminate unnecessary costs.

4.0 The Performance Management Process

4.1. The Process Components. The performance management process is comprised of several components:

- *Continually communicating expectations*
- *Reviewing and validating performance measures and sources of measurement data*
- *Performance Measurement*
- *Developing performance reports*
- *Reviewing performance measurement data and trends with the contractor*
- *Making consultative decisions with the contractor on action to be taken*
- *Attending Performance Management Meetings*
- *Performance Management Team*

4.2. Continually Communicating Expectations. The performance management process depends upon free and open communications between the government and the contractor. The government will provide on-going communication via NETCENTS-2 web site, phone, or other media. Performance expectations for the service areas are delineated in the PWS, SDS and the PP. The government will partner with the contractor to explore means to reduce the costs of the service while maintaining or improving the overall service level within the constraints of the

contract and the level of funding. The contractor will keep the government informed of the status of outside taskings and roadblocks to performance. It is the contractor's responsibility to balance customer satisfaction, fiscal constraints, and mission priorities.

4.3. Reviewing and validating performance measures and sources of measurement data. The contractor will be provided with a list of performance measures selected by the government that measure contractor performance against outcomes identified in the PWS and SDS and against customer satisfaction in the PP. The SDS table is provided as an attachment to this PP. The government will provide the contractor with any known data sources for the performance measures. The contractor will collect and maintain the source data for all of the performance measures and make this data available for validation of the contractor's reported performance.

4.3.1. Quality Control Plan (QCP). The contractor will create a QCP that details how the contractor will gather, store, and make available to the PMT the data used to calculate all of the performance measures. The data collected by the contractor should support monthly, quarterly, semi-annual and annual performance reporting. The contractor will use government legacy systems, whenever possible, as the primary systems for performance measurement data collection. The contractor may need to augment existing systems and tools for capturing and controlling all performance measurement data and make this data available. Performance measurement data will be non-proprietary. The government will have open access to any data collection system that contains performance measurement data. The request for government acceptance of the QCP should specifically address the following for every measurement:

- *The process used by the contractor to collect all performance measurement data*
- *The sources from which the data will be collected*
- *The tools that will be used to collect data - government systems or other*
- *How the contractor proposes to validate the data collected*
- *How the data will be controlled and made available*

4.4. Performance Measurement. The post award team will be actively involved with both vendors and customers through CDRLs, CPARs, and PMRs at both the contract and individual task order levels. Performance metrics will be tracked, validated by random surveillance, and discussed at PMRs.

4.4.1. Small Business (SB) Goals. Contractors will be measured in how they achieved their SB goals. Achievement of this goal will be cumulative and calculated on an annual basis. The goals are described in H-133, Small Business Subcontracting Requirements and Incentives (Apr 2009).

4.5 Changes to Performance Measures. The government reserves the right to unilaterally change or replace performance measures and change the method, frequency or types of audits and inspections. In the spirit of partnership the government will work with the contractor on projected changes.

	Category Department of the Air Force	Percent Marketing	Functional Skill Sets HQ 754 Electronic Systems Group 2 (NETCENTS-2) Applications Services	Offeror Labor Category	Offeror Labor Category Description (Qualifications, Skill Sets, Skill Levels)	Experience/Training
	Administrative					
			Responsible for the operational planning, establishment, execution, and evaluation of a multifaceted program/project typically consisting of a set of closely related subprograms or associated activities. Responsible for fiscal, operational, administrative, and human resources management of the program; seeks and develops outside funding sources, serves as principal point of representation and liaison with external constituencies on operational matters, and provides day-to-day technical/professional guidance and leadership as appropriate to the area of			
			ft Under general direction, provides second-tier support to end-users for PC, server, mainframe applications, and hardware. Handles problems that the first-tier of help desk support is unable to resolve. May interact with network services, so			
			ware systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user			

1	Program Manager, Senior Level	10%		Program Manager, Senior Level	Qualifications and skills as described in column D, plus PMI & ITIL (at least foundation) certified. Bachelor's degree. Clearance up to TS/SCI level.	Up to 8 years experience in this work. PM/PMI Training (includes at least fundamentals of project management, risk management, schedule and cost management training). Defense Industry Initiative (DII) training. IBM Data Security & Privacy training.
2	Help Desk Support Specialist, Senior Level	5%	problems	Help Desk Support Specialist, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. At least a High School diploma. Clearance up to TS/SCI level.	Up to 3 years experience in operating a help desk as first or second tier support. Trained in trouble ticketing systems. Trained in the systems supported. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.

	Category	Percent	Functional Skill Sets	Offeror Labor Category	Offeror Labor Category Description (Qualifications, Skill Sets, Skill Levels)	Experience/Training

3	Configuration Management Specialist, Senior Level	5%	Under general direction, responsible for effectively tracking, logging, categorizing, and maintaining changes made against the accepted baseline(s) standards. Develops, distributes, and tracks all change packages resulting from approved Configuration Control Board action. Provides daily support and direction to staff as to change status requirements, deadlines, and problems.	Configuration Management Specialist, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. Bachelor's degree. Clearance up to TS/SCI level.	Up to 8 years experience in the IT field specializing in configuration management. Trained in the use of configuration management processes and tools. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.
4	Disaster Recovery Administrator, Senior Level	5%	Under general direction, designs and administers programs to include policies, standards, guidelines, training programs, and a viable quality assurance process for disaster recovery. Under general direction, reviews the testing and implementation of software, data systems, and data networks to ensure that the integrity and security of electronic data and data systems are adequately protected. Facilitates the preparation of an organization-wide business resumption plan.	Disaster Recovery Administrator, Senior Level	Qualifications and skills as described in column D, plus, ITIL (at least foundation) certification. May be certified in one of Certified Functional Continuity Professional (CFCP), Certified Business Continuity Professional (CBCP), Master Business Continuity Professional (MBCP), CBCP (Certified Business Continuity Professional) or Master (MBPC) certified. and MBCP (Master Business Continuity Professional) certified. Bachelor's degree in computer sciences or related field. Clearance up to TS/SCI level.	Up to 8 years experience in managing large multi-site data center and experience leading the development and maintenance of Disaster Recovery Plans. Training towards certification. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.

	Category	Percent	Functional Skill Sets	Offeror Labor Category	Offeror Labor Category Description (Qualifications, Skill Sets, Skill Levels)	Experience/Training
	Functional					
5	Functional Expert, Senior Level	25%	Responsible for providing analytical skills to support process improvement, specialized studies, and definition of requirements. Typical duties include analysis, planning, developing requirements documents, building functional models, developing procedures, developing functional architectures, and other related management and technical duties. Requires expertise in specialty area	Functional Expert, Senior Level	Qualifications and skills as described in column D, plus Bachelor's degree. Clearance up to TS/SCI level.	Up to 8 years experience in this field of work. Knowledge of software development, trained in business modeling tools. Defense Industry Initiative (DII) training. IBM Data Security & Privacy training.
	Technical					
6	Applications Programmer, Senior Level	5%	Responsible for devising or modifying procedures to solve complex problems considering computer equipment capacity and limitations, operating time and form of desired results. Designs, codes, tests, debugs and documents those programs.	Applications Programmer, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. Bachelor's degree in computer sciences or related field. Clearance up to TS/SCI level.	Up to 8 years experience in this field of work. Trained in specific languages for web applications e.g. HTML, CGI and JavaScript. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.

	Category	Percent	Functional Skill Sets	Offeror Labor Category	Offeror Labor Category Description (Qualifications, Skill Sets, Skill Levels)	Experience/Training
7	Applications System Analyst, Senior Level	5%	Responsible for formulating/defining system scope and objectives based on user needs. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time and form of desired results. Prepares detailed specifications from which programs will be written. Analyzes and revises existing system logic difficulties and documentation as necessary. May use CASE tools.	Applications System Analyst, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. Bachelor's degree, could be certified in area of specialty (e.g. Service Oriented Architecture or Systems Architecture field). Clearance up to TS/SCI level.	Up to 8 years experience in this field of work. Trained in CASE. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.
8	Computer Systems Analyst, Senior Level	5%	Responsible for providing technical and administrative direction for personnel performing software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinates with the Project and/or Program Manager to ensure problem solution and user satisfaction. Makes recommendations if needed for approval of major system installations. Prepares milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives. Provides daily supervision and direction to support staff	Computer Systems Analyst, Senior Level	Qualifications and skills as described in column D, plus IBM Architect Certification or equivalent. ITIL (at least foundation) certified. Bachelor's degree. Clearance up to TS/SCI level.	Up to 8 years experience in this work. Training classes required for certification as an Architect, including Service Oriented Architecture (SOA), J2EE Architecture, and/or Enterprise Architecture certification. Trained in one or more of RequisitePro, Rational Rose, SoDA. Defense Industry Initiative (DII) training. IBM Data Security & Privacy training.

	Category	Percent	Functional Skill Sets	Offeror Labor Category	Offeror Labor Category Description (Qualifications, Skill Sets, Skill Levels)	Experience/Training
9	Database Analyst, Senior Level	5%	Responsible for designing, implementing and maintaining complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Includes maintenance of database dictionaries, overall monitoring of standards and procedures, and integration of systems through database design.	Database Analyst, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. Certified in specific area of focus such as Microsoft SQL Server. Bachelor's degree in computer sciences or related field. Clearance up to TS/SCI level.	Up to 8 years experience in this field of work. Oracle, Microsoft, and/or SQL training. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.

	Category	Percent	Functional Skill Sets	Offeror Labor Category	Offeror Labor Category Description (Qualifications, Skill Sets, Skill Levels)	Experience/Training
	Engineering					
10	Electronic Data Interchange (EDI) Specialist, Senior Level	5%	Under general direction, analyzes, designs, and develops specifications for enhancements and extensions with EDI application interfaces and maps. Coordinates EDI testing and trading partner implementation initiatives. Provides support for EDI database analysis, design, and operations. Establishes and maintains communications within organization and with partners. Conducts and manages product evaluations. Provides product installation, configuration, and training. Performs systems maintenance to update records, specifications, and operating procedures of partner systems. Maintains EDI account transaction activities.	Electronic Data Interchange (EDI) Specialist, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. Bachelor's degree in computer science or related area. Clearance up to TS/SCI level.	Up to 8 years experience in this work. Trained in EDI and programming. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.

	Category	Percent	Functional Skill Sets	Offeror Labor Category	Offeror Labor Category Description (Qualifications, Skill Sets, Skill Levels)	Experience/Training
11	Systems Engineer, Senior Level	20%	Responsible for performing high-level systems analysis, evaluation, design, integration, documentation, and implementation of very complex applications that require a thorough knowledge of administrative and technical skills. Directs and participates in all phases of system development with emphasis on planning, analysis, evaluation, integration, testing and acceptance phases (IV&V and DT&E). Applies higher-level business or technical principles and methods to very difficult technical problems to arrive at automated engineering solution. Designs and prepares technical reports and related documentation, and makes charts and graphs to record results.	Systems Engineer, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. Bachelor's degree in Computer science or related area. Clearance up to TS/SCI level.	Up to 8 years experience in designing complex large scale IT systems across the entire stack - applications, hardware and network. Ability to lead and guide a team of less experienced system engineers. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.
12	Computer Security Specialist, Senior Level	5%	Responsible for using current information security technology disciplines and practices to ensure the confidentiality, integrity and availability of corporate information assets in accordance with established standards and procedures. Develops and maintains knowledgebase on changing regulatory, threat, and technology landscapes to continually develop or maintain security policies and standards, and ensure compliance throughout the organization.	Computer Security Specialist, Senior Level	Qualifications and skills as described in column D, plus ITIL (at least foundation) certified. Certified in Information Systems Security Professional (CISSP), or Certified Information Systems Auditor (CISA), or Certified Information Security Manager (CISM). Clearance up to TS/SCI level.	Up to 8 years experience in this field of work. Training for certifications. Defense Industry Initiative (DII) and IBM Data Security and Privacy training.

$120.00	$123.44	$127.03	$130.80	$134.72	$138.68	$142.58	$146.68	350	$45,385.20
$126.31	$129.95	$133.71	$137.69	$141.82	$145.97	$150.10	$154.42	350	$47,503.40
$130.63	$134.40	$138.30	$142.39	$146.68	$150.97	$155.24	$159.70	350	$49,317.10
$127.35	$131.01	$134.80	$138.84	$142.99	$147.16	$151.32	$155.66	350	$48,101.20
$136.36	$140.29	$144.34	$148.62	$153.09	$157.58	$162.02	$166.68	350	$51,668.05
$127.35	$131.01	$134.80	$138.84	$142.99	$147.16	$151.32	$155.66	350	$47,884.90
$129.93	$133.66	$137.52	$141.62	$145.87	$150.15	$154.38	$158.82	1,750	$244,181.00
$93.79	$96.48	$99.28	$102.24	$105.30	$108.38	$111.45	$114.64	350	$35,631.75
$124.66	$128.25	$131.97	$135.90	$139.97	$144.06	$148.14	$152.41	700	$95,044.60
$127.35	$131.01	$134.80	$138.84	$142.99	$147.16	$151.32	$155.66	1,400	$193,368.00

Total Labor-Hour Price $951,383.30

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: To be cited in each individual task order

b. LEVEL OF SAFEGUARDING REQUIRED: To be cited in each individual task order

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER: To be cited in each individual task order	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: FA8771-09-R-0020	DUE DATE *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*
	b. REVISED *(Supersedes all previous specs)*	REVISION NO.	DATE *(YYYYMMDD)*
	c. FINAL *(Complete Item 5 in all cases)*		DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
IBM Corporation 6710 Rockledge Drive Bethesda, MD 20817	8W884	Linda A. Armstrong 11107 Sunset Hills Road Reston, Virginia 20190

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

To be cited in each individual task order for the Application Services contract.

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RESTRICTED DATA			b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		
(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
(2) Non-SCI			g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
f. SPECIAL ACCESS INFORMATION			h. REQUIRE A COMSEC ACCOUNT		
g. NATO INFORMATION			i. HAVE TEMPEST REQUIREMENTS		
h. FOREIGN GOVERNMENT INFORMATION			j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
i. LIMITED DISSEMINATION INFORMATION			k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
j. FOR OFFICIAL USE ONLY INFORMATION			l. OTHER *(Specify)*		
k. OTHER *(Specify)*					

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release _____ Direct _____ Through *(Specify)*

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. I I Yes I I No
Of Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 *if additional space is needed)*

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. I I Yes I I No
(If *Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)*

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*

d. ADDRESS *(include Zip Code)*	17. R EQUIRED DISTRIBUTION a. CONTRACTOR b. SUBCONTRACTOR c COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR d. U.S ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION e ADMINISTRATIVE CONTRACTING OFFICER f OTHERS AS NECESSARY	
a. SIGNATURE		

NETCENTS-2 APPLICATION SERVICES FULL AND OPEN GLOSSARY

ACRONYM/TERM	MEANING
A&AS	Advisory & Assistance Services
ABSS	Automated Business Services System
ADS	Authoritative Data Source
AF	Air Force
AF EA	Air Force Enterprise Architecture
AFCA	Air Force Communications Agency
AFCAP	AF Certification and Accreditation C&A Program
AFECMO	Air Force Enterprise Configuration Management Office
AFFARS	Air Force Federal Acquisition Regulation Supplement
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFMC	Air Force Materiel Command
AFNOC	Air Force Network Operations Center
AFOSH	Air Force Occupational Safety, Fire Prevention, and Health Program
AFPD	Air Force Policy Directive
AFSN	Air Force Systems Networking
AFSO21	Air Force Smart Operations for the 21st Century
AFWAY	(*not an acronym*) the Air Force Web-based ordering system for IT
AMPS	Automated Metadata Population Services
ANSI	American National Standards Institute
AOR	Area of Responsibility
APC	Area Processing Capability
APL	Approved Products List
ASP	Acquisition Strategy Panel
BEQ	Best Estimated Quantity
BPM	Business Process Management
C&A	Certification and Accreditation
C&I	Communications and Information
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Common Access Card
CCB	Configuration Control Board
CCD	Combat Capability Document
CDD	Capability Development Document
CDP	Contract Data Package
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CES	Core Enterprise Services
CFE	Contractor Furnished Equipment
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CITS	Combat Information Transport System
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CLIN	Contract Line Item Number
CM	Configuration Management
CMMI	Capability Maturity Model Integrated
CND	Computer Network Defense
CO	Contracting Officer
COI	Community of Interest
CONUS	Continental (Contiguous) United States
COR	Contracting Officer's Representative
COTS	Commercial Off-The-Shelf

ACRONYM/TERM	MEANING
CPAF	Cost Plus Award Fee
CPAR	Contractor Performance Assessment Report
CPARS	Contractor Performance Assessment Reporting System
CPD	Capability Production Document
CPFF	Cost Plus Fixed Fee
CPIF	Cost Plus Incentive Fee
CPRA	Cost/Price Realism Assessment
CS	Combat Support
CSO	Cognizant Security Office
DAES	Defense Acquisition Executive Summary
DCAA	Defense Contract Audit Agency
DCMA	Defense Contract Management Agency
DDMS	DoD Discovery Metadata Specification
DECC	DoD Enterprise Computing Center
DFAR	Defense Federal Acquisition Regulation
DFARS	Defense Federal Acquisition Regulation Supplement
DIACAP	DoD Information Assurance Certification and Accreditation Process
DII	Defense Information Infrastructure
DII COE	Defense Information Infrastructure Common Operating Environment
DIS	Defense Investigative Service
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DoD IT Standards Registry
DITSCAP	DoD Information Technology Security Certification and Accreditation Process (DoD Instruction 5200.40)
DMS	Defense Message System
DNI	Department of National Intelligence
DO	Delivery Order
DoD	Department of Defense
DoDAF	DoD Architectural Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DoDISS	DoD Index of Specifications and Standards
DOSR	Delivery Order Status Report
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
DREN	Defense Research & Engineering
DRI&R	Deficiency Reporting, Investigation, and Resolution
DRM	Data Reference Model
DS	Distribution System
DSN	Defense Switched Network
DSS	Decision Support System
EC/EDI	Electronic Commerce/Electronic Data Interchange
EIA	Electronic Industries Association
EITDR	Enterprise Information Technology Data Repository
ELS	Enterprise-Level Security
EN	Evaluation Notice
ENSC	Enterprise Network Support Center
EoIP	Everything over Internet Protocol
EPA	Economic Price Adjustment
ERP	Enterprise Resource Planning
ESD	Enterprise Service Desk
ESI	Enterprise Software Initiative

ACRONYM/TERM	MEANING
ESU	Enterprise Service Unit
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
FDR	Final Design Review
FED-LINE	Fedline Payment System
FFP	Firm-Fixed-Price
FIPS	Federal Information Processing Standard
FMR	Financial Management Review
FMS	Foreign Military Sales
FOC	Full Operational Capability
FPAF	Fixed Price Award Fee
FPI	Fixed Price Incentive
FPRA	Forward Pricing Rate Agreement
FTP	File Transfer Protocol
GCSS	Global Combat Support System
GEM	GIG Enterprise Management
GFE	Government Furnished Equipment
GFM/GFP	Government Furnished Material/Property
GIG	Global Information Grid
GIS	Geospatial Information System
GND	GIG Network Defense
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IA	Information Assurance
IAW	In Accordance With
IBR	Integrated Baseline Review
ICD	Initial Capabilities Document
ID/IQ	Indefinite Delivery/Indefinite Quantity
IDECS	Investment Budget Documentation & Execution System
IEEE	Institute of Electrical and Electronics Engineers
IFPP	Instructions for Proposal Preparation
ILS	Integrated Logistics Support
IMPAC	International Merchant Purchase Authorization Card
INCITS	International Committee for Information Technology Standards
INFOCON	Information Operations Condition
I-NOSC	Integrated Network Operations Security Center
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISO	(*not an acronym*) short name for the International Organization for Standardization
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITCC	Information Technology Commodity Council
ITIL	Information Technology Infrastructure Library
ITN	Information Transport Node
ITO	Integrated Task Order
ITO	Instructions to Offerors
i-TRM	Infostructure Technology Reference Model
J&A	Justification and Approval
JDRS	Joint Deficiency Reporting System

ACRONYM/TERM	MEANING
JITC	Joint Interoperability Test Command
JMS	Java Messaging Services
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTF-GNO	Joint Task Force-Global Network Operations
JV2020	Department's Joint Vision 2020
JWICS	Joint Worldwide Intelligence Communications System
KPP	Key Performance Parameters
LAN	Local Area Network
LOI	Letter of Intent
LPTA	Lowest Priced Technically Acceptable
MAJCOM	Major Command
MAN	Metropolitan Area Network
MC	Mission Capability
MCCC	MAJCOM Coordination Center
MDE	Metadata Environment
MDR	Metadata Registry
MILDEP	Military Department
MILSTAR	Military Strategic Tactical Relay
MOCAS	Mechanization of Contract Administration Services
MOSA	Modular Open Systems Architecture
MOSB	Minority-Owned Small Business
MTBCF	Mean Time Between Critical Failure
MTBF	Mean Time Between failure
MTTR	Mean Time to Repair
NAC	National Agency Check
NAFTA	North America Free Trade Agreement
NAICS	North American Industry Classification System
NAS	Network-Attached Storage
NBD	Next Business Day
NBS	National Bureau of Standards
NCC	Network Control Center
NCDS	Netcentric Data Strategy
NCITNTS	Network-Centric Information Technology, Networking, Telephony Security
NCSC	National Computer Security Center
NESI	Net-Centric Enterprise Solutions for Interoperability
NETCENTS	Network-Centric Solutions
NETCENTS-2	Network-Centric Solutions-2
NetOps	Network Operations
NIAP	National Information Assurance Partnership
NIPRNET	Non-Classified Internet Protocol Router Network
NISPOM	National Industrial Security Program Operations Manual
NIST	National Institute for Standards and Technology
NM/ND	Network Management/Network Defense
NOD	Network Operations Division
NOSC	Network Operations Security Center
NSD	Network Security Division
O&M	Operations & Maintenance
OCI	Organizational Conflict of Interest
OCONUS	Outside the Continental (Contiguous) United States
ODBC	Open Database Connectivity
ODC	Other Direct Costs
OEM	Original Equipment Manufacturer

ACRONYM/TERM	MEANING
OLAP	Online Asynchronous Processing
OPPM	Outside the Principal Period of Maintenance
OPSEC	Operations Security
ORCA	Online Representation and Certification Application
OSHA	Occupational Safety & Health Administration
OTD	Open Technology Development
OWL	Web Ontology Language
PCAG	Performance Confidence Assessment Group
PCMCIA	Personal Computer Memory Card International Association
PCO	Procuring Contracting Officer
PDA	Personal Digital Assistant
PDF	Portable Document Format
P-DOCS	Procurement Documents
PDR	Preliminary Design Review
PKE	Public Key PK-enabled
PKI	Public Key Infrastructure
PMD	Program Management Directive
PMO	Program Management Office
PMR	Program Management Review
POC	Point of Contact
POM	Program Office Memoranda
PPBE	Planning, Programming, Budgeting and Execution
PPIRS	Past Performance Information Retrieval System
PPNM	Preliminary Price Negotiation Memoranda
PPT	Performance Price Tradeoff
PRM	Process Reference Model
PWS	Performance Work Statement
QAE	Quality Assurance Evaluator
QAP	Quality Assurance Personnel
QEB	Quarterly Enterprise Buy
QoS	Quality of Service
R&D	Research and Development
RFP	Request for Proposal
RFQ	Request for Quote
RIA	Rich Internet Application
SA	Situational Awareness
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SAR	Selected Acquisition Reports
SATCOM	Satellite Communications
SB	Small Business
SCI	Sensitive Compartmented Information
SDR	System Design Review
SDVOSB	Service-Disabled Veteran-Owned Small Business
SE	Systems Engineering
SEI	Software Engineering Institute
SEP	Systems Engineering Process
SF	Standard Form
SFUG	Security Features User's Guide
SIP	Systems Installation Specification Plan
SIPRNET	Secret Internet Protocol Router Network
SISSU	Security, Interoperability, Supportability, Sustainability, and Usability
SLA	Service Level Agreement

ACRONYM/TERM	MEANING
SM	Service Management
SMART	System Metric and Reporting Tool
SME	Subject Matter Expert
SMI	Singularly-Managed Infrastructure
SMI-ELS	Singularly-Managed Infrastructure and Enterprise-Level Security
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOFA	Status of Forces Agreement
SOO	Statement of Objectives
SOW	Statement of Work
SPCM	Standard Per-Call Maintenance
SPECAT	Special Category
SPR/PER	Spring Program Review/Program Executive Review
SQL	Structured Query Language
SRM	System Reference Model
SS&IP	Site Survey & Integration Plan
SSA	Source Selection Authority
SSAC	Source Selection Advisory Council
SSAN	Social Security Account Number
SSCG	System Security Classification Guide
SSET	Source Selection Evaluation Team
SSL	Secure Sockets Layer
SSP	Source Selection Plan
ST&E	Security Test and Evaluation
STE	Secure Terminal Equipment
STIGs	Security Technical Implementation Guides
STINFO	Scientific and Technical Information
T&M	Time and Material
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDO	Term Determining Official
TEP	Total Evaluated Price
TFM	Trusted Facility Manual
TIM	Technical Interchange Meeting
TIN	Taxpayer Identification Number
TO	Task Order
TRM	Technical Reference Model
TRN	Technical Requirements Notice
TRP	Task Requirements Package
TSL	Transport Security Layer
TSPR	Total System Performance Responsibility
UDDI	Universal Description, Discovery and Integration
UID	Unique Identification
UPS	Uninterruptible Power Supply
USAF	United States Air Force
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network
WBS	Work Breakdown Structure
Wi-Fi	Wireless Fidelity
WOSB	Woman-Owned Small Business

ACRONYM/TERM	MEANING
WS-*	Web Service Standards
WSDL	Web Services Description Language
WWW	World Wide Web
XML	Extensible Markup Language
XSD	XML Schema Definition