AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
J - FFP	1 of 4

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ.NO.	5. PROJECT NO. *(If applicable)*
P00011	22 SEP 2016		

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
AFLCMC/HICK	FA8771		FA8771

DEPARTMENT OF THE AIR FORCE (AFMC)
AFLCMC/HIK
490 EAST MOORE DR., SUITE 270
MAFB - GUNTER ANNEX AL 36114-3000
MANIVANH S. MUNDY 334-416-3089
manivanh.mundy@us.af.mil

DEPARTMENT OF THE AIR FORCE (AFMC)
AFPEO/EIS (ESC/HIK)
490 EAST MOORE DRIVE SUITE 270
MAFB-GUNTER ANNEX AL 36114-3000

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and ZIP Code)*

ACTIONET, INC.
2600 PARK TOWER DR STE 1000
VIENNA VA 22180-7370
(703) 204-0090

CODE 1E7A5 FACILITY CODE

(X)

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

X

10A. MODIFICATION OF CONTRACT/ORDER NO.
FA8771-12-D-1012

10B. DATED *(SEE ITEM 13)*
21 JUN 2012

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

13. THIS ITEM APPLIES ONLY TO MODIFICATION OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(X)	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: ( ) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. ITEM 10A.
X	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation data, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☒ is not, ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

SEE SCHEDULE

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (*Type or print*)		16A. NAME AND TITLE OF SIGNER *(Type or print)*	
		PATRICK J. KENNERSON Contracting Officer	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
_____ *(Signature of person authorized to sign)*		//signed// BY_____ *(Signature of Contracting Officer)*	22 SEP 2016

A. The purpose of this modification is to add Cybersecurity requirements as defined in FAR 4.19 and FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

B. Add FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

C. Incorporate revised PWS, dated August 2016, update paragraph 4.5 Cyber Security and 4.6 Security as follows:

FROM:

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.

TO:

4.5 Cyber Security

The contractor shall ensure that all the requirements meet the DoD Cyber Security Risk Management Framework (RMF) and DoDI 8500.2, Intelligence Community Directive (ICD) 503, or the most current standards and guidance that are applicable. This includes Certification and Accreditation (C&A) activities. The contractor shall provide application services that are in compliance with and support DoD, USAF, or IC Public Key Infrastructure (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) and applicable IC standards.

As specified by the Task Order, the contractor shall provide COTS IA and IA-enabled products IAW AFI 33-200, Cyber Security or other specified guidance. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant, requiring them to be validated by accredited labs under the National Cyber Security Partnership (NCSP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP) or IC standards as applicable.

The contractor shall ensure that all infrastructure deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and Computer Network Defense (CND), which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

FROM:

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.

TO:

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, RMF processes, SISSU processes, Enterprise Information Technology Data Repository (EITDR) certification or ICD 503.

IAW DFARS 239.7103(b), Information Assurance Contractor Training and Certification (JAN 2008):

(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including-
  (1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and
  (2) Appropriate operating systems certification for information assurance technical positions as required by DoD 8570.01-M.

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

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

C. All other terms and conditions remain the same.

DOCUMENT	PGS	DATE	TITLE
ATTACHMENT 1	26	31 AUG 2016	PERFORMANCE WORK STATEMENT (PWS)

NETCENTS-2 SOLUTIONS

Application Services Small Business Companion Performance Work Statement (PWS)

August 2016

NETCENTS-2 Application Services Small Business Companion

1. NETCENTS-2 INTRODUCTION

1.1 Organization

AFLCMC/HIK -- Directorate of Acquisition

1.1.1 Identification

AFLCMC/HICK
ATTN: Patrick Kennerson, 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 Indefinite Delivery Indefinite Quality (IDIQ) 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) Service Oriented Architecture (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 (AF) 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 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 DoD, United States AF 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:

- NetCentric Products – COTS products to support the network.
- Telephony Products and Solutions – COTS products and services to support legacy telephony requirements.
- NetOps and Infrastructure Solutions – Solutions to support network operations, core enterprise services and infrastructure development and operations.
- 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.
- Enterprise Integration and Service Management - Enterprise level integration/portfolio management activities.

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.

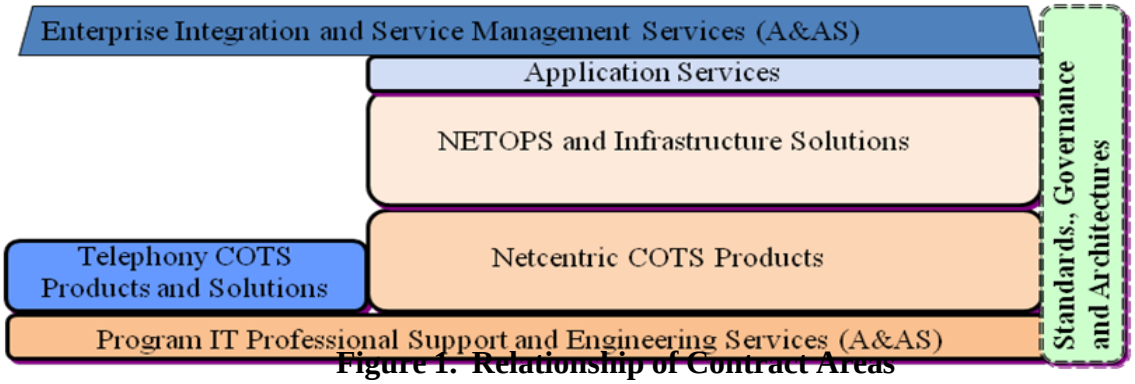

Figure 1. Relationship of Contract Areas

1.5 AF IT Challenge

Currently, the AF 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 NetCentric 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:

- SMI: The SMI 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 Major Command (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.

- ELS: The ELS 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. 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 AF operations will be subject to the oversight of an AF enterprise level governance structure and set of processes. The governance processes will employ systems engineering fundamentals, ensure adherence to the AF EA 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 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 (COI), 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 AF 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 AF 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 AF 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:

- Related to requirements for interoperability with AF capabilities;
- Supports AF IT infrastructure, applications or operations;
- Supports host-tenant arrangements involving AF units; or
- Supports joint operations or solutions.

The AF 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 Cyber Security Risk Management Framework and DoDI 8500.2, Intelligence Community Directive (ICD) 503 as applicable in the task order. The contractor shall provide requirements management and configuration management.

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 tools or approved COTS tools for systems design and development, or incorporation in system solutions, in accordance with AF Manual 33-153, Communications and Information, and AF Policy directive 33-2, Information Assurance (IA) Program and the Air Force 33-200 series publication. 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 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 COI. 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 EA 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, 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 NetCentric 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 AF 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. The Contractor shall ensure that services, solutions and products meet the standards identified in the AF Standard Center of Excellence Repository (SCOER) located at http://netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp

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 NetCentric 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 DoD Architectural Framework (DoDAF) Enterprise Architecture guidance or other frameworks as identified in the task order.

4.5 Cyber Security

The contractor shall ensure that all the requirements meet the DoD Cyber Security Risk Management Framework (RMF) and DoDI 8500.2, Intelligence Community Directive (ICD) 503, or the most current standards and guidance that are applicable. This includes Certification and Accreditation (C&A) activities. The contractor shall provide application services that are in compliance with and support DoD, USAF, or IC Public Key Infrastructure (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) and applicable IC standards.

As specified by the Task Order, the contractor shall provide COTS IA and IA-enabled products IAW AFI 33-200, Cyber Security or other specified guidance. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant, requiring them to be validated by accredited labs under the National Cyber Security Partnership (NCSP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP) or IC standards as applicable.

The contractor shall ensure that all infrastructure deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and Computer Network Defense (CND), which includes the need for source code scanning, the DISA Database STIG, and a Web

Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

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, RMF processes, SISSU processes, Enterprise Information Technology Data Repository (EITDR) certification or ICD 503.

IAW DFARS 239.7103(b), Information Assurance Contractor Training and Certification (JAN 2008):

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

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

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

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

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

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 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 noncommercial 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, and 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 small business companion 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, and 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:

- Provide quality products, incidentals and customer support.
- 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.
- Timely and accurate reports.
- Responsive proposals.
- 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.

In addition, small business companion contract awardees that elect to take advantage of provisions outlined in clause H139 must also comply with the following outcome: 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 Exhibit B, CDRL A002 verifies SB requirements were met	100% of the time

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 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 user id/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 (e.g., conduit, panduit, wire, cable, etc) 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 Contractor Manpower Reporting Application (CMRA) help desk at contractormanpower@hqda.army.mil.

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

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: Contractor Manpower Reporting

In addition, small business companion contract awardees that elect to take advantage of provisions outlined in clauses H139 and H140 shall provide the data identified below. The format for each can be found in Section J, Exhibit B.

CDRL B001: Small Business Graduate Data Submission Instructions
CDRL B002: Small Business Requirements
CDRL B003: 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

The prime contractor shall be appraised at Level 2 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, or comparable documented systems engineering processes, for the entire performance period of the contract, inclusive of options. Formal certifications must be held at the organizational level performing the contract. If not SEI appraised, acceptable comparable Systems Engineering (SE) processes shall be maintained for the entire performance period of the contract, inclusive of options. These processes include: requirements management; configuration management; development of specifications; definition and illustration of architectures and interfaces; design; test and evaluation/verification and validation; deployment and maintenance. The Government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract.

In addition, small business companion contract awardees that elect to take advantage of provisions outlined in clause H139 must comply with the quality processes requirement. This means that at the time of award and as a minimum, the prime contractor shall be appraised CMMI Development 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 and must be held at the prime offeror's organizational level performing the contract for the entire performance period of the contract, inclusive of options. Evidence of comparable Systems Engineering (SE) processes will not be accepted.

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 in the AF Standard Center of Excellence Repository (SCOER) referenced in section 4.1 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	6a. AFI 33-364, Records Disposition – Procedures and Responsibilities, http://www.e-publishing.af.mil/shared/media/epubs/AFI33-364.pdf
6b. AFMAN 33-363, Management of Records, http://www.e-publishing.af.mil/shared/media/epubs/AFMAN33-363.pdf	7. Air Force Metadata Environment Concept https://www.gcss-af.com/noosphere/exec/version?name=USAF+Guidance+Documents&version=13
7a. Air Force Policy Directive 33-3, Information Management, http://www.fas.org/irp/doddir/usaf/afpd33-3.pdf	7b. Air Force Policy Directive 33-4, Enterprise Architecting

7c. Air Force Instruction 33-401, Implementing Air Force Architectures, March 2007	8. American National Standards Institute (ANSI) Documents. http://www.ansi.org/
9. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C	10. CJCSI 6211.02c - DISN Policy and Responsibilities http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf
11. CMMI® for Development (CMMI-DEV), Version 1.2 (August 2006), http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html	12. COI Primer, 30 October 2006
13. Code of Federal Regulations (CFRs). http://www.access.gpo.gov/nara/cfr/	14. Data Interchange Standards Community (E-Business) http://www.disa.org/
14a. Department of Defense Architecture Framework (DoDAF) Version 2.0 Volumes 1,2, and 3, dtd 28 May, 2009	15. DoDI 5200.40 - DoD Information Assurance Certification and Accreditation Process (DIACAP) http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf
16. DoD IPv6 Memorandum, June 9, 2003, and DoD CIO IPv6 Memorandum, 29 September 2003	17. DoD IPv6 Generic Test Plan, Version 3
18. DoD Discovery Metadata Specification (DDMS Version 1.4.1; http://metadata.dod.mil/mdr/irs/DDMS/documents/Document_index.html	19. DoD Net-Centric Data Strategy dated May 9, 2003. http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf
20. DoD 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 06	21. SMI-ELS Strategic Concept Document, 1 September 2009
22. DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 2 https://www.opengroup.org/gesforum/ipv6/uploads/40/14291/DISR_IPv6_Product_Profile_v2.0_final_15Jun07.pdf	23. DOD Guidance 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing" http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf
24. DoDD 8500.1 - Information Assurance (IA) http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf	25. DODI 8500.2, Information Assurance (IA) Implementation, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf
26. DoDI 8510.01, Information Assurance Certification and Accreditation Process (DIACAP), http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf	27. DoD IT Standards Registry (DISR) https://disronline.disa.mil/a/DISR/index.jsp
28. DoD Open Technology Development Guidebook (http://www.acq.osd.mil/jctd/articles/OTDRoadmapFinal.pdf)	29. Engineering for System Assurance, Version 1.0 (October 2008), http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct2008.pdf
30. Federal Desktop Core Configuration (FDCC), http://nvd.nist.gov/fdcc/index.cfm	31. Global Information Grid (GIG) https://www.jtfgno.mil/misc/mission.htm

32. Info-structure Technology Reference Model (i-TRM) https://itrm.hq.af.mil/itrm/Welcome.php	33. Institute of Electrical and Electronics Engineers (IEEE) Standards. Institute of Electrical and Electronics Engineers http://www.ieee.org/
34. ISO/IEC 15288: Systems and Software Engineering—Systems Life Cycle Processes, http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=43564	35. ISO/IEC 12207: Systems and Software Engineering—Software Life Cycle Processes, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43447
36. International Committee for Information Technology Standards http://www.ncits.org/	37. ISO/IEC 26702: Systems Engineering—Application and Management of the SE Process, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43693
38. International Standards Organization (ISO) Documents. http://www.iso.ch/iso/en/ISOOnline.openerpage	39. JTF-GNOP WARNORD 07-37, Public Key Infrastructure Implementation Phase 2
40. Joint Interoperability Test Command (JITC) Requirements http://jitc.fhu.disa.mil/	41. National Institute for Standards and Technology (NIST) (formerly National Bureau of Standards, NBS) Documents. http://www.nist.gov/
42. National Computer Security Center (NCSC) Documents. http://www.radium.ncsc.mil/	43. National Security Agency Guidelines http://www.niap-ccevs.org/
44. National Security Agency Rainbow Series http://www.fas.org/irp/nsa/rainbow.htm	45. Organization for the Advancement of Structured Information (Oasis) Standards http://www.oasis-open.org/home/index.php
46. Netcentric Enterprise Solutions for Interoperability (NESI), http://nesipublic.spawar.navy.mil/	47. Security Technical Implementation Guides (STIGS) http://iase.disa.mil/stigs/index.html
48. The Common Criteria Evaluation and Validation Scheme http://www.niap-ccevs.org/cc-scheme/	49. Singularly Managed Infrastructure – Enterprise Level Services Concept Document, September 2009
50. Systems Engineering Guide for Systems of Systems, Version 1.0 (August 2008), http://www.acq.osd.mil/sse/docs/SE-Guide-for-SoS.pdf	51. USAF Deficiency Reporting, Investigation and Resolution, TO 00-35D-54, http://www.tinker.af.mil/shared/media/document/AFD-070517-037.PDF
52. World Wide Web Consortium (W3C) Glossary http://www.w3.org/TR/ws-gloss/	53. Joint Vision 2020 http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf
54. FAR Subpart 37.6, Performance-Based Acquisition. http://farsite.hill.af.mil/vffara.htm	55. Intelligence Community Directive 503, IT Systems Security, Risk Management, Certification and Accreditation 15 Sep 08, http://www.dni.gov/electronic_reading_room/ICD503.pdf

56. Joint Capabilities Integration and Development System (JCIDS), CJCSI 3170.01G, 1 March 2009, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf	57. Interoperability and Supportability of Information Technology and National Security Systems, CJCSI 6212.01E, 15 December 2008, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf
57. 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	58. 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/463005p.pdf
59. Operation of the Joint Capabilities Integration and Development System, CJCSM 3170.01C, 1 May 2007, http://www.dtic.mil/cjcs_directives/cdata/unlimit/m317001.pdf	60. 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
61. OASD Net-Centric Checklist, Ver. 2.1.3, 12 May 2004, https://acc.dau.mil/CommunityBrowser.aspx?id=22203	62. Net-Centric Operations & Warfare Reference Model, https://acc.dau.mil/CommunityBrowser.aspx?id=28986&lang=en-US
63. Industry Best Practices in Achieving Service Oriented Architecture (SOA), 22 April 2005, http://www.sei.cmu.edu/library/assets/soabest.pdf	64. 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
65. 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	
57. 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	58. 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/463005p.pdf
59. Operation of the Joint Capabilities Integration and Development System, CJCSM 3170.01C, 1 May 2007, http://www.dtic.mil/cjcs_directives/cdata/unlimit/m317001.pdf	60. 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
61. OASD Net-Centric Checklist, Ver. 2.1.3, 12 May 2004, https://acc.dau.mil/CommunityBrowser.aspx?id=22203	62. Net-Centric Operations & Warfare Reference Model, https://acc.dau.mil/CommunityBrowser.aspx?id=28986&lang=en-US

63. Industry Best Practices in Achieving Service Oriented Architecture (SOA), 22 April 2005, http://www.sei.cmu.edu/library/assets/soabest.pdf	64. 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
65. Global Information Grid (GIG) Overarching Policy, DODD 8100.1, 21 November 2003, http://www.acq.osd.mil/ie/bei/pm/ref-	66
library/dodd/d81001p.pdf	

Table 2. Applicable Documents and Standards