SECTION C
STATEMENT OF WORK

C.1   BACKGROUND

The Basic Contract will provide Federal government agencies with integrated Information Technology (IT) solutions for evolving needs on a global basis. Integrated IT solutions are comprised of some or all components described below in Section C.3, and may be tailored to meet agencies' mission needs. Work may be performed at headquarters and/or field offices located throughout the world, as specified in each Order, to provide a variety of IT solutions and support services, including new and emerging technologies that will evolve over the life of the Basic Contract.

C.2   SCOPE

The scope of the Basic Contract includes any and all components of an integrated IT solution, including all current and any new technologies which may emerge during the life cycle of the Basic Contract and information technology systems and services in support of National Security Systems, as defined in FAR 39.002. The Basic Contract provides IT solutions through performance of a broad range of services which may include the integration of various technologies critical to the services being acquired.

As the definition of IT changes over the lifecycle of the Basic Contract, the scope of the Basic Contract will be considered to coincide with the current definition at any given time.

C.2.1   Definition of Information Technology

Per Section C.1, definitions of Information Technology are provided as follows:

C.2.1.1   Clinger-Cohen Act

(a) The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(b) The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(c) Notwithstanding subparagraphs (A) and (B), the term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

C.2.1.2 Federal Acquisition Regulation (FAR)

The FAR defines information technology in section 2.101(b):

"Information technology" means any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(a) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—(i) Its use; or (ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(b) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(c) The term "information technology" does not include any equipment that— (i) Is acquired by a contractor incidental to a contract; or (ii) Contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

C.3   COMPONENTS OF AN IT SOLUTION

The Contractor shall provide Infrastructure and related services, Applications and related services, and IT Management Services to support agencies' integrated IT solution requirements.

In order to provide a common framework for defining and understanding the components of an IT solution, this section will refer to terminology included in the Federal Enterprise Architecture (FEA) and Department of Defense Enterprise Architecture (DoDEA). More detailed information about FEA and DoDEA may be found in Section J, Attachment 5. Usage of this terminology or structure is not required within individual Orders placed on this contract.

The Contractor shall promote IT solutions that support Federal government operational requirements for standardized technology and application service components. This shall facilitate integration requirements for broad Federal IT and E-Gov initiatives, as well as promote the sharing, consolidation, and "re-use" of business processes and systems across the Federal government. The Contractor shall promote the use of open source solutions and open technology development where practicable to enable this re-use.

Within each section below, an overview of the contract solution and service offerings is provided, followed by examples of work to be performed relative to Order requirements. Examples are not meant to be all-inclusive, but rather general indications of the types of products or services within a given category. Other products and services not listed as examples which adhere to the definition for each section are also within scope. For more detailed on information about the particular components of the FEA/DoDEA reference models listed below, see Section J, Attachment 5.

C.3.1 Infrastructure

Infrastructure serves as the foundation and building blocks of an integrated IT solution. It is the hardware which supports Application Services (C.3.2) and IT Management Services (C.3.3); the software and services which enable that hardware to function; and the hardware, software, and services which allow for secure communication and interoperability between all business and application service components.

Infrastructure services facilitate the development and maintenance of critical IT infrastructures required to support Federal government business operations. This section includes the technical framework components that make up integrated IT solutions. One or any combination of these components may be used to deliver IT solutions intended to perform a wide array of functions which allow agencies to deliver services to their customers (or users), whether internal or external, in an efficient and effective manner.

Infrastructure includes hardware, software, licensing, technical support, and warranty services from third party sources, as well as technological refreshment and enhancements for that hardware and software.

This section is aligned with the FEA/DoDEA Technical Reference Model (TRM) which describes these components using a vocabulary that is common throughout the entire Federal government. A detailed review of the TRM is provided in Section J, Attachment 5.

Infrastructure includes complete life cycle support for all hardware, software, and services represented above, including planning, analysis, research and development, design, development, integration and testing, implementation, operations and maintenance, information assurance, and final disposition of these components. The services also include administration and help desk functions necessary to support the IT infrastructure (e.g., desktop support, network administration).

Infrastructure components of an integrated IT solution can be categorized as follows:

C.3.1.1   Service Access and Delivery

These components are responsible for facilitating the end-to-end collection and distribution of data that is either entered or requested by a user. These components include all functions necessary to communicate in a client-server environment. Examples of these components include, but are not limited to, web browsers, Virtual Private Network (VPN), Remote Authentication Dial-In User Service (RADIUS), Peer-to-peer, Section 508 compliance, HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP).

C.3.1.2   Service Platform and Infrastructure

These components include all functions necessary for processing and storing data. These components provide and manage the resources available for Application Services (C.3.2). Examples of these components include, but are not limited to, desktops, laptops, servers, mainframes, routers, switches, printers, Asynchronous Transfer Mode (ATM), T1, Digital Subscriber Line (DSL), Ethernet, Windows/UNIX, Java/.NET; web server/portal; database, data storage, data warehouse; *software development tools*: testing, modeling, versioning, configuration management.

C.3.1.3   Component Framework

These components consist of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. These components define higher level logical functions to provide services in a way that is useful and meaningful to users and other Application Services (C.3.2). Examples of these components include, but are not limited to, digital certificates, biometrics; *business logic*: JavaScript, Visual Basic; *data interchange*: Simple Object Access Protocol (SOAP), Resource Description Framework (RDF); *data management*: Structured Query Language (SQL), Open DataBase Connectivity (ODBC), and OnLine Analytical Processing (OLAP).

C.3.1.4   Service Interface and Integration

These components define the discovery, interaction and communication technologies joining disparate systems and information providers. Application Services (C.3.2) leverage and incorporate these components to provide interoperability and scalability. Examples of these components include, but are not limited to: Messaging-Oriented Middleware (MOM), Object Request Broker (ORB), Enterprise Application Integration (EAI), EXtensible Markup Language (XML), Electronic Data Interchange (EDI), Web Services Description Language (WSDL), Universal Description, Discovery and Integration (UDDI).

C.3.2   Application Services

Application Services provide support for all applications and collaborative service capabilities. These services include support for developing and implementing enterprise and departmental-level applications. These applications may be "cross-cutting" in nature, with inter-related service processing components extending across/beyond the enterprise, or unique to a particular agency/department's mission requirements.

Application Services are aligned with the FEA/DoDEA Service Component Reference Model (SRM). The Contractor shall support all "service domains" outlined in the FEA SRM, to enable the advancement of business and performance objectives. These "service domains" identify the service capabilities required by Federal government agencies to support enterprise/departmental processes and applications.

The Contractor shall promote, to the maximum extent practicable use of commercially available technologies (e.g. Commercial Off-the-Shelf (COTS) and non-developmental items) to support Federal government agencies' IT solution requirements. The Contractor shall provide competencies to employ agencies' enterprise architectures (EAs) as required by individual Orders, to support IT solutions development and implementation and alignment with the FEA.

Application Services include complete life cycle support, including planning, analysis, research and development, design, development, integration and testing, implementation, operations and maintenance, information assurance, and final disposition.

In conjunction with the Application Services supporting each of the Service Domains defined in the FEA/DoDEA SRM, the Contractor shall provide Applications Services for systems required to support unique agency and departmental-level mission requirements, as specified in individual Orders. These services include support for existing and/or new/emerging mission requirements not yet served by the FEA model.

The following represents either components of applications or capabilities which Application Services will support. Each particular area includes, but is not limited to, support for the described functions.

C.3.2.1   Customer Services

Customer Relationship Management (CRM): All aspects of the CRM process, including planning, scheduling, and control activities involved with service delivery. The service components facilitate agencies' requirements for managing and coordinating customer interactions across multiple communication channels and business lines.

Customer Preferences: Customizing customer preferences relative to interface requirements and information delivery mechanisms (e.g., personalization, subscriptions, alerts and notifications).

Customer Initiated Services: Initiating service requests and seeking assistance from government agencies via online communication channels (e.g., online help, tutorials, self-service, reservation/registration, multilingual support, scheduling).

C.3.2.2   Process Automation

Tracking and Workflow: Automated routing, tracking, and management of documents (e.g., process tracking, case management, conflict resolution).

Routing and Scheduling: Automated distribution and scheduling activities (e.g., inbound/outbound correspondence management).

C.3.2.3   Business Management:

Process Management: Development and implementation of standard methodologies and automated process management systems, to facilitate agencies' requirements for managing and monitoring activities surrounding their core business operations (e.g., change management, configuration management, requirements management, program/project management, governance/policy management, quality management, risk management).

Organizational Management: Collaboration and communication activities (e.g., workgroup/groupware, network management).

Investment Management: Selecting, managing, and evaluating agencies' investments and capital asset portfolios (e.g., strategic planning/management, portfolio management, performance management).

Supply Chain Management: All aspects of supply chain management, from the initial sourcing phase through customer delivery (e.g., procurement, sourcing management, inventory management, catalog management, ordering/purchasing, invoice tracking, storefront/shopping cart, warehouse management, returns management, logistics/transportation).

C.3.2.4   Digital Asset Services

Content Management: Content development, maintenance, updates, and distribution (e.g., content authoring, content review/approval, tagging/aggregation, content publishing/delivery, syndication management).

Document Management: Capturing, indexing, and maintaining documents (e.g., document imaging, optical character recognition (OCR), document revisions, library/storage, review/approval, document conversion, indexing/classification).

Knowledge Management: Collecting and processing data from multiple sources and generating information to support business requirements (e.g., information retrieval, information

mapping/taxonomy, information sharing, categorization, knowledge engineering, knowledge capture/distribution/delivery, smart documents).

Records Management: Administration of official government records (record linking/association, record storage/archival, document classification, document retirement, digital rights management).

C.3.2.5   Business Analytical Services

Analysis and Statistics: Applying analysis and statistics to examine/resolve business issues (e.g., mathematical, structural/thermal, radiological, forensics).

Visualization: Transforming data into graphical or image form (e.g., graphing/charting, imagery, multimedia, mapping/geospatial/elevation/global positioning systems (GPS), computer-aided design (CAD)).

Knowledge Discovery: Identifying and extracting information from multiple data source containing files stored in various formats (e.g., data mining, modeling, simulation).

Business Intelligence: Collecting information relevant to historical, existing, or future business needs (e.g., demand forecasting/management, balanced scorecard, decision support planning).

Reporting: Generating reports derived from single or multiple data sources (e.g., ad hoc reporting, standardized/canned reporting, OLAP).

C.3.2.6   Back Office Services

Data Management: Creating, using, processing, and managing data resources (e.g., data exchange, data mart, data warehouse, meta data management, data cleansing, extraction and transformation, data recovery). The data management services include support for agencies' use of the FEA/DoDEA Data Reference Model (DRM). For more information about the FEA/DoDEA DRM, see Section J, Attachment 5.

Human Resources: Recruitment, training, and management of government personnel (e.g., recruiting, career development/retention, time reporting, awards/benefit management, retirement management, education/training, travel management).

Financial Management: Government financing and accounting activities (e.g., billing and accounting, credit/charge, expense management, payroll, payment/settlement, debt collection, revenue management, internal controls, auditing, activity based management, currency translation).

Asset/Material Management: Acquisition and management of Federal government assets (property/asset management, asset cataloging/identification, asset transfer/allocation/maintenance, facilities management, computers/automation management).

Development and Integration: Development and integration of systems across diverse operating platforms (e.g., legacy integration, enterprise application integration, data integration, instrumentation/testing, software development).

Human Capital/Workforce Management Development and Integration: Planning and supervisory operations surrounding government personnel (e.g., resource planning/allocation, skills management, workforce directory/locator, team/organization management, contingent workforce management).

C.3.2.7   Support Services

Security Management: Assuring desired levels of protection for Federal systems, data, and related assets are achieved (e.g., identification/authentication, access control, encryption, intrusion detection, verification, digital signature, user management, role/privilege management, audit trail capture/analysis).

Collaboration: Communications, messaging, information sharing, scheduling and task management activities (e.g., email, threaded discussions, document library, shared calendaring, task management).

Search: Searching, querying, and retrieving data from multiple sources (e.g., precision/recall ranking, classification, pattern matching)

Communications: Voice, data, and video communications in multiple formats and protocols (e.g., real time chat, instant messaging, audio/video conferencing, event/news management, community management support, computer/telephony integration, voice communications).

Systems Management: All aspects of systems management (e.g., software distribution/license management, configuration/installation, remote systems control, enhancements/service updates, system resource monitoring, helpdesk support/issue tracking).

Forms Management: Creating, managing, and processing online forms to support business operations (e.g., forms creation, modification).

C.3.2.8   DoDEA Mission Area Support

The Alliant SB Basic Contract provides support for the DoDEA reference models relating DoD's specialized mission, business, and program areas. Though the DoDEA is an emerging standard, policy and procedures have been formalized for maintaining, evolving, and using the DoDEA reference models.

The DoDEA reference models leverage existing DoD standards and reflect the alignment with the FEA. The Alliant SB Basic Contract includes IT support services for DoD's Global Information Grid (GIG) architecture, Business, Warfighter, Intelligence, and Enterprise

Information Environment (EIE) mission areas. More detailed information about DoDEA may be found in Section J, Attachment 5.

C.3.3 IT Management Services

IT Management Services provide support for operations and IT resource management requirements across the Federal government. These services encompass support for all strategic planning, management, and control functions integral to IT initiatives. The IT Management Services provide the foundational support to effectively align IT requirements with Federal government business operations.

IT Management Services provide support for all government lines of business, functions, and service components that comprise the FEA/DoDEA Performance Reference Model (PRM) and Business Reference Model (BRM). For more information about the PRM and BRM, see Section J, Attachment 5.

IT Management Services shall enable the development and implementation of enhanced governance capabilities, to efficiently and effectively support government agencies' mission requirements and service delivery operations. The services include, but shall not be limited to, support for the following functions:

C.3.3.1 Controls and Oversight

Development and implementation of management controls and systems required by agencies to evaluate, manage, and monitor program performance relative to IT initiatives (e.g., agency, program, and project-level performance plans for IT initiatives; performance measures to support evaluation and reporting requirements for IT initiatives in compliance with FEA/DoDEA PRM standards, etc.).

C.3.3.2 Risk Management and Mitigation

Identification of risk and preparation of risk management plans for IT projects, initiatives, and ongoing operations. Contingency planning to ensure continuity of IT operations and service recovery during emergency events (e.g., risk assessments to determine contingency planning requirements for IT operating environments; develop/maintain contingency, Continuity of Operations (COOP), and disaster recovery plans for IT components, develop/implement emergency preparedness systems).

C.3.3.3 Regulatory Development

Facilitate the development of IT policies, guidelines and standards to facilitate implementation of Federal laws and regulations. The services include support for development, implementation and maintenance of systems to support agencies' IT regulatory development, compliance, and

enforcement activities (e.g., monitoring/ inspection/auditing of IT regulated activities to ensure compliance).

C.3.3.4 Planning and Resource Allocation

Facilitate the planning of IT investments, as well as determine and manage managing overall IT resources to efficiently and effectively support agencies' mission operations. This service area includes, but shall not be limited to support for the following functions:

Budget Formulation/Execution: Facilitate the integration of budgets and plans, at agency and departmental levels, to effectively link IT functions, activities, and resources with mission objectives.

Capital Planning: Facilitate the selection, management, and evaluation of IT investments relative to Federal government agencies' overall capital asset portfolios.

Enterprise Architecture (EA): Development and use of EA work products to manage current and future needs of Federal government business operations (i.e., "baseline" and "target" architectures). The services include transition planning and migration support for all EA components (e.g., business, information, application, and technology architectures), to advance the development and implementation of "core EA capabilities."   The services shall provide support relative to Federal government mandates for measuring and reporting on the completion and usage of EA programs, as well as evaluating results for E-Gov alignment and implementation of Federal lines of business and other cross-governmental initiatives (e.g., SmartBUY, IPv6, HSPD-12).

Strategic Planning: Facilitate the effective alignment of IT requirements/ Information Resource Management (IRM) plans with strategic business plans and program initiatives.

Management Improvements: Development and implementation of improved systems and business practices to optimize productivity and service delivery operations (e.g., analysis, and implementation of improvements in the flow of IT work and program processes and tool utilization, including business system analysis, identification of requirements for streamlining, re-engineering, or re-structuring internal systems/business processes for improvement, determination of IT solution alternatives, benchmarking).

C.3.3.5 IT Security

Development and implementation of management, operational, and technical security controls required by agencies to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

C.3.3.6 System and Network Controls

Facilitate the planning, development, implementation, and management of system and network control mechanisms to support communication and automated needs. Facilitate the planning, organizing, coordinating, and controlling of the arrangement of the elements of protection and monitoring capabilities, and incident recovery actions of the information environment. The process takes configuration orders; status reports; and operational and functional performance requirements as inputs and provides performance capabilities and service and infrastructure controls as outputs.

System and network controls are controlled by environment standards such as policy and operational guidance. The service control requirements enable network controls and operational performance capabilities.

C.3.4 Ancillary **Support**

The Contractor shall provide ancillary **support as necessary to offer** an integrated IT solution. The ancillary **support** described here may only be included in an Order when it is integral to and necessary for the IT effort. Ancillary **support** may include, but is not limited to, such things as: clerical support; data entry; training; subject matter expertise; **server racks, mounts, or similar items;** and construction, alteration, and repair. **A Contractor may propose a new or different skill level category when proposing Ancillary Support consistent with this Section, provided that the Contractor complies with all applicable contract clauses and labor laws, including the Service Contract Act or the Davis Bacon Act, as applicable.**

C.3.4.1 Telecommunications/Wireless

Orders which may include requirements for Telecommunications, Wireless, and Satellite products and services may be fulfilled under the Basic Contract scope, provided the work to be performed is incidental to a larger IT initiative. Contractors are authorized to use government sources of supply in accordance with FAR 51.101, and are encouraged to use GSA's Networx and Satcom II.

(END OF SECTION C)