

C.1 GENERAL/BACKGROUND

Government-wide Acquisition Contracts or GWACs are indefinite delivery/indefinite quantity (IDIQ) contracts for various information technology (IT) resources negotiated, awarded and administered by one particular agency but available to other Federal agencies for purchases. Each GWAC is operated by an executive agent, such as the General Services Administration, designated by the Office of Management and Budget (OMB) pursuant to section 5112(e) of the Clinger-Cohen Act. In accordance with Section 5112(e) of the Information Technology Management Reform Act (ITMRA), 40 U.S.C. § 1412(e), “the Director [of the Office of Management and Budget] may designate one or more heads of Executive agencies as executive agents for Government-wide acquisitions of information technology.” GWACs are not subject to the requirements and limitations of the Economy Act, 31 U.S.C. § 1535.

GWACs are valuable tools for the acquisition of information technology services and supplies, but the Ordering Contracting Officer (OCO) must ensure that: (1) the GWAC is not used to circumvent applicable agency policies or regulations; (2) the ordering agency properly administers all contract terms and conditions and adheres to Federal Acquisition Regulations and policy; (3) agency requirements are within the scope of the master GWAC contract; and (4) subsequent task orders are within the scope of the contract.

C.2 OBJECTIVE

The objective of this solicitation and the resulting VETS GWAC is to provide civilian agencies and the Department of Defense (DoD) the ability to obtain a broad range of Comprehensive IT support services in a timely and cost-effective manner under a multiple award contract. VETS GWAC is a Multiple Award Indefinite Delivery, Indefinite Quantity (MA/IDIQ) contract providing a wide range of information technology support services, while providing the greatest amount of flexibility possible to efficiently and effectively support agency daily operations, protection of infrastructure, the fight against terrorism, and the development and marketing of emerging technologies. The VETS GWAC is accessible to civilian agencies and DoD and is designed to achieve innovative solutions and best value products and services to support Federal Agencies worldwide.

C.3 SCOPE

VETS GWAC is a Multiple Award/Indefinite Delivery Indefinite Quantity (MA/IDIQ) to provide worldwide Information Technology (IT) solutions to client agencies. VETS GWAC is designed to provide the greatest amount of flexibility possible to efficiently and effectively support the federal government's needs in its daily operations, its protection of infrastructure, the fight against terrorism and the development and marketing of emerging technologies. To this end, VETS GWAC was created to fulfill the Information Technology (IT) requirements of GSA and other Federal Agencies. Work may be performed at headquarters and/or field offices located throughout the world, as specified in each task order, to provide a variety of IT support services, including new and emerging technologies which will evolve over the life of VETS GWAC. The scope of work under this contract is defined as within the North American Industrial Classification System (NAICS) codes defined in C.10 of this statement of work. The Government shall order services under this contract by means of task orders with specifically defined scopes, deliverable products, and schedules. *(Amendment 2) VETS order terms include fixed-price(all in FAR 16.2), time-and-materials (per FAR 16.6) and labor-hour (per FAR*

16.6). VETS also allows requiring activities to choose among the incentive features found in FAR 16.4 that are tied to fixed-price, time-and-materials and labor-hour terms.

C.4 TASK ORDERS Amendment 2 (Replaced in its entirety)

The work description is intended to outline the general requirements of contractors awarded VETS GWAC contracts. Specific details of work assignments, deliverables, documentation, training, applicable government/departmental/industry standards, etc., will be provided in individual task orders, preferably performance based. The anticipated services require a diversity of skills suitable to a multitude of information technology environments in support of a variety of IT support areas. The contractor shall perform work under this contract only as directed in task orders issued by authorized COs. The Contractor shall ensure adequate resources are dedicated to satisfy the requirements of work assignments including, but not limited to, furnishing the necessary personnel, material, services, and facilities, as required. In addition, inherent in providing these goods and services, the Contractor shall provide the supervision and management effort necessary for efficient and effective administration and control of work performed under VETS GWAC.

C.5 SECURITY CLEARANCES Amendment 2 (Replaced in its entirety)

Performance of this contract may require access to varying levels of secured information and/or areas. This will be determined on individual task orders. As such, contractor personnel must have a current clearance appropriate to the level of security identified in the task order. See Section H.8 for information on security requirements.

C.6 TRAVEL Amendment 2 (Replaced in its entirety)

Contractor travel may be required for this contract in performance of an individual task order and will be reimbursed to the Contractor in accordance with the Federal Travel Regulations, Joint Travel Regulations, and Joint Federal Travel Regulations.

C.7 HARDWARE, SOFTWARE, AND/OR LICENSING Amendment 2 (Replaced in its entirety)

Integral to the services necessary in performing task orders in the designated functional areas, acquisition of hardware/software and/or licensing of software from 3rd party sources may also be required of the Contractor. Under any of these functional areas, a task order may be used to acquire hardware/software that is integral to the services being provided. Purchase of hardware/software or licenses of software from 3rd party sources in support of task orders in any functional area shall not impact the determination of the appropriate functional area classification of the task order. Functional area classification shall be determined solely upon the preponderance of services provided. The types of hardware/software envisioned would include, but are not limited to, such items as: network devices, switches, routers, bridges, hubs, protocol translators, modems, cabling, wiring closet hardware, wireless access devices, voice and data integration products, Defense Message System (DMS) peripherals, Internet and electronic commerce access gateways, IT infrastructure hardware/software utilities, CASE tools (e.g., Oracle Case, ER-WIN, Predict, System Architect, Knowledgeware, Frontier Super TCP, Netscape, Web Browser), models, database management systems, personal computers, workstations, servers, printers, application software products, compact disk/read only memory (CD-ROM), digital libraries, imaging and

optical character recognition equipment, commercial off-the-shelf (COTS) items, general supplies, etc. Technological refreshment/enhancements of hardware/software as well as special access considerations for IT resources may be required by individual task orders.

C.8 INFORMATION TECHNOLOGY TASK ORDERS INVOLVING SOME CONSTRUCTION WORK Amendment 2 (Replaced in its entirety)

In the event that alteration or minor construction of real property is required to achieve the primary purpose of a Task Order issued against the VETS GWAC contract, such alteration or minor construction shall be deemed within the scope of this contract. The expressed purpose of the VETS GWAC contracts is to provide ordering agencies a wide range of information technology support services using the latest technology and systems. It is not the intent of the VETS GWAC contracts to do “minor construction” unrelated to Information Technology requirements. Minor construction is considered as acceptable work under the VETS GWAC contracts **only** when it is **incidental** to a larger Information Technology task order. In any event, the “minor construction” portion of an Information Technology task order issued against this contract may not exceed any statutory, regulatory, or policy limitations imposed by the Ordering Agency applicable to construction. For example, if the Ordering Agency regulates and/or imposes thresholds for the use of O&M dollars for “minor construction” imbedded in Task Orders for other than construction, those same limitations will apply to task orders issued against the VETS GWAC contracts. The Davis-Bacon Act requirements apply to construction work to be performed as part of Information Technology task orders under this contract if-

- (1) The construction work is to be performed on a public building or public work;
- (2) The contract contains specific requirements for a substantial amount of construction work exceeding the monetary threshold for application of the Davis-Bacon Act (the word "substantial" relates to the type and quantity of construction work to be performed and not merely to the total value of construction work as compared to the total value of the contract); and
- (3) The construction work is physically or functionally separate from, and is capable of being performed on a segregated basis from, the other work required by the contract.

C.9 ORDERING AGENCY STANDARDS

Each ordering agency/organizational component will specify the standards, which the Contractor shall follow in performance of a prospective task order. The Contractor shall be required to work according to the architectures, standards, guidelines, and procedures as stated in individual task orders, including, but not limited to, various standards as set forth in agency guidance.

C.10 NORTH AMERICAN INDUSTRIAL CLASSIFICATION SYSTEM (NAICS) CODES

The following NAICS codes are applicable to the VETS GWAC.

541512 Computer Systems Design Services

541511 Custom Computer Programming Services

541513 Computer Facilities Management Services

541519 Other Computer Related Services

518210 Data Processing, Hosting, and Related Services

611420 Computer Training

All the above mentioned codes are applicable to both Functional Areas of the VETS GWAC. This procurement is set-aside for small businesses. For the purposes of the VETS GWAC contract the primary NAICS Code is designated as 541512. The size standard for NAICS Code 541512 is \$21.0 million.

C.11 IT SUPPORT FUNCTIONAL AREAS

Separate and distinct contracts will be awarded in two (2) Functional Areas which will cover the full range of IT solutions. The Functional Areas, and examples of the types of tasks included, are listed below. Many types of tasks will overlap both Functional Areas and may be competed across both Functional Areas. Additional IT efforts, as required, can be obtained under this Statement of Work as long as the requirement fits within the scope of the designated NAICS Codes in C.9 and the Functional Areas specified herein.

C.11.1 FUNCTIONAL AREA ONE (1) – SYSTEMS OPERATIONS AND MAINTENANCE

- (1) Chief Knowledge Officer (CKO) Support
 - i) Informatics
 - ii) Knowledge Management
- (2) Configuration Management and Licensing
- (3) Database Design and Administration and Data Storage Management
 - i) Database Design
- (4) E-Business Planning and Support
- (5) Electronic Commerce (EC) and Electronic Data Interchange Support
- (6) Emerging Technologies
 - i) IT Research and Development
 - ii) Nanotechnology
- (7) Independent Verification and Validation
- (8) Information Architecture Analysis and Web Object Indexing
- (9) Information Management Life Cycle Planning/Support
 - i) Information Management Support
- (10) Integration Support
- (11) Internet System Architecture and Webmaster Support
 - i) Website Development and Support
- (12) Mainframe/Data Processing System Support
- (13) Media/Training Center/Video Teleconferencing Support
- (14) Network Support (including Interdepartmental Data Network (IDN), Local Area Networks (LAN), Wide Area Networks (WAN), Internet access, etc.)
 - i) Connectivity and IT infrastructure Support (including Data Networks, Interdepartmental Data Network (IDN), Local Area Networks (LAN), Wide Area Networks (WAN), Storage Area Networks (SAN))
- (15) Office Automation Support/Help Desk Support
- (16) Performance Measures and Metrics Planning
- (17) Seat Management
 - i) Systems Operations
- (18) Section 508 Compliance Assistance
- (19) Supply Chain Management (Logistics)
- (20) Systems Management Support

- i) Information Systems Support
- (21) Technical Support
 - i) Computer Center Technical Support
- (22) Telemedicine
- (23) Test and Evaluation Support
- (24) Training, Training Development, and Training Center Support (including Computer Based Training)
 - i) Distance Learning
 - ii) Training Requirements Analysis and Planning
- (25) Virtual Data Center
 - i) Data Warehousing
- (26) Anti-Virus Management Service
 - i) Intrusion Detection and Prevention Service
 - ii) Virus Detection, Elimination, and Prevention
- (27) Biometrics
 - i) Smart Card Technologies
- (28) Computer Security Awareness, and Training
 - i) Computer Security Incident Response
 - ii) Computer Security Planning
 - iii) Security Policy Compliance
- (29) Disaster Recovery, Continuity of Operations, and Contingency Planning
 - i) Critical Infrastructure Protection
 - ii) Hot-site and Cold-site Support Services
 - iii) Incident Response Service
 - iv) System Recovery Support Services
- (30) Hardware and Software Maintenance and /or Licensing
 - i) Software/Hardware Maintenance and /or Licensing
- (31) Independent Verification and Validation (Security)
 - i) Certification of Sensitive Systems
 - ii) Mainframe Automated Information Security Support
 - iii) Security for Small Systems, Telecommunications, and Client Service
- (32) Managed E-Authentication Service
- (33) Managed Firewall Service
- (34) Privacy Data Protection
- (35) Public Key Infrastructure (PKI)
 - i) Crypto Systems
 - ii) Digital Signature Technology
- (36) Secure Managed Email Service (SMEMS)
- (37) Security Certification and Accreditation
- (38) Systems Vulnerability Analysis/Assessment and Risk Assessment
 - i) Quantitative Risk Analysis of Large Sensitive Systems
 - ii) Vulnerability Scanning Service

C.11.2 FUNCTIONAL AREA TWO (2) – INFORMATION SYSTEMS ENGINEERING

- (1) System and Software Design, Development, Engineering, and Integration
 - i) Software Development
 - ii) System Design Alternative Studies
 - iii) Software Distribution, Licensing, Maintenance
- (2) Information Technology (IT) Strategic Planning, Program Assessment, and Studies

- i) Feasibility Studies
- ii) Information Technology (IT) Strategic Planning and Mission Need Analysis
- iii) Information Technology Organizational Development
- iv) Information Technology Program Analysis, Assessments and Studies
- v) Information Technology Research and Development
- (3) Automated Workflow System Development and Integration
- (4) Business Process Reengineering (BPR)
 - i) Benchmarking/Operational Capability Demonstrations
 - ii) Change Management
- (5) Chief Information Officer (CIO) Support
 - i) Enterprise Resource Systems Management
 - ii) Enterprise Resource Systems Planning
 - iii) Information Assurance Activities
 - iv) Information Operations
 - v) Inter/Intra-Agency Enterprise Resource Planning
- (6) Global Information Systems
- (7) Software Life Cycle Management (SLCM)
 - i) Cost Benefit Analysis, Cost Effectiveness Analysis
 - ii) Risk Analysis and Assessment
 - iii) Stakeholder Analysis
 - iv) Total Cost of Ownership Studies
- (8) Software Engineering (SWE)
 - i) Software Quality Assurance
- (9) Customer Relationship Management
- (10) Information Technology Architecture (ITA) Support
- (11) Infrastructure Quality Assurance
- (12) Instructional Design, and Modeling & Simulation
- (13) SCE/CMM/CMMI Analyses and Implementation Support
- (14) Anti-Virus Management Service
 - i) Intrusion Detection and Prevention Service
 - ii) Virus Detection, Elimination, and Prevention
- (15) Biometrics
 - i) Smart Card Technologies
- (16) Computer Security Awareness, and Training
 - i) Computer Security Incident Response
 - ii) Computer Security Planning
 - iii) Security Policy Compliance
- (17) Disaster Recovery, Continuity of Operations, and Contingency Planning
 - i) Critical Infrastructure Protection
 - ii) Hot-site and Cold-site Support Services
 - iii) Incident Response Service
 - iv) System Recovery Support Services
- (18) Hardware and Software Maintenance and /or Licensing
 - i) Software/Hardware Maintenance and /or Licensing
- (19) Independent Verification and Validation (Security)
 - i) Certification of Sensitive Systems
 - ii) Mainframe Automated Information Security Support
 - iii) Security for Small Systems, Telecommunications, and Client Service

- (20) Managed E-Authentication Service
- (21) Managed Firewall Service
- (22) Privacy Data Protection
- (23) Public Key Infrastructure (PKI)
 - i) Crypto Systems
 - ii) Digital Signature Technology
- (24) Secure Managed Email Service (SMEES)
- (25) Security Certification and Accreditation
- (26) Systems Vulnerability Analysis/Assessment and Risk Assessment
 - (i) Quantitative Risk Analysis of Large Sensitive Systems
 - (ii) Vulnerability Scanning Service

C.12 INTEGRATED SOLUTIONS AND DESCRIPTIONS

The Government requires assistance with integrated solutions and services. This section addresses all things integrated at all organizational levels as well as describing the functional requirements and provides information that the Contractor may need to know in order to perform the tasks.

C.12.1 FUNCTIONAL AREA ONE (1)

C.12.1.1 Chief Knowledge Officer (CKO) Support

The Chief Knowledge Officer is responsible for knowledge management within an organization. They are senior corporate executives with "knowledge" in their titles. In other words, we could assume that they had been appointed specifically to orchestrate a knowledge management program. They are all first incumbents in the role, most having been in office less than two years with their collective experiences.

C.12.1.1.1 Informatics

The study of information and the ways to handle it, especially by means of information technology (e.g. computers and other electronic devices). The study of the application of computer and statistical techniques to the management of information.

C.12.1.1.2 Knowledge Management

The use of computer technology to organize, manage, and distribute electronically all types of information, customized to meet the needs of a wide variety of users. The information is stored in a special database called a knowledge base and is used to enhance organizational performance. Capturing, organizing, and storing knowledge and experiences of individual workers and groups within an organization and making it available to others in the organization.

C.12.1.2 Configuration Management and Licensing

C.12.1.3 Database Design and Administration and Data Storage Management (C.11.1(3))

Database Design - The function of composing records, each containing fields together with a set of operations for searching sorting, recombining, and other functions. This includes determination of content, internal structure, and access strategy for a database, as well as defining security and integrity, and monitoring performance. A database is considered to be a collection of information organized in such a way that a computer program can quickly select desired pieces of data.

C.12.1.4 E-Business Planning and Support

C.12.1.5 Electronic Commerce (EC) and Electronic Data Interchange Support

(C.11.1(5))

The Contractor shall provide resources to support, define, develop, and maintain electronic inter-organizational business networks. EC functions include, but are not limited to electronic exchange of requests for quotations, quotes, purchase orders, notices of award, electronic payments, document interchange, supporting databases, and other activities associated with the procurement and payment process. Guidance on the use of EC in the procurement process can be found in the Federal Acquisition Regulation.

C.12.1.6 Emerging Technologies

C.12.1.6.1 IT Research and Development

C.12.1.6.2 Nanotechnology

A field of science whose goal is to control individual atoms and molecules to create computer chips and other devices that is thousands of times smaller than current technologies permit.

C.12.1.7 Independent Verification and Validation

The Contractor shall provide technical resources to define, develop, and conduct Independent Validation and Verification (IV&V) Tests to assess: 1) the capacity of BPR to improve system services and capabilities; 2) Software Life Cycle Management (SLCM) functions; 3) the support provided for electronic commerce; and 4) other IV&V as required or identified in TO. Validation tests shall be designed to ensure that the software developed fully addresses the requirements established to provide specific system operation functions and capabilities. Verification testing shall be designed to determine whether the software code is logically correct for the operation functions for which it was designed. It is expected that the operational areas listed above will be contracted as separate IV&V tasks.

C.12.1.8 Information Architecture Analysis and Web Object Indexing

Analysis of the hardware and/or software, or a combination of hardware and software, of a system. The architecture of a system always defines its broad outlines, and may define precise mechanisms as well. Web Object Indexing is a website intended to enable a user to obtain other resources on the web. The web index may contain a search facility or may merely contain individual hyperlinks to the resources indexed.

C.12.1.9 Information Management Life Cycle Planning/Support

C.12.1.9.1 Information Management Support

C.12.1.10 Integration Support

Assistance in assembling diverse hardware and/or software components together to work as a system.

C.12.1.11 Internet System Architecture and Webmaster Support

C.12.1.12 Mainframe/Data Processing System Support

C.12.1.13 Media/Training Center/Video Teleconferencing Support

The Contractor shall provide planning, analysis, troubleshooting, integration, acquisition, installation, operations, maintenance, training, documentation, and administration services for multi-media and education centers. The Contractor shall also maintain a centralized technical assistance service that supports problem resolution and distributes general multi-media and learning information.

C.12.1.14 Network Support (including Interdepartmental Data Network (IDN), Local Area Networks (LAN), Wide Area Networks (WAN), Internet access, etc.)

The Contractor shall provide planning, analysis, troubleshooting, integration, acquisition, installation, operations, maintenance, training, documentation, and administration

services for all types of data networks, including, but not limited to, enterprise systems, the Interdepartmental Data Network (IDN) “backbone”, Local Area Networks (LAN), Wide Area Networks (WAN), client-server, Internet access, and videoconferencing. The Contractor shall also maintain a centralized technical assistance service that supports problem resolution and distributes general network information.

C.12.1.14.1 Connectivity and IT infrastructure Support (including Data Networks, Interdepartmental Data Network (IDN), Local Area Networks (LAN), Wide Area Networks (WAN), Storage Area Networks (SAN)

C.12.1.15 Office Automation Support/Help Desk Support

C.12.1.16 Performance Measures and Metrics Planning

C.12.1.17 Seat Management

The Contractor shall provide desktop computing as a service and the Government will purchase these services as a utility and will pay for them by the “seat.” The services include the entire suite of hardware, COTS software, connectivity, and support services required to deliver the support to the desktop.

C.12.1.18 Section 508 Compliance Assistance

Unless specifically exempted, all task orders issued under this contract shall comply with Section 508 of the Rehabilitation Act Amendments of 1998 to ensure IT accessibility to disabled persons. For information see the web site at

www.section508.gov

C.12.1.19 Supply Chain Management (Logistics)

The design and management of seamless, value-added processes across organizational boundaries to meet the real needs of the end customer. The development and integration of people and technological resources are critical to successful supply chain integration.

C.12.1.20 Systems Management Support

C.12.1.20.1 Information Systems Support

C.12.1.21 Technical Support

Computer Center Technical Support - The Contractor shall provide planning, analysis, troubleshooting, integration, acquisition, installation, operations, maintenance, training, documentation, and administration services for computer centers. The Contractor shall also maintain a centralized technical assistance service that supports problem resolution and distributes general computer center information.

C.12.1.22 Telemedicine

C.12.1.23 Test and Evaluation Support

C.12.1.24 Training, Training Development, and Training Center Support (including Computer Based Training)

C.12.24.1 Distance Learning

C.12.24.2 Training Requirements Analysis and Planning

C.12.1.25 Virtual Data Center

VDC provides a complete open-source, digital library system for the management, dissemination, exchange, and citation of virtual collections of quantitative data. The VDC functionality provides everything necessary to maintain and disseminate an individual collection of research studies: including facilities for the storage, archiving, cataloging, translation, and dissemination of each collection. On-line analysis is provided, powered by the R Statistical environment. The system provides extensive support for distributed and federated collections including: location-independent naming of objects, distributed authentication and access control, federated metadata harvesting, remote repository

caching, and distributed "virtual" collections of remote objects.

Data Warehousing - The Contractor shall coordinate the collection of data designed to support management decision-making. Data warehouses contain a wide variety of data that present a coherent picture of business conditions at a single point in time.

Development of a data warehouse includes development of systems to extract data from operating systems plus installation of a warehouse database system that provides managers flexible access to the data. The term data warehousing generally refers to the combination of many different databases across an entire enterprise.

C.12.1.26 Anti-Virus Management Service (AVMS)

Anti-Virus Management Service enables the detection and removal of system viruses. The service scans executable files, boot blocks and incoming traffic for malicious code. Anti-virus applications are constantly active in attempting to detect patterns, activities, and behaviors that may signal the presence of viruses. AVMS enables Agencies to procure anti-virus capabilities that protect their infrastructure.

C.12.1.26.1 Intrusion Detection and Prevention Service (IDPS)

Agency enterprise networks, like their commercial counterparts, continue to be challenged with increasing security risks. Intrusion Detection and Prevention Service (IDPS) will serve as a component of the Agency's security infrastructure by providing an extra layer of protection for its internal networks. IDPS is a security offering that helps reduce network service disruptions caused by malicious attacks.

C.12.1.26.2 Virus Detection, Elimination, and Prevention

The Contractor shall provide virus detection, elimination, and prevention support.

C.12.1.27 Biometrics

The Contractor shall provide biometrics services including the reading of the measurable, biological characteristics of an individual in order to identify them to a computer or other electronic system. Biological characteristics normally measured include fingerprints, voice patterns, retinal and iris scans, faces, and even the chemical composition of an individual's perspiration. For the effective "two-factor" security authorization of an individual to a computer system, normally a biometric measure is used in conjunction with a token (such as a smartcard) or an item of knowledge (such as a password). Biometrics might include fingerprints, retina pattern, iris, hand geometry, vein patterns, voice password, or signature dynamics. Biometrics can be used with a smart card to authenticate the user. The user's biometric information is stored on a smart card, the card is placed in a reader, and a biometric scanner reads the information to match it against that on the card. This is a fast, accurate, and highly secure form of user authentication.

C.12.1.27.1 Smart Card Technologies

C.12.1.28 Computer Security Awareness and Training

The Contractor shall provide computer security awareness and training.

C.12.1.28.1 Computer Security Incident Response

C.12.1.28.2 Computer Security Planning

C.12.1.28.3 Security Policy Compliance

C.12.1.29 Disaster Recovery, Continuity of Operations, and Contingency Planning

The Contractor shall provide disaster recovery, continuity of operations, and contingency planning support, including those for software applications, which are processed on various computer platforms (e.g., personal computers, mainframes, and mini-computers).

C.12.1.29.1 Hot-site and Cold-site Support Services

Contractor will provide disaster recovery sites, computer systems, network resources and technical professional services to support disaster recovery test exercises and disaster recoveries within twelve (12) hours of a disaster declaration, or when Government personnel occupy the contractor's recovery facility, whichever is sooner.

Contractor personnel assigned to support the customer's recovery exercises and recovery events shall be U.S. citizens and shall be subjected to background investigations to determine suitability for employment, and receive computer security awareness training in accordance with the Computer Security Act of 1987.

C.12.1.29.2 Critical Infrastructure Protection

C.12.1.29.3 Incident Response Service (INRS)

In an effort to combat cyber attacks and crime, Agencies intend to implement Incident Response Service (INRS) as part of their security portfolio. This offering is one of the security tools that will help in responding to potential malicious attacks that can lead to service disruptions. INRS allows Agencies to complement their in-house security expertise, or obtain outside assistance with a greater depth and breadth of experience.

INRS is comprised of both proactive and reactive activities. Proactive services are designed to prevent incidents. They include onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training. Reactive services involve telephone and on-site support for responding to malicious events such as Denial of Services (DoS) attacks; virus, worm, and trojan horse infections; illegal inside activities, espionage, and compromise of sensitive internal agency databases. INRS provides an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks. In addition, INRS provides forensics services that can assist in apprehending and prosecuting offenders.

C.12.1.29.4 System Recovery Support Services

The Contractor shall provide personnel resources to ensure a system recovery capability that will support Government goals and objectives. As a minimum, the Contractor must provide the capability for hot-site/cold-site recovery of all critical software programs and sensitive Government information. The requirements for system recovery support services will be based on the analysis of strategic planning factors; the strengths and weaknesses of the system, as obtained through threat assessment and risk analyses; and cost and benefit trade-offs.

System recovery support services include, but are not limited to the capability to:

C.12.1.30 Hardware and Software Maintenance and/or Licensing

The Contractor shall provide for software/hardware maintenance and/or software licenses from 3rd party vendors in support of tasks falling within this functional area.

C.12.1.31 Independent Verification and Validation (Security)

The Contractor shall provide technical resources to define, develop, and conduct Independent Validation and Verification (IV&V) Tests for Mainframe Automation Information Security; Certification of Sensitive Systems; and Security for Small Systems, Telecommunications, and Client Server. Validation testing shall be designed to ensure that the software developed fully addresses the requirements established to provide specific operation functions. Verification testing shall be designed to determine

whether the software code is logically correct for the operation functions for which it was designed. It is expected that the operational areas listed above will be contracted as separate IV&V tasks.

C.12.1.31.1 Certification of Sensitive Systems

The Contractor shall provide support in the certification of sensitive systems.

C.12.1.31.2 Mainframe Automated Information Security Support

The Contractor shall provide operational and analytical support related to security for mainframe information assets.

C.12.1.31.3 Security for Small Systems, Telecommunications, and Client Service

The Contractor shall provide security for small systems, telecommunications, and client server support.

C.12.1.32 Managed E-Authentication Service (MEAS)

Managed E-Authentication Service (MEAS) provides Agencies with electronic authentication services in order to seamlessly conduct electronic transactions and implement E-Government initiatives via the Internet. The service enables an individual person to remotely authenticate his or her identity to an Agency Information Technology (IT) system. The service shall connect to Agency networking environments including, but not limited to Agency Demilitarized Zones (DMZs) and secure LANs. Managed EAuthentication

Service consists of hardware and software components that provide for remote authentication of individual people over a network for the purpose of electronic government and commerce. The service provides for the electronic validation and verification of a user's identity and enables the use of electronic signatures over the Internet and other public networks.

C.12.1.33 Managed Firewall Service

Agencies intend to implement Managed Firewall Service in order to secure their internal networks. Similarly to commercial enterprises, Agencies face increasing network security risks, which they seek to mitigate. This offering is one of the security tools that will help reduce service disruptions caused by malicious access. Managed Firewall Service will prevent unauthorized access to or from private networks, such as Local Area Networks (LANs).

C.12.1.34 Privacy Data Protection

C.12.1.35 Public Key Infrastructure (PKI)

A type of electronic signature that is generally considered the most reliable and secure. Digital signatures use public key infrastructure (PKI) to authenticate the sender and verify the information contained in the document. With the passage of the electronic signatures act, digital signatures are expected to become increasingly popular for exchanging information, conducting transactions and signing contracts over the Internet. The Contractor shall provide a set of policies, processes, server platforms, software, and workstations used to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. The PKI consists of systems which collaborate to provide and implement the PCS and possibly other related services. The term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of digital certificates, certification authorities, and other

registration authorities that verify and authenticate the validity of each party involved in an electronic transaction.

C.12.1.36 Secure Managed Email Service (SMEMS)

Secure Managed Email Service (SMEMS) provides Agencies with a complete secure and fully managed email security solution. Email security solutions implemented at Agency gateways and desktops usually attempt to handle events that have already breached the network. Any delay in applying security updates to this infrastructure exposes the network to rapid outbreaks and dynamic threats. SMEMS offers an additional layer of protection by proactively scanning and monitoring email traffic at the contractor's security platform, before it enters the Agency's network. The service supports email security functions such as Anti-Virus Scanning, Anti-Spam Filtering, and Content Control. Security engines are continuously updated to maintain effectiveness against threats and inappropriate material. SMEMS works in conjunction with existing Agency email systems, and is implemented without additional investment in hardware and software at Agency sites.

C.12.1.37 Security Certification and Accreditation

C.12.1.38 Systems Vulnerability Analysis/Assessment and Risk Assessment

C.12.1.38.1 Quantitative Risk Analysis of Large Sensitive Systems

The Contractor shall provide support in performing quantitative risk analyses of large sensitive systems, generally including the risk analysis package as an attachment to the system security plan.

C.12.1.38.2 Vulnerability Scanning Service (VSS)

Vulnerability Scanning Service (VSS) allows agencies to conduct effective and proactive assessments of critical networking environments, and correct vulnerabilities before they are exploited. This offering helps to guard Agency systems and network infrastructure against emerging threats.

C.12.2 FUNCTIONAL AREA TWO (2)

C.12.2.1 System and Software Design, Development, and Integration

C.12.2.1.1 Software Development

A set of activities that results in software products. Software development may include new development, modification, reuse, re-engineering, maintenance, or any other activities that result in software products. Providing for project management, planning, design, building and implementation of client specific applications, taking responsibility for achieving contractually specified results.

C.12.2.1.2 System Design Alternative Studies

C.12.2.1.3 Software Distribution, Licensing, Maintenance

The Contractor shall provide for software maintenance and/or software licenses from 3rd party vendors in support of tasks falling within this functional area

C.12.2.2 Information Technology (IT) Strategic Planning, Program Assessment, and Studies

The Contractor shall provide resources to support in the development, analysis, and implementation of IT strategies, architectures, program planning and assessment, and risk, trade-off, requirements, alternatives, and feasibility studies that advance the goals and objectives of the Government.

C.12.2.2.1 Feasibility Studies

The Contractor shall provide resources to facilitate evaluation of a prospective project for the purpose of determining if the project should be undertaken.

Feasibility studies normally consider the time, budget, and technology required for completion.

C.12.2.2.2 Information Technology (IT) Strategic Planning and Mission Need Analysis

C.12.2.2.3 Information Technology Organizational Development

C.12.2.2.4 Information Technology Program Analysis, Assessments and Studies

C.12.2.2.5 Information Technology Research and Development

The Contractor shall provide the resources to identify and research emerging technologies in the IT area. Based on this research, the Contractor shall develop and evaluate prototype solutions and present findings and recommendations to the Government for their consideration.

C.12.2.3 Automated Workflow System Development and Integration

The defined series of tasks within an organization to produce a final outcome. Sophisticated workgroup computing applications allow you to define different workflows for different types of jobs. The workflow software ensures that the individuals responsible for the next task are notified and receive the data they need to execute their stage of the process.

C.12.2.4 Business Process Reengineering

The Contractor shall provide resources to support in the development, analysis, and implementation of improvements in the flow of business, work, and program processes and tool utilization.

C.12.2.4.1 Benchmarking/Operational Capability Demonstrations

C.12.2.4.2 Change Management

C.12.2.5 Chief Information Officer (CIO) Support

Typically, a CIO is involved with analyzing and reworking existing business processes, with identifying and developing the capability to use new tools, with reshaping the enterprise's physical infrastructure and network access, and with identifying and exploiting the enterprise's knowledge resources. Many CIOs head the enterprise's efforts to integrate the Internet and the World Wide Web into both its long-term strategy and its immediate business plans.

C.12.2.5.1 Enterprise Resource Planning Systems Development and Integration

An approach to organizational integration management that relies on integrated application software to provide data on all aspects of the enterprise, such as finance, inventory, human resources, sales, etcetera. The objective of an Enterprise Resource Planning Systems is to provide data, when as needed, to enable an entity to monitor and control its overall operation.

C.12.2.5.2 Enterprise Resource Systems Management

C.12.2.5.3 Enterprise Resource Systems Planning

C.12.2.5.4 Information Assurance Activities

C.12.2.5.5 Information Operations

C.12.2.5.6 Inter/Intra-Agency Enterprise Resource Planning

C.12.2.6 Global Information Systems

C.12.2.7 Software Life Cycle Management (SLCM)

The Contractor shall provide resources to support any or all phases and stages of SLCM, including planning, analysis, troubleshooting, integration, acquisition, installation, operation, maintenance, training, documentation, and administration. The Contractor

may be responsible for obtaining and/or supporting the necessary software, hardware, firmware, resources, etc. required for a system project.

C.12.2.7.1 Cost Benefit Analysis, Cost Effectiveness Analysis

C.12.2.7.2 Risk Analysis and Assessment

C.12.2.7.3 Stakeholder Analysis

C.12.2.7.4 Total Cost of Ownership Studies

C.12.2.8 Software Engineering

The Contractor shall provide software engineering support (including planning, analysis, design, evaluation, testing, quality assurance, and project management) in the application of computer equipment through computer programs, procedures, tools, and associated documentation.

C.12.2.8.1 Software Quality Assurance

C.12.2.9 Customer Relationship Management

CRM entails all aspects of interaction a company has with its customer, whether it is sales or service related.

C.12.2.10 Information Technology Architecture (ITA) Support

C.12.2.11 Infrastructure Quality Assurance

C.12.2.12 Instructional Design, and Modeling & Simulation

The Contractor shall provide instructional design, and modeling & simulation. Instructional Design is the systematic development of instructional specifications using learning and instructional theory to ensure the quality of instruction. It is the entire process of analysis of learning needs and goals and the development of a delivery system to meet those needs. It includes development of instructional materials and activities; and tryout and evaluation of all instruction and learner activities. Instructional Design is that branch of knowledge concerned with research and theory about instructional strategies and the process for developing and implementing those strategies. Instructional Design is the science of creating detailed specifications for the development, implementation, evaluation, and maintenance of situations that facilitate the learning of both large and small units of subject matter at all levels of complexity. Instructional Design can start at any point in the design process. Often a glimmer of an idea is developed to give the core of an instruction situation. By the time the entire process is done the designer looks back and she or he checks to see that all parts of the "science" have been taken into account. Then the entire process is written up as if it occurred in a systematic fashion.

C.12.2.13 SCE/CMM/CMMI Analyses and Implementation Support

SOFTWARE CAPABILITY EVALUATION (SCE) -- It may be necessary on certain task orders to perform software capability evaluations (SCE). The Government may use the SCE (see 1.5.1 and 1.5.2) developed by the Software Engineering Institute (SEI) Carnegie Mellon University (CMU) www.sei.cmu.edu , Pittsburgh, PA, 15213, in evaluating the contractor's/subcontractor's task order proposal. The SCE level required will be specified in individual task orders.

CAPABILITY MATURITY MODEL (CMM) -- The Capability Maturity Model for Software (or SW-CMM) is used for judging the maturity of the software processes of an organization and for identifying the key practices that are required to increase the maturity of these processes.

CAPABILITY MATURITY MODEL INTEGRATION (CMMI) -- The Capability Maturity Model Integration (CMMI) provides models for achieving product and process improvement. The output of the CMMI project is a suite of products, which provides an integrated

approach across the enterprise for improving processes, while reducing the redundancy, complexity and cost resulting from the use of separate and multiple capability maturity models (CMMs). To improve the efficiency of model use and increase the return on investment, the CMMI project was created to provide a single integrated set of models.

C.12.2.14 Anti-Virus Management Service (AVMS)

Reference Section C.12.1.26 for description.

C.12.2.15 Biometrics

Reference Section C.12.1.27 for description.

C.12.2.16 Computer Security Awareness and Training

Reference Section C.12.1.28 for description.

C.12.2.17 Disaster Recovery, Continuity of Operations, and Contingency Planning

Reference Section C.12.1.29 for description.

C.12.2.18 Hardware and Software Maintenance and/or Licensing

Reference Section C.12.1.30 for description.

C.12.2.19 Independent Verification and Validation (Security)

Reference Section C.12.1.31 for description.

C.12.2.20 Managed E-Authentication Service (MEAS)

Reference Section C.12.1.32 for description.

C.12.2.21 Managed Firewall Service

Reference Section C.12.1.33 for description.

C.12.2.22 Privacy Data Protection

Reference Section C.12.1.34 for description.

C.12.2.23 Public Key Infrastructure

Reference Section C.12.1.35 for description.

C.12.2.24 Secure Managed Email Service

Reference Section C.12.1.36 for description.

C.12.2.25 Security Certification and Accreditation

Reference Section C.12.1.37 for description.

C.12.2.26 Systems Vulnerability Analysis/Assessment and Risk Assessment

Reference Section C.12.1.38 for description.

C.13 INFORMATION SYSTEM SECURITY (ISS)

The General Services Administration, other civilian Federal Agencies, the Department of Defense, federally recognized Native American tribes, and state and local Government entities require assistance in developing ISS products, including implementation. ISS addresses the security of information and computing resources at all organizational levels. All security requirements were included in both Functional Area One (1) and Functional Area Two (2). The descriptions in Section C.11 describe the ISS functional requirements and cover the location, source, and contact for any other information that the Contractor may need to know in order to perform ISS tasks. This includes the results of any previous audits, reviews, studies, certifications, risk, and vulnerability analyses, etc. that address the computer security of a system(s). All work completed under this contract shall comply with the latest versions of all applicable agency ISS guidance (e.g., Office of Management and Budget (OMB) circulars, General Services Administration (GSA) issuances, Public Laws (PLs), American National Standards Institute (ANSI) standards, and National Institute of Standards and Technology (NIST) standards, including Federal Information Processing Standards

(FIPS) publications. Also, individual task/delivery orders will reference applicable versions of standards or exceptions as necessary.