

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.

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.