ATTACHMENT 0001

PERFORMANCE WORK STATEMENT

FOR

INFORMATION TECHNOLOGY ENTERPRISE SOLUTIONS – 3 SERVICES (ITES-3S)

30 September 2021

Prepared by:
Product Director,
Computer Hardware, Enterprise Software and Solutions
9351 Hall RD, Building 1456
Fort Belvoir, VA 22060

TABLE OF CONTENTS

Information Technology Enterprise Solutions-3 Services (ITES-3S)
Performance Work Statement (PWS)

1. GENERAL

1.1 Description of Services/Introduction

The U.S. Army Computer Hardware, Enterprise Software and Solutions (CHESS), in coordination with the Army Contracting Command, Rock Island (ACC-RI), seeks qualified contractors to support the Army enterprise infrastructure and infostructure goals with information technology (IT) services worldwide (inside the contiguous United States (CONUS) and outside the contiguous United States (OCONUS)), including warzone areas.

The Army is seeking contractors who are willing to partner with the Army to fulfill its mission. The Army is structuring the ITES-3S contract in a manner that ensures that the contractors' goals and objectives are in alignment with those of the Army. Superior performance on the contractors' part will directly and indirectly link to superior Army mission accomplishment through the economic and efficient use of information technology. (Within the context of the Army/contractor partnership, the terms "partner" and "partnership" should not be read to suggest any formal legal partnership or joint venture between the contractor and the agency.) The Army/contractor partnership will reflect the attributes of an open, collaborative, and customer-oriented professional relationship.

The Army develops, maintains, and defends LandWarNet (LWN) as its portion of the Department of Defense's (DoD) Global Information Grid (GIG). The GIG is defined as a "globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel." Linking the force through reliable, simple, and effective network access is imperative for the modern Army to ensure that information gets to the decision-maker accurately, whether tactical or operational, in a timely manner, and under all circumstances to provide a force multiplier to that end-user.

1.2 Mission

The CHESS mission is to be the primary source to support the Warfighter's information dominance objectives by developing, implementing, and managing commercial IT contracts that provide enterprise-wide net-centric hardware, software, and engineering and support services for the Army.

1.3 Background

The Army LWN/Army Enterprise Infostructure (AEI) includes owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services. Non-LWN IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

ITES-3S provides IT services for LWN-associated IT that are directed towards enterprise connected IT, and not standalone systems.

In May of 2013, the Deputy Secretary of Defense directed DoD Components to participate in and implement the Joint Information Environment (JIE) under the direction of the DoD Chief Information Officer (CIO). The objective of the JIE is to "provide a single, secure, reliable, timely, effective, and agile command, control, communications and computers (C4) enterprise information environment for use by Joint forces and non-DoD mission partners across the full spectrum of operations, at all echelons, and in all operational environments." The Army is working various initiatives to transition the LWN/AEI into the JIE construct.

The Army strives to maintain the existing LWN and Army Enterprise Services while also undertaking the initiative to transition to the JIE.

1.4 Overall Objectives

The overall objective of ITES-3S is to provide industry best practice, best value, non-personal services to enable a broad range of enterprise-level support services for IT integration and service management activities to the Army, other DoD agencies, and all other Federal agencies including, but not limited to, locations CONUS, OCONUS, and warzone areas.

1.4.1 Contract Objectives

1.4.1.1 Establish and maintain contract methodologies and operations that are flexible, facilitate change, and allow for continuity of user support over the life of the contract.

1.4.1.2 Continuously improve task order competition throughout the life of the contract.

1.4.1.3 Increase use of subcontractors and teaming partners to bring expert talent and ingenuity to the varied work under ITES-3S, and effectively utilize small businesses to assure achievement of mandatory subcontracting goals.

1.4.1.4 Promote the contract to the Army, other DoD agencies, and all other Federal agencies to increase potential customers' awareness of available services, solutions, and benefits of this contract.

1.4.1.5 Support and partner with CHESS hardware and software contract holders as a preferred source of supply.

1.4.2 Program Objectives

1.4.2.1 Provide compliant, state-of-the-market, sustainable, supportable, and interoperable IT service solutions worldwide.

1.4.2.2 Identify and implement best commercial practices, new technologies, and streamlined approaches that afford the Army and other customers' IT and telecommunications structure the ability to improve their performance and IT business processes (e.g. offering tools, techniques, and practices for migration to a joint enterprise environment, supporting enterprise level services).

1.4.2.3 Support and partner with CHESS on the Army's data and reporting requirements through electronic interface and CHESS' *IT e-mart*.

1.4.2.4 Promote the benefits of performance-based contracting by educating the Army users.

1.4.2.5 Continuously seek ways to increase customer satisfaction through delivery of best value and superior IT services.

1.4.2.6 Assure affordable, best value, best priced IT solutions.

1.5 Scope

The ITES-3S scope will include a full range of services and solutions necessary for the Army to satisfy its support of the Army Enterprise infostructure and infrastructure goals with IT services throughout CONUS and OCONUS locations, including warzone areas. The scope includes the Command, Control, Communications, Computers, and Information Management (C4IM) requirements as defined in Army Regulation 25-1 (AR 25-1). Additionally, ITES-3S will include the services and solutions necessary for the Army and other services to transition from current service-centric information environments to the enterprise JIE as directed by the DoD CIO.

ITES-3S contemplates IT services-based solutions under which contractors may be required to provide a full range of equipment and software associated with those services. In addition to equipment and software, incidental construction may be required to provide a total solution. Therefore, end-to-end solutions to satisfy worldwide development, deployment, operation, maintenance, and sustainment requirements are included. Also included is support to analyze requirements, develop and implement recommended solutions, operate and maintain legacy systems and equipment. The types of services and solutions required for this acquisition will fall under the following Task Areas: Cybersecurity Services; IT Services; Enterprise Design, Integration, and Consolidation; Network/Systems Operation and Maintenance; Telecommunications/Systems Operation and Maintenance; Business Process Reengineering; IT Supply Chain Management; IT Education & Training, Intelligent Automation (Artificial Intelligence (AI)/Robotic Process Automation (RPA)), Cloud Services, and Data Services. It is the intent of the Government to establish a scope that is broad, sufficiently flexible to satisfy requirements that may change over the period of performance, and fully comprehensive so as to embrace the full complement of services that relate to IT.

ITES-3S will allow for ordering by all DoD and Federal agencies, but is being specifically crafted to be utilized as a strategic source for the Army.

All efforts supported under this contract shall be provided in accordance with Department of Defense, United States Army, DOD Intelligence Information Systems (DoDIIS), and National Security Agency standards as applicable to each task order.

Efforts under this contract will support industry best practices when prescribed by the aforementioned standards.

The services acquired on this contract apply to the full range of security domains, from Unclassified through Top Secret/Sensitive Compartmented Information (SCI).

1.5.1 Period of Performance

The ITES-3S basic contract awards will consist of multiple Indefinite Delivery Indefinite Quantity (IDIQ) contracts with a base period of five years, plus four one-year options, for a total of nine years of performance if all options are exercised.

1.6 General Information

1.6.1 Quality Assurance

The Government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.6.2 Recognized Holidays

New Year's Day
Martin Luther King Jr.'s Birthday
President's Day
Memorial Day
Juneteenth
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

Work at a Government site shall not take place on Federal holidays or weekends (but may require off-hour work due to network loading or other disruptions that could occur) unless directed by the Contracting Officer (KO) on individual task orders.

1.6.3 Hours of Operation:

The contractor is responsible for conducting business during the hours required on each individual task order, except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the workforce are essential. The contractor may also be required to support 24/7 operations 365 days per year as identified in individual task orders.

1.6.4 Place of Performance

The place of performance shall be identified in individual task orders. Locations will be Government or contractor sites within CONUS and/or OCONUS locations, including warzone areas. Locations may include Federal, State, or military data centers, and facilities, as defined in individual task orders.

1.6.5 Type of Contract

This is a Multiple Award Task Order (MATO) IDIQ contract. Individual task orders allowed under this agreement are Fixed Price (FP), Time and Materials (T&M), and Cost Reimbursement (CR).

1.6.6 Special Provisions

1.6.6.1 DOD Enterprise Software Initiative (ESI) and SmartBUY

The DOD ESI and SmartBUY are two initiatives that establish Enterprise Software Agreements (ESA) for commercial software. In accordance with the Defense Federal Acquisition Supplement (DFARS) Procedures, Guidance, and Information (PGI) 208.7403, in situations where the purchase of new commercial software, including preloaded software, is needed to satisfy the requirements of a particular order, requirements shall be fulfilled with software through the DOD ESI or SmartBUY sources. The contractor shall order from the DOD ESI and SmartBUY sources to obtain the software to satisfy the requirement. The contractor is responsible for reviewing available DOD ESI and SmartBUY sources. The listing of commercial software available from DOD ESI sources can be viewed on the website at http://www.esi.mil/. The listing of commercial software available from SmartBUY sources can be viewed on the website at http://www.gsa.gov/portal/content/105119. Also see SmartBUY Policy, dated 22 Dec 2005, DOD CIO Office, Department of the Defense Support of the SmartBUY initiative; electronic copy can be found at http://www.esi.mil/download.aspx?id=463. In addition, the contractor may be required to utilize software provided by the Government as Government-furnished property.

1.6.6.2 Waiver Process

If the software is not available from the DOD-ESI or SmartBUY sources, and such software is to be used as part of the total solution, the Army requiring activity is responsible for obtaining a Statement of Non-Availability (SoNA) from CHESS and an Information Technology Approval System (ITAS) waiver from the CIO/G6 office. CHESS will issue a SoNA to the requestor. The SoNA does not constitute approval to purchase or deviate from any Army Regulation or policy. Please refer to the Army Waiver Process for Commercial Off-the-Shelf Information Technology (COTS IT) non-CHESS Procurements Memorandum. HQDA-CIO/G-6 will approve all requests from all Army organizations seeking to purchase COTS IT through sources other than PD CHESS, regardless of cost or appropriation. Commands funding the purchase of IT hardware or software not utilizing PD CHESS will need to obtain an ITAS waiver through HQDA-CIO/G-6 via the following website: https://cprobe.army.mil/enterprise-portal/web/itas/home. Additional information regarding the waiver process can be found on the CHESS website at https://CHESS.army.mil.

1.6.7 Security Requirements

Contractor personnel performing work under this contract shall have the appropriate security clearance as specified in each individual task order at time of the proposal submission, and shall maintain the level of security required for the life of the contract.

1.6.7.1 DD Form 254

Overarching security requirements and contractor access to classified information shall be as specified in the basic DD Form 254, “Department of Defense Contract Security Classification Specification,” which will be further identified in the DD Form 254 for each TO, as required. All contractor personnel with access to unclassified information systems, including e-mail, shall have at a minimum a favorable National Agency Check (NAC).

1.6.7.2 Visitor Group Security Agreement

The contractor may be required to sign a Contractor Visitor Group Security Agreement to protect classified information involved in performance under individual task orders. The Agreement will outline responsibilities in the following areas: Contractor security supervision; Standard Practice Procedures; access, accountability, storage, and transmission of classified material; marking requirements; security education; personnel security clearances; reports; security checks; security guidance; emergency protection; protection of Government resources; DD Forms 254; periodic security reviews; and other responsibilities, as required.

1.6.7.3 Physical Security

The contractor shall be responsible for safeguarding all Government equipment, information and property provided for contractor use. At the close of each work period (according to the time defined within the requiring task order), Government facilities, equipment, and materials shall be secured.

1.6.7.4 Cyber Security Training

All contractor employees and associated subcontractor employees must complete the DoD Cyber Awareness Challenge Training (formerly Information Assurance Awareness Training) before issuance of network access, and annually thereafter. IAW DoDD 8570.01 and AR25-2, all contractor personnel supporting Cybersecurity functions shall complete appropriate training within specified timelines and attain and maintain the required Information Technology (IT) and cybersecurity training certifications.

1.6.7.5 Anti-Terrorism (AT) Training

All Contractor employees, to include subcontractor employees, requiring access to Army installations, facilities and controlled access areas shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR or to the contracting officer, if a COR is not assigned, within 5 calendar days after completion of training by all employees and subcontractor personnel.

1.6.7.6 Access and General Protection/Security Policy and Procedures

The contractor and all associated subcontractor employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services, or Security Office. Contractor workforce must comply with all personal identity verification requirements (Federal Acquisition Regulation (FAR) clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA, and/or local policy. In addition to the changes otherwise authorized by the "changes clause" of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

1.6.7.7 Contractors That Do Not Require CAC But Require Access to a DoD Facility or Installation

The contractor and all associated subcontractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

1.6.7.8 Threat Awareness Reporting Program

For all contractors with security clearances. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a counterintelligence special agent or other trainer as specified in 2-4b.

1.6.8 Post Award Conference/Periodic Progress Meetings

The contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with FAR Subpart 42.5, "Post award Orientation." The Contracting Officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings, the Contracting Officer will apprise the contractor of how the Government views the contractor's performance, and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government.

1.6.9 Contracting Officer Representative (COR)

The COR will be identified by separate letter for the basic contract and for each individual task order. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor contractor's performance and notify both the Contracting Officer and contractor of any deficiencies; coordinate availability of Government furnished property; and provide site entry of contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates, or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.6.10 Badges

1.6.10.1 Corporate Identification

Contractor personnel shall wear and clearly display an identification badge with their full name and corporate affiliation at all times while performing Government-site duties and while at TDY locations on official business. All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor's participation is appropriately disclosed.

1.6.10.2 Common Access Card (CAC)

Contractor personnel shall be required to obtain a CAC, which will provide access to facilities in addition to allowing access to the Nonsecure Internet Protocol (IP) Router Network (NIPRnet).

1.6.10.3 CAC Issuance

The contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI), or an equivalent or higher investigation in accordance with Army Directive 2014-05 and the requirements of this contract. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD Federally-controlled facilities on behalf of the DoD on a recurring basis for a period of six (6) months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully completed NACI at the Office of Personnel Management. Contractors will NOT be sponsored to obtain a CAC or given access to the PEO EIS Information Systems until this can be verified in Joint Personnel Adjudication System (JPAS). The Trusted Associate Sponsorship System Trusted Associate has the responsibility to verify the Contractor's clearance.

1.6.11 Contractor Travel (TDY)

TO related travel costs, (i.e., relocation and temporary duty (TDY) to include travel, lodging and meals) are reimbursable, may be required, and will be specified in the in each individual task order. All travel requirements (including plans, agenda, itinerary, or dates) shall be pre-approved by the Government (subject to local policy procedures). Costs for travel shall be billed in accordance with the regulatory implementation of Public Law 99-234 and FAR 31.205-46, Travel Costs (subject to local policy & procedures; may reference FAR). The contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. All travel requires Government approval/authorization and notification to the COR.

1.6.12 Other Direct Costs

The Other Direct Costs (ODC) category provides an estimate of the types and quantity of material, equipment, bonding, and travel necessary for the contractor to perform the work expected to be accomplished. ODCs consist of IT Solution Equipment, IT Solution Software, Travel and Per Diem, and Other ODCs and are reimbursable under cost reimbursement CLINs. The contractor shall include a detailed description of all proposed ODCs in individual TO proposals. The cost of general purpose items required for the conduct of the contractor's normal business operations will not be considered an allowable ODC in the performance of this contract.

1.6.13 Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational

Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI, and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and, in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.14 Phase-In Period

To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the contractor shall have personnel on board during the sixty (60) calendar day phase-in periods. During the phase-in period, the contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date.

The contractor shall be ready to propose of task order requests at the conclusion of the sixty (60) day phase-in period, following issuance of the notice to proceed. During that period the contractor shall:

(1) Develop an ordering guide and a website which shall be provided to the Government for review;

(2) Secure required personnel;

(3) Coordinate for security clearances (interim clearances will be requested until final clearances are issued, if required);

(4) Provide labor categories and pricing to PD CHESS for inclusion in the PD CHESS *IT e-mart* (See Section 2.4.1, Contract Management);

(5) Provide sample copies of required reports to PD CHESS for review and approval (See Section 2.4.1, Contract Management); and

(6) Provide a complete list of the Program Management team, to include names, positions, phone numbers, and email addresses.

2. TASKS

2.1 Non-Personal Services

The Government shall neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for individual contractor employees. It shall be the

responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Procuring Contracting Officer (PCO) immediately.

2.2 Services

The Army strives to sustain and improve the existing LWN and Army Enterprise Services while also undertaking the initiative to transition to the JIE. The ITES-3S service solutions will provide the required support to achieving these initiatives.

As cited in AR 25-1, the C4IM Services List is the foundation of the LWN Services Catalog. The LWN Services Catalog identifies and defines IT services supported or provided by Army Network Enterprise Centers (NEC). The service portfolios identified are: Cyber-security Services; IT Services; Business Process Reengineering; Enterprise Design, Integration, and Consolidation; Network/Systems Operation and Maintenance; Telecommunications/Systems Operation and Maintenance; IT Supply Chain Management; and IT Education & Training.

The JIE is dependent upon developing and implementing new technical capabilities on an unprecedented scale. As described in "The Department of Defense Strategy for Implementing the Joint Information Environment, September 18, 2013," the JIE focuses around six complex technical areas:

- **Single Security Architecture (SSA)** – Establishing an SSA will collapse network security boundaries, reduce the Department's external attack surface, enable better containment and maneuver in reaction to cyberattack, and standardize management, operational, and technical security controls.
- **Network Normalization** – DoD's current system of disparate network, processing, and storage infrastructures impedes internal and external collaboration for the warfighter and mission partners. As such, a foundational aspect of achieving the JIE is to provide a single, protected information environment that securely, reliably, and seamlessly interconnects warfighters.
- **Identity and Access Management** – Optimized Global Identification, Authentication, Access Control, and Directory Services are central to satisfying the warfighter's need for a portable identity and the ability to share contact information between organizations.
- **Enterprise Services** – An enterprise service is a service, like email, that is provided in a common way across the Department, and is provided by a single organization acting as the enterprise-service provider. DoD is emphasizing development and deployment of enterprise services as part of JIE that are designed to operate in deployed, disconnected, or low-bandwidth information environments.
- **Cloud Computing** – DoD's move to cloud computing presents challenges, especially in the management of thousands of shared computer servers, cybersecurity (as part of single security architecture), resilience and failover, and migration of software applications onto the cloud.
- **Data Center Consolidation** – The DoD will continue to consolidate computing power by closing and consolidating data centers across the Department, while concurrently

identifying existing data centers to be transitioned into JIE Core Data Centers (CDCs). Data center consolidation will be integral to facilitating the move the Department to a standardized computing architecture.

The service portfolios identified below support the design, implementation, and sustainment of these JIE technical areas.

ITES-3S service solutions are categorized under the appropriate DoD Services Taxonomy Services Portfolio Groups identified and enumerated below. The task areas are further defined to list a subset of efforts that typically fall under each task area. Specific details of task assignments, deliverables, documentation, training, applicable Government/department/industry standards, etc., will be provided within individual task orders.

The listed sub-tasks under the Task Areas/Service Portfolios are not all inclusive. There are many other sub-tasks that are within ITES-3S scope not only belonging under the Service Portfolios listed below but also to Task Areas/Service Portfolios not listed.

The contractor shall provide coverage of all of the labor categories as listed and identified in Appendix 2.

2.2.1 Cybersecurity Services

As defined in Department of Defense Instruction (DoDI) 8500.01, Cybersecurity is the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Cyber Security Development/Solutions **DJ01**
Cyber Operations **DJ01**
Computer Network Defense and Offense Services **DJ01**
Identity Management Solutions **DJ01**
Continuous Monitoring Solutions/Services **DJ01**
Cyber Security Architecture **DA01**
Cyber Forensics & Analytics **DJ01**
Mobile Security Solutions **DD01, DJ01**
Computer Security Awareness and Training **DJ01**
Computer Security Incident Response **DJ01**
Information, System, Data, and Physical Security **DJ01**
Mainframe Automated Information Security Support **DJ01**
Biometrics **DJ01**
Continuity of Operations **DC01, DJ01**
Contingency Planning **DA01, DJ01**
Critical Infrastructure Protection **DC01, DJ01**
Cryptographic Support and Service **DJ01**
Disaster Recovery **DC01, DJ01**
Policy and Compliance **DD01, DA01**
Commercial Solutions for Classified (9999)

Public Key Infrastructure and CAC authentication **DJ01**
Remote Monitoring/Intrusion Detection **DJ01**
Security Architecture Design **DA01, DJ01**
Security Hardening **DJ01**
Secure Video Teleconferencing **DJ01**
System Certification and Accreditation **DJ01**
System Recovery Support Services **DC01, DJ01, DJ01**

2.2.2 Information Technology Services

The Committee on National Security Systems (CNSS) Instruction No. 4009 defines Information Technology as "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 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources."

Application and Service Hosting **R415, R425, DC01, DA10, DA01, DG11, DJ01, DK01**
Automated Workflow System Development and Integration **DA01, R412, DA01, R425, DJ01, AD24, AD25**
Big Data Analysis/Management **DD01**
Configuration Management **DC01**
Capacity Management **DC01**
Computer Aided Design/Engineering/Management (CAD/CAE/CAM) **DA01**
Computer Systems Administration, Management, and Maintenance **DC01**
Design/Specifications for Information Systems **DD01**
Data and/or Media Management **DH01, DH01**
Data Storage Management **DD01, DC01, DK01**
Data Warehousing **DK01, DJ01, DJ01, DH01, DH01, DH01**
Database Applications Development **DH01, DA01, DA01**
Design/Specifications for Information Dissemination **DD01**
DODAF-based Operational & System Architecture Design & Development **DA01**
Economic/Business Case Analysis (Cost/Benefit and Risk) **DJ01**
Electronic Commerce and Electronic Data Interchange Support **DJ01**
Global/Geographic Information Systems **DH01**
Informatics **DH01, DD01, DD01, DH01, DA01**
Information Architecture Analysis **DA01**
IT Architecture Support **DA01**
Internet/Intranet/Web Applications/Network Computing **DB10, DA01, DG01**
Legacy Systems Modernization **DA01**
Performance Benchmarking/Performance Measurements **DA01**
Property Management **DC01**

Section 508 Compliance Support **DA01**
Simulation and Modeling **R412**
Software/Middleware Development **DA01**
Source Data Development **DA01**
Statistical Analysis **DD01**
Systems Development and Software Maintenance **DA01, DA10**
Systems Programming **DA01**
Telecommunications Specialist **DG01**
Video Teleconferencing/Audio /Visual/Media Systems **DC01**
Voice over Internet Protocol (VOIP) **DD01**
Web and Computer Systems Decision Support Tools **DB10, DJ01, DG11**
Web Enabled Applications **DB10, DJ01, DG11**

2.2.3 Enterprise Design, Integration, and Consolidation

Collaboration Systems/Facility Development **R425**
Compliance with Interoperability Standards **R425**
Cost Benefit/Cost Effectiveness Analysis **R425, DJ01**
Independent Verification and Validation **R425**
Information and Knowledge Engineering **R425**
Information Management Life Cycle Planning/Support **R425, DJ01**
Integrated Solutions Management **R425**
Knowledge Engineering/Management **R425**
Market Research and Prototyping **R425**
Measuring Return on Investment (ROI) **R425, DJ01**
Earned Value Management **R425**
Product Integration **R425**
Reliability and Maintainability **R425, DJ01**
Requirements Analysis **R425**
Resource Planning Systems Development and Integration **R425**
Resource Systems Management **R425**
Resource Systems Planning **R425**
Reverse Engineering **R425**
Software Engineering **R425**
Software Life Cycle Management **R425**
Systems Integration **R425**
Technology Insertion **R425**
Test and Evaluation **R425, H258, H259**
Wireless Networking **R425, DG11**

2.2.4 Network/Systems Operation and Maintenance

Computer Center Technical Support **DC01, DA01**
Commercial Off-the-Shelf Software Products and Support **DG01**
Computer Systems Administration **DG01**
Computer Systems Facilities Management and Maintenance **DC01**
Licensing Support **DA10**

Legacy Systems Maintenance **DA10, DE01**
Network Management **DG01**
Help Desk Support **DE01, DJ01, DA01**
Desktop Support **DE01, DJ01, DA01**
Software License Management **DA10**
Supply Chain Management **DE01, DJ01, DA01**
Network Infrastructure Support **DE01, DJ01, DA01**
Office Automation Support **DE01, DJ01, DA01**
Seat Management/Asset Management **DE01, DJ01, DA01**

2.2.5 Telecommunications/Systems Operation and Maintenance

Telecommunications Infrastructure Office Automation Support **DE01, DJ01, DA01**
Voice over IP Support **DD01**
Handset Management/Asset Management **DE01, DJ01, DA01**

2.2.6 Business Process Reengineering (BPR)

BPR is a means to restructure an organization by means of a radical reassessment of its core processes and predominant competencies and often involves the analysis and redesign of workflow within and between enterprises. BPR helps entities to radically restructure their organizations by focusing on the ground-up design of their business processes.

Benchmarking/Operational Capability Demonstrations **R412**
Business Case Analysis **DA01, DJ01**
Customer Relationship Management **DK01**
E-Business Planning and Support **DK01**
Functional Requirements Decomposition **DJ01, DD01**
Gap Analysis **DJ01, DD01**
IT Capital Planning **DD01**
Quality Assurance **DD01, H159**
Risk Management **DJ01, DD01**
Workflow Analysis **DJ01, DD01**

2.2.7 IT Supply Chain Management

Logistics **DA01**, **DJ01**
Purchasing **DD01, DA01**, **DJ01**
Inventory Management **DA01**, **DJ01**
Vendor Management **DA01**, **DJ01**
Subcontractor Management **DA01**, **DJ01**

2.2.8 IT Education & Training

User Training Purchasing **DA01**, **DA01, U001**

Instructional Design and Modeling & Simulation **U008, U012, R412**
Design & execution of computer-generated imaging/training **U008**

2.2.9 Intelligent Automation [**Artificial Intelligence (AI)/Robotic Process Automation (RPA)]**

Robotic Process Automation (RPA) is an emerging technology area that has not been officially defined by NIST but is being promoted as a commercial solution.

Artificial Intelligence (AI) Engineer – Intermediate DB01
Machine Learning Engineer – Intermediate DB01
Machine Learning (Data) Scientist – Senior DB01

2.2.10 Cloud Services

Hosting **DC10**
Modernization **DD01**
Transition Support **DD01**

2.2.11 Data Services

Data Analytics **DH01**

2.3 Business Relations

The contractor shall successfully integrate and coordinate all activity needed to execute the requirement. The contractor shall manage the timeliness, completeness, and quality of problem identification. The contractor shall provide corrective action plans, proposal submittals, timely identification of issues, and effective management of subcontractors. The contractor shall seek to ensure customer satisfaction and professional and ethical behavior of all contractor personnel.

2.4 Contract Administration and Management

The following subsections specify requirements for contract, management, and personnel administration.

2.4.1 Contract Management

The contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement. The contractor must maintain continuity between the support operations at ACC-RI, CHESS, and the contractor's corporate offices.

(a) Contract Management. The Contractor shall maintain a status review process for planning and controlling the activities necessary to meet the requirements of this contract.

(b) Meetings and Conferences. During the life of the contract, periodic meetings will be held at both contractor and Government sites. Contractors shall attend the meetings in order to

review program status, assess contractor performance, refine current processes, and plan future actions. Army PD CHESS conducts the Army Information Technology Conference (AITC) (minimum of one, maximum of two per year) at various locations. Participation in meeting and conferences shall be at no additional cost to the Government.

(c) Contract Management Reports. All contract management deliverables shall be delivered to PD CHESS for review and comment or approval. The contractor shall submit reports as indicated below. All reports shall be submitted electronically to CHESS at the following email address: peoeis.pdchess.vndrrpts@us.army.mil. Contract management and reports shall be provided at no additional charge to the Government. A report for "no activity" is required via email message. All reports are to be provided as specified in below in Appendix 5.

(1) Order Transactions (OT) Report. The contractor shall provide the monthly OT report to PD CHESS and ACC-RI by the 15th of each month for inclusion into its Order Tracking database. Monthly submission shall be used for reporting new orders or new order modifications that have not been previously reported. The specific file layout definition and submission instructions will be specified in the basic contract.

(2) Monthly Task Order Status Report (MTOSR). The contractor shall provide the MTOSR to PD CHESS and ACC-RI by the 15th of each month. The report shall include a brief summary of significant activities, problems, and developments occurring during the reporting period, as well as progress made at the task order level. It provides an activity summary by order number. A sample format is specified in the basic contract.

(3) Small Business Participation Report (SBPR). The Contractor shall provide the ITES-3S SBPR to PD CHESS and ACC-RI by the 15th of each month. The specific file layout definition and submission instructions will be specified in the basic contract.

(4) *IT e-mart* Online Catalog Information. The contractor shall provide a listing of Labor Rates for their companies at contract start up. The specific file layout definition and submission instructions will be specified in the basic contract. The Labor Rates provided by the contractor will be the same Labor Rates proposed in the contractor's proposal.

(5) Performance-based Progress Report (PBPR). The contractor shall provide the report on a quarterly basis to report the performance-based aspects (proposed measures/metrics and incentives/disincentives). Submission of this report will commence at least within six months after receipt of initial task order. The report shall be submitted to PD CHESS and ACC-RI by the 15th of the month following the end of a quarter.

(6) Additional reports shall be provided as required in individual orders.

2.4.2 Contract Administration

Notwithstanding the contractor's responsibility for total management during the performance of this contract, the administration of the contract requires maximum coordination between the Government and the contractor. The following provides the roles and their respective authority during the performance of the contract:

(1) Contracting Officer (KO). The KO is the only person authorized to direct changes in any of the requirements under this contract, and, notwithstanding any provisions contained elsewhere in this contract, said authority remains solely with the KO. In the event the contractor effects any such change at the direction of any person other than the KO, the change will be considered to have been made without authority and solely at the risk of the contractor.

All contract administration will be effected by the KO. Communications pertaining to contractual administrative matters shall be addressed to the KO. No changes in or deviation from the terms and conditions shall be effected without a written modification to the contract, executed by the KO, authorizing such changes.

(2) Contracting Officer's Representative (COR). The KO shall designate contract level CORs during the term of this contract in accordance with DFARS clause 252.201-7000 "Contracting Officer's Representative." The COR will provide assistance in identification and resolution of problems, conflicts in priority, subtask requirement definitions, and other operations type problems.

(3) Ordering Contracting Officers (OCO). OCOs within the Army, DoD, and other Federal agencies are authorized to place orders within the terms of this contract and within the expert of their authority. They are not authorized to make changes to the contract terms. OCO authority is limited to the individual task orders.

(4) Order Contracting Officer's Representative (OCOR). The OCOR may designate individuals to act as OCORs under any resultant task order. OCORs may provide technical guidance in direction of the work, but they will not be authorized to change any of the terms and conditions of the contract or order. OCORs will be designated by a letter of appointment from the OCO.

(5) Contractor. The contractor shall not accept any instructions issued by any person employed by the U.S. Government or otherwise, other than the KO, or the TO COR acting within the limits of his or her authority. The contractor shall not in any way represent that it is a part of the U.S. Government, or that it has the authority to contract or procure supplies for the account of the United States of America

2.5 Technology Refreshment

(a) In order to maintain ITES-3S as a viable contract vehicle, current with the IT solution services required within scope, the Government may solicit, and the Contractor is encouraged to propose independently, technology improvements to the task areas, labor categories, or other requirements of the contract. These improvements may be proposed to add labor categories; reduce or increase composite and/or fixed labor rates for labor categories in the Labor Rates Table; add task/subtask areas in PWS; improve overall performance, or for any other purpose which presents a technological advantage to the Government. Use of any labor categories not incorporated into the basic contract are subject to Government approval prior to use. Those proposed technology improvements that are acceptable to the Government will be processed as modifications to the contract.

(b) As a minimum, the following information shall be submitted by the Contractor with each technology improvement proposal to the Contracting Officer and Contracting Officer's Representative via email:

(1) A description of the difference between the existing contract requirement and the proposed change, and the comparative advantages and disadvantages of each;

(2) Itemized requirements of the contract that must be changed if the proposal is adopted, and the proposed revision to the contract for each such change;

(3) A price proposal including the following shall be submitted: An estimate of the changes in performance and price, if any, that will result from adoption of the proposal; and an item-by-item summary of any "street pricing" (at least three sources) of the items including a reference and hyperlink to the source of the "street price" and GSA Schedule pricing, if any (include GSA Schedule Number, with hyperlink to the schedule). Include an electronic version of the revised Labor Rates Table reflecting the change to facilitate contract modification, as well as an updated Product Attribute (PA) file;

(4) A statement and supporting rationale of the proposed effective date of the contract modification adopting the proposal, in order to obtain the maximum benefits of the changes during the remainder of this contract; and

(5) Identify any effect on the contract completion time or delivery schedule.

(c) The Government will not be liable for proposal preparation costs or any delay in acting upon any proposal submitted pursuant to this clause. The Contractor has a right to withdraw, in whole or in part, any proposal not accepted by the Government within the period specified in the proposal. The decision of the KO as to the acceptance of any such proposal under this contract is final and not subject to the "Disputes" clause of this contract.

(d) The KO may accept any proposal submitted pursuant to this clause by issuance of a modification to this contract. Unless and until a modification is executed to incorporate a proposal under this contract, the Contractor shall remain obligated to perform in accordance with the requirements, terms and conditions of the existing contract. Upon issuance of the modification, the approved modification will be loaded to the CHESS *IT e-mart*.

(e) If a proposal submitted pursuant to this clause is accepted and applied to this contract, the increasing or decreasing of the contract price shall be in accordance with the procedures of the "Changes" clause. The resulting contract modification will state that it is made pursuant to this clause.

2.6 Subcontract Administration

The Small Business Participation Plan reporting will be as required in Section 2.4.1, Contract Management. This reporting is separate from the Small Business Subcontracting Plan requirement as required for Contractors with a business size designation of "other than small" in accordance with Section I, FAR clause 52.219-9, Small Business Subcontracting Plan, Alt II and

DFARS clause 252.219-7003, Small, Small Disadvantaged, and Women-Owned Small Business Subcontracting Plan (DoD Contracts).

2.7 Contractor Personnel, Disciplines, and Specialties

(a) The contractor shall employ, for the purpose of performing that portion of the contract work in the State of Hawaii, individuals who are residents thereof and who, in the case of any craft or trade, possess or would be able to acquire promptly the necessary skills to perform the contract.

(b) The contractor shall insert the substance of this clause, including this paragraph (b), in each subcontract awarded under this contract.

Conduct of Contractor Personnel: If the KO finds it to be in the best interest of the Government, within the foreign environment in which the contractor will be performing outside the limits of the United States and its possessions, the KO may at any time during the performance of this contract TO request the contractor to remove any of its personnel from further performance under this contract for reasons of their moral character, unethical conduct, security reasons, and for violation of installation regulations. In the event that it becomes necessary to replace any contractor personnel for any of the above reasons, the contractor shall bear all costs associated with such removal, including the costs for the replacement of any personnel so removed. The contractor or contractor personnel shall be responsible for the return of all logistical support items (i.e., ID cards, ration cards, POV tags and registration, POV and GOV operator's licenses, etc.) prior to departure from an overseas area of operation.

2.8 Notice of Internet Posting of Awards

It is the Government's intent to electronically post the ITES-3S contracts and modifications to the CHESS *IT e-mart* web site. This does not include contractor proposals or any other proprietary information provided by contractors relevant to performance of this contract. Posting of the awards and modifications via the *IT e-mart* is in the best interest of the Government as well as the contractors. It will allow contractors to direct future customers to the site to view labor categories and rates as they develop their Independent Government Cost Estimates (IGCE) in preparation of proposed RFPs.

2.9 Contractor Management Reporting (CMR)

(Only applies to Army customers): The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where the contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this contract. The contractor shall completely fill in all the information in the format using the following web address https://Contractormanpower.army.pentagon.mil. The required information includes: (1) Contracting Office, Contracting Officer, Contracting Officer's Technical Representative (COTR) (also known as the Contracting Officer's Representative (COR)); (2) Contract number, including task order number; (3) Beginning and ending dates covered by the reporting period; (4) Contractor's name, address, phone number, e-mail address, identity of contractor employee

entering data; (5) Estimated direct labor hours (including sub-contractors); (6) Estimated direct labor dollars paid this reporting period (including sub-contractors); (7) Total payments (including sub-contractors); (8) Predominant Federal Service Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each sub-contractor if different); (9) Estimated data collection cost; (10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information); (11) Locations where contractor and sub-contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website); (12) Presence of deployment or contingency contract language; and (13) Number of contractor and sub-contractor employees deployed in theater this reporting period (by country). As part of its submission, the contractor shall provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period shall be the period of performance not to exceed 12 months, ending September 30 of each Government fiscal year, and must be reported by 31 October of each calendar year. Contractors may use a direct XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's system to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the website.

APPENDIX 1: DEFINITIONS AND ACRONYMS

DEFINITIONS AND ACRONYMS

1. Definitions

1.1 Contractor
A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

1.2 Contracting Officer
A person with the authority to enter into, administer, and/or terminate contracts, and make related determinations and findings on behalf of the Government. Note: The only individual who can legally bind the Government.

See also: FAR 2.101

1.3 Contracting Officer's Representative (COR)
An employee of the U.S. Government appointed by the Contracting Officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the contractor, as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

See also: FAR 2.101 and DFARS 202.101

1.4 Defective Service
A service output that does not meet the standard of performance associated with the Performance Work Statement.

1.5 Deliverable
Anything that can be physically delivered, but may include non-manufactured things such as meeting minutes or reports.

1.6 Key Personnel
At the task order level, contractor personnel that are evaluated in a source selection process that may be required to be used in the performance of a contract as listed in the PWS. When said personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

1.7 Physical Security
Actions that prevent the loss or damage of Government property.

1.8 Quality Assurance
The Government procedures to verify that services being performed by the contractor are performed according to acceptable standards.

1.9 Quality Assurance Surveillance Plan (QASP)
An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

1.10 Quality Control
All necessary measures taken by the contractor to assure that the quality of an end product or service shall meet contract requirements.

1.11 Subcontractor
One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

1.12 Work Day
The number of hours per day the contractor provides services in accordance with the TO.

1.13 Work Week
Work week as specified per task order directive.

2. Acronyms

ACC	Army Contracting Command
ACC-RI	Army Contracting Command, Rock Island
ACOR	Alternate Contracting Officer's Representative
AEI	Army Enterprise Infostructure
AFARS	Army Federal Acquisition Regulation Supplement
AIN	Agency Internet Network
API	Application Programming Interface
AR	Army Regulation
AV	Audio Visual
BEA	Business Enterprise Architecture
BLS	Bureau of Labor Statistics
BPR	Business Process Reengineering
BTA	Business Transformation Agency
C&A	Certification and Accreditation
C4	Command, Control, Communications, and Computers
C4IM	Command, Control, Communications, Computers, and Information Management
CAC	Common Access Card
CAD	Computer Aided Design
CAE	Computer Aided Engineering
CAM	Computer Aided Management
CASE	Computer-Aided Software Engineering

CCE	Contracting Center of Excellence
CDC	Core Data Center
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CGI	Common Gateway Interface
CHESS	Computer Hardware, Enterprise Software and Solutions
CIO	Chief Information Officer
COMSEC	Communications Security
CM	Configuration Management
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
CSIRT	Computer Security Incident Response Team
DA	Department of the Army
DBMS	Database Management System
DD250	Department of Defense Form 250 (Material Inspection and Receiving Report)
DD254	Department of Defense Form 254 (Department of Defense Contract Security Classification Specification)
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoD-ESI	Department of Defense Enterprise Software Initiative
DoDIIS	Department of Defense Intelligence Information Systems
DT&E	Development, Test, & Evaluation
ERP	Enterprise Resource Planning
FAE	Functional Area Expert
FAR	Federal Acquisition Regulation
FFP	Firm-Fixed-Price
FPIF	Fixed Price Incentive Firm
FP-LOE	Fixed Price Level of Effort
FTP	File Transfer Protocol
GAO	Government Accountability Office
GIG	Global Information Grid
HIPAA	Health Insurance Portability and Accountability Act of 1996
HQDA	Headquarters Department of the Army
HTML	Hyper Text Markup Language
IA	Information Assurance
IDIQ	Indefinite Delivery Indefinite Quantity
INFOSEC	Information Security
IT	Information Technology

IV&V	Independent Verification and Validation
JCL	Job Control Language
JIE	Joint Information Environment
JTR	Joint Travel Regulation
KO	Contracting Officer
LAN	Local Area Network
LWN	LandWarNet
MATO	Multiple Award Task Order
NAC	National Agency Check
NEC	Network Enterprise Center
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
OMB	Office of Management and Budget
OT	Order Transaction
PC	Personal Computer
PCAP	Packet Capture
PCO	Procuring Contracting Officer
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
RFID	Radio Frequency Identification
ROI	Return on Investment
SA	System Architect
SCI	Sensitive Compartmented Information
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOC	Standard Occupational Classification
SQL	Structured Query Language
TCP	Transmission Control Protocol
TDY	Temporary Duty
TE	Technical Exhibit
T&M	Time and Materials
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network
XML	Extensible Markup Language

APPENDIX 2: LABOR CATEGORIES

LABOR CATEGORIES AND DESCRIPTIONS

The Government's minimum requirements for each labor category are identified in the paragraphs below. The contractor may augment their labor categories and job descriptions on a task order basis; however, use of any labor categories not incorporated into the basic contract are subject to Government approval prior to use. The contractor may propose to the Government, at their discretion, additional labor categories and job descriptions within the scope of ITES-3S. Contractors may also propose deviations from the education and experience requirements for particular labor categories when responding to task order solicitations. These deviations shall be clearly identified in the task order proposal.

ITES-3S labor categories have been harmonized with the Office of Management and Budget's (OMB) Standard Occupational Classification (SOC) for which the Bureau of Labor Statistics (BLS) maintains compensation data. Labor categories are further defined as Associate, Intermediate, and Senior based on years of experience, education, and duties/responsibilities as follows:

- **SENIOR**: A Senior employee has over 10 years of experience and an MA/MS degree. A Senior employee typically works on high-visibility or mission critical aspects of a given program and performs all functional duties independently. A Senior employee may oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job.

- **INTERMEDIATE**: An Intermediate employee has more than 5 years of experience and a BA/BS or MA/MS degree. An Intermediate employee typically performs all functional duties independently.

- **ASSOCIATE**: An Associate employee has less than 5 years of experience and a BA/BS degree (or in certain technical roles, a BS). An Associate employee is responsible for assisting more senior positions and/or performing functional duties under the oversight of more senior positions.

SUBJECT MATTER EXPERT (SME)/FUNCTIONAL AREA EXPERT (FAE): An SME/FAE is an individual whose qualifications and/or particular expertise are exceptional and/or highly unique. SMEs/FAEs do not have specific experience/education qualifications, but are typically identified as recognized industry leaders for a given area of expertise. SMEs/FAEs typically perform the following kinds of functions: Initiates, supervises, and/or develops requirements from a project's inception to conclusion for complex to extremely complex programs; Provides strategic advice, technical guidance, and expertise to program and project staff; Provides detailed analysis, evaluation and recommendations for improvements, optimization development, and/or maintenance efforts for client-specific or mission critical challenges/issues; Consults with client to define need or problem supervises studies and leads surveys to collect and analyze data to provide advice and recommend solutions.

1. Program Management

SOC No. 11-3021, Computer and Information Systems
SOC No, 11-1021, General and Operations
SOC No. 11-3011, Administrative Services
SOC No. 11-3131, Training and Development

1.1 Program Manager – Senior (Project Management Institute (PMI) certification required)

Description: Under indirect supervision, oversees the operational planning, establishment, execution, and evaluation of a multifaceted program/project typically consisting of a set of closely related subprograms or associated activities. Oversees fiscal, operational, administrative, and human resources management of the program; seeks and develops outside funding sources, serves as principal point of representation and liaison with external constituencies on operational matters, and provides day-to-day technical/professional guidance and leadership as appropriate to the area of expertise.

1.2 Program Manager – Intermediate (PMI certification desired)

Description: Under general direction, oversees the operational planning, establishment, execution, and evaluation of a multifaceted program/project typically consisting of a set of closely related subprograms or associated activities. Oversees fiscal, operational, administrative, and human resources management of the program; seeks and develops outside funding sources, serves as principal point of representation and liaison with external constituencies on operational matters, and provides day-to-day technical/professional guidance and leadership as appropriate to the area of expertise.

1.3 Program Manager – Associate

Description: Under immediate supervision, oversees the operational planning, establishment, execution, and evaluation of a multifaceted program/project typically consisting of a set of closely related subprograms or associated activities. Oversees fiscal, operational, administrative, and human resources management of the program; seeks and develops outside funding sources, serves as principal point of representation and liaison with external constituencies on operational matters, and provides day-to-day technical/professional guidance and leadership as appropriate to the area of expertise.

2. Project Management

SOC No. 11-3021, Computer and Information Systems Manager
SOC No. 11-1021, General and Operations Manager
SOC No. 11-3011, Administrative Services, Facilities Manager,
SOC No. 11-3131, Training and Development Manager
SOC No. 17-2071, Electrical Engineer
SOC No. 17-2072, Electronics Engineer
SOC No. 17-2061, Computer Hardware Engineer

SOC No. 17-2199, Engineer, all others
SOC No. 15-1142, Computer Systems, Wide Area Network, Network, Network Security Administrator
SOC No. 15-1141, Database, Database Security Administrator
SOC No. 13-1071, Staffing Support

2.1 Project Manager – Senior (PMI certification required)

Description: Responsible for all aspects of the development and implementation of assigned projects and provides a single point of contact for those projects. Takes projects from original concept through final implementation. Interfaces with all areas affected by the project including end users, computer services, and client services. Defines project scope and objectives. Develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensures adherence to quality standards and reviews project deliverables. Manages the integration of vendor tasks and tracks and reviews vendor deliverables. Provides technical and analytical guidance to project team. Recommends and takes action to direct the analysis and solutions of problems.

2.2 Project Manager – Intermediate (PMI certification desired)

Description: Under general direction, responsible for all aspects of the development and implementation of assigned projects and provides a single point of contact for those projects. Takes projects from original concept through final implementation. Interfaces with all areas affected by the project including end users, computer services, and client services. Defines project scope and objectives. Develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensures adherence to quality standards and reviews project deliverables. Manages the integration of vendor tasks and tracks and reviews vendor deliverables. Provides technical and analytical guidance to project team. Recommends and takes action to direct the analysis and solutions of problems.

2.3 Project Manager – Associate

Description: Under direct supervision, responsible for assigned aspects of the development and implementation of assigned projects and provides a single point of contact for those aspects. Interfaces with all areas affected by the project including end users, computer services, and client services. Ensures adherence to quality standards and reviews project deliverables. Manages the integration of vendor tasks and tracks and reviews vendor deliverables. Recommends action to direct the analysis and solutions of problems.

2.4 Enterprise Architect

Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Under general direction, has duties of instructing, directing, and checking the work of other project engineers. Responsible for developing strategies for technical IT infrastructures and the completion of assigned engineering projects within budgetary and scheduling guidelines. Leads a group of engineers, analysts, and/or technicians assigned for the duration of a project or may function as ongoing lead within a group of engineers associated with one or more technical areas within the telecom function (such as, but not limited to, network design, engineering,

implementation, or operations/user support). Does not have formal supervisory responsibilities, although may provide input for (project) team member performance appraisals.

2.5 Business Analyst – Functional

Experience/Education: Minimum of 5 years of experience and BA/BS degree
Description: Under general supervision, has duties of instructing, directing, and checking the work of other project engineers. Responsible for the completion of assigned engineering projects within budgetary and scheduling guidelines. Leads a group of engineers, analysts, and/or technicians assigned for the duration of a project or may function as ongoing lead within a group of engineers associated with one or more technical areas within the telecom function (such as, but not limited to, network design, engineering, implementation, or operations/user support). Does not have formal supervisory responsibilities, although may provide input for (project) team member performance appraisals.

2.6 Business Analyst – Technical

Experience/Education: Minimum less than 5 years of experience and BA/BS degree
Description: Under direct supervision, has duties of instructing, directing, and checking the work of other project engineers. Reviews design documents and ensures technical specifications and designs are correct. Responsible for the completion of assigned engineering projects within budgetary and scheduling guidelines. Leads a group of engineers, analysts, and/or technicians assigned for the duration of a project or may function as ongoing lead within a group of engineers associated with one or more technical areas within the telecom function (such as, but not limited to, network design, engineering, implementation, or operations/user support). Does not have formal supervisory responsibilities, although may provide input for (project) team member performance appraisals.

2.7 Project Administrator

Experience/Education: Minimum of 5 years of experience and BA/BS degree
Description: Under general direction, interpret and compose complex correspondences and presentations to include charts and diagrams directly supporting the DoD Enterprise infrastructure and infostructure IT goals and projects. Accountable for financial budgeting and tracking project KPI's and goals. Apply effective networking skills to carry out job responsibilities. Gather pertinent information from a variety of sources to perform duties. Resolve administrative issues/problems that arise and recommend process improvements. Ensure timely completion of multiple, simultaneous, independent events and projects of moderate complexity. Coordinate multiple work projects and other responsibilities (i.e. Training/status reporting, etc.). Some duties may be considered special assignments particular to either the department or manager. Prepare reports and correspondence from information gathered to support the entire effort. Interprets and applies standard policies and procedures to respond to complex inquiries, to resolve issues.

2.8 Project Administrator – Associate

Description: Under immediate supervision, interpret and compose complex correspondences and presentations to include charts and diagrams directly supporting the DoD Enterprise infrastructure and infostructure IT goals and projects. Apply effective networking skills to carry

out job responsibilities. Gather pertinent information from a variety of sources to perform duties. Resolve administrative issues/problems that arise and recommend process improvements. Ensure timely completion of multiple, simultaneous, independent events and projects of moderate complexity. Coordinate multiple work projects and other responsibilities (i.e. Training/status reporting, etc.). Some duties may be considered special assignments particular to either the department or manager. Prepare reports and correspondence from information gathered to support the entire effort. Interprets and applies standard policies and procedures to respond to complex inquiries, to resolve issues.

2.9 Facility Staff Support – Senior

Description: Under indirect supervision, assists in developing & monitoring assigned department budget and risk management efforts directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Can include tasks associated with receiving, distributing, or shipping of materials. Must possess strategic planning skills and have a thorough understanding of internal & external compliance policies. Accurately completes paperwork or system transactions applicable to function, such as documentation of material movement (i.e., Receipt, Shop Order, and Packing Lists). Ability to organize, plan & schedule work with minimal supervision.

2.10 Facility Staff Support – Intermediate

Description: Under general direction, assists in developing & monitoring assigned department budget and risk management efforts directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Can include tasks associated with receiving, distributing, or shipping of materials. Must possess strategic planning skills and have a thorough understanding of internal & external compliance policies. Accurately completes paperwork or system transactions applicable to function, such as documentation of material movement (i.e., Receipt, Shop Order, and Packing Lists). Ability to organize, plan & schedule work with minimal supervision.

2.11 Facility Staff Support – Associate

Description: Under immediate supervision, assists in developing & monitoring assigned department budget and risk management efforts directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Can include tasks associated with receiving, distributing, or shipping of materials. Must possess strategic planning skills and have a thorough understanding of internal & external compliance policies. Accurately completes paperwork or system transactions applicable to function, such as documentation of material movement (i.e., Receipt, Shop Order, and Packing Lists). Ability to organize, plan & schedule work with minimal supervision.

3. Quality Assurance

SOC No. 17-2199, Engineer, all others
SOC No. 13-1111, Program, Management Analyst
SOC No. 15-2041, Statistical Analyst
SOC No. 15-1121, Information Systems Analyst

3.1 Quality Assurance Manager – Senior (Lean Six Sigma Black Belt Certification Required)

Description: Under general direction, carries out procedures to ensure that all information systems products and services meet organization standards and end-user requirements. Performs and leads tests of software to ensure proper operation and freedom from defects. May create test data for applications. Documents and works to resolve all complex problems. Reports progress on problem resolution to management. Devises improvements to current procedures and develops models of possible future configurations. Acts as information resource about assigned areas to technical writers and other Quality Assurance Analysts. Performs complex workflow analysis and recommends quality improvements.

3.2 Quality Assurance Analyst – Intermediate (Lean Six Sigma Green Belt Certification Required)

Description: Under general supervision, carries out procedures to ensure that all information systems products and services meet minimum organization standards and end-user requirements. Thoroughly tests software to ensure proper operation and freedom from defects. Documents and works to resolve all problems. Reports progress on problem resolution to management. Devises improvements to current procedures and develops models of possible future configurations. Performs workflow analysis and recommends quality improvements.

3.3 Quality Assurance Analyst – Associate

Description: Under direct supervision, carries out procedures to ensure that all information systems products and services meet organization standards and end-user requirements. Assists in the testing of software to ensure proper operation and freedom from defects. Documents and works to resolve basic problems. Reports progress on problem resolution to management. This position is staffed by beginners who have had sufficient educational background and/or experience to qualify them to start in quality assurance analysis.

3.4 Telecommunications Specialist – Senior

Description: Provides installation and operational support of voice and data communications hardware and software systems. Designs, develops, implements, tests, debugs, and maintains communications systems. Performs configuration of operating system and security patches for host and distributed systems, and implements incident response procedures during incidents of a network or host security breach. May provide leadership and direction to a team of specialists for these functions. Reviews customer requirements and makes recommendations for changes to existing technical architecture. Complies with prescribed customer, industry and agency standards.

3.5 Telecommunications Specialist – Intermediate

Description: Provides installation and operational support of voice and data communications hardware and software systems. Designs, develops, implements, tests, debugs, and maintains communications systems. Performs configuration of operating system and security patches for host and distributed systems, and implements incident response procedures during incidents of a network or host security breach. Complies with prescribed customer, industry and agency standards.

3.6 Telecommunications Specialist – Associate

Description: Assists in providing installation and operational support of voice and data communications hardware and software systems. Participates in design, development, implementation, test, debugging, and maintaining communications systems. Complies with prescribed customer, industry and agency standards.

4. IT Systems Architecture

SOC No. 15-1121, Systems Architect
SOC No. 15-1143, Computer Network Architect
SOC No. 15-1133, Computer System Software Architect, Software Systems Developer, Embedded Systems Software Developer, Software Systems Engineer
SOC No. 15-1132, Software Applications Architect, Software Applications Developer, Software Applications Engineer
SOC No. 15-1130, Software Developers and Programmers
SOC No. 15-1131, System Programmers
SOC No. 17-2199, Engineer, all others

4.1 Chief Enterprise Architect

Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Leads and directs large teams with diverse functional and technical disciplines to include enterprise architects, systems engineers, business analysts, and network engineers.
Works directly with senior executives of the enterprise to consult, coach, and advise on strategy, business alignment, enterprise architecture, information technology solutions, and the associated impact on the organization and its stakeholders. Coordinates resolution of highly complex problems and tasks, selling new ideas and concepts in support of operational goals and objectives. Provides technical and analytical guidance to enterprise architecture team. Integrates and translates complex concepts into tactical action plans. Directs high-level enterprise architecture analysis, evaluation, design, integration, documentation, and development. Has a deep understanding of DoD business transformation and processes, DoD organizational structure, experience in developing briefings and responses to GAO, OMB, and executives within the department, and coordinated and developed Business Enterprise Architecture (BEA) Compliance Guidance criteria and various BEA evolution strategies. Possesses extensive knowledge of the DoDAF, the DoD Net-Centric and Data Strategies, the DoD Information Assurance Guidance, and the DoD Federation Strategy, and has had hands-on experience with the BEA and Enterprise Transition Plan, Service Oriented Architecture, and the Business Mission Area Federation Strategy and Roadmap.

4.2 Lead Enterprise Architect

Experience/Education: Minimum of 10 years of experience and a MA/MS degree
Description: Responsible for all aspects of the development and maintenance of assigned enterprise architecture project and takes project from planning through final delivery. Interfaces with all areas affected by the project including end users, computer services, and client services. Defines project scope and objectives and develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for

project tracking and analysis. Leads a group of engineers, architects, and analysts and ensures adherence to quality standards and reviews enterprise architecture deliverables. Provides technical and analytical guidance to enterprise architecture team. Directs and participates in high-level enterprise architecture analysis, evaluation, design, integration, documentation, and development. Applies high-level business and technical principles and methods to very difficult technical problems to arrive at creative engineering solutions. Recommends and takes action to direct the analysis and solutions of problems. Has a deep understanding of DoD business transformation and processes, DoD organizational structure, and experience in developing briefings and responses to GAO, OMB, and executives within the department. Possesses extensive knowledge of and hands-on experience with the DoDAF, the Business Enterprise Architecture and Enterprise Transition Plan, Service Oriented Architecture, and the Business Mission Area Federation Strategy and Roadmap. Lead the development of the BEA and updates to the BEA Development Methodology and Architecture Planning Guide. Familiar with the Core Business Mission and Business Enterprise Priority architecture liaisons.

4.3 Senior IT Systems Solution Architect

Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Participates in the design, creation, and maintenance of computerized databases. Responsible for the quality control and auditing of Telelogic System Architect (SA) databases to ensure accurate and appropriate use of data. Consults with and advises users on access, works directly with users to resolve data conflicts and inappropriate data usage, and directs the maintenance and use of the enterprise architecture encyclopedia. Consults with SA programming personnel to resolve system performance issues. Responsible for the installation, maintenance, configuration, and integrity of SA. Implements application enhancements that will improve the reliability and performance of the application. Works with network engineers to schedule installations and upgrades and maintains them in accordance with established IT policies and procedures. Responsible for file maintenance, control, and product support and facilitates change control, problem management, and communication among architects, engineers, and analysts. Establishes and enforces processes to ensure a consistent, well-managed, and well-integrated application infrastructure. Develops appropriate application and process documentation. Expertise with the BEA SA repository and its internal structure, Visual Basic, SA macros, Windows XT server, SQL server, and DoDAF modeling methodology. Has a deep understanding of Business Transformation Agency (BTA) and enterprise architecture's role in it, the BTA organizational structure, and experience in coordinating delivery and publishing of the Business Enterprise Architecture (BEA).

4.4 Client/Server Network Architect

Experience/Education: Minimum of 10 years of experience and a MA/MS degree
Description: Top-level technical expert responsible for design and development of a client/server environment. Develops strategy of client/server system and the design infrastructure necessary to support that strategy. Advises on selection of technological purchases with regards to processing, data storage, data access, and applications development. Sets standards for the client/server relational database structure for the organization (SQL, ORACLE, SYBASE, etc.). Advises of feasibility of potential future projects to management.

4.5 Software Architect

Experience/Education: Minimum of 10 years of experience and a MA/MS degree

Description: Works independently designing and developing new software products or major enhancements to existing software. May lead a large development team in design of highly complex software systems. Acts as highest-level technical expert, addressing problems of systems integration, compatibility, and multiple platforms. Responsible for project completion. Performs feasibility analysis on potential future projects to management.

4.6 Systems Engineer – Senior

Description: Under general direction, performs high-level systems analysis, evaluation, design, integration, documentation, and implementation of very complex application that require a thorough knowledge of administrative and technical skills. Directs and participates in all phases of system development with emphasis on planning, analysis, evaluation, integration, testing and acceptance phases (IV&V and DT&E). Applies higher-level business or technical principles and methods to very difficult technical problems to arrive at automated engineering solution. Designs and prepares technical reports and related documentation, and makes charts and graphs to record results. Prepare and deliver presentations and briefings as required by the Task Order. May be required to serve as Task Leader. Responsible for ensuring the quality and services delivered for particular task(s) for which this skill is performing the Task Leader position.

4.7 Systems Engineer – Intermediate

Description: Under general supervision, performs high-level systems analysis, evaluation, design, integration, documentation, and implementation of very complex application that require a thorough knowledge of administrative and technical skills. Directs and participates in all phases of system development with emphasis on planning, analysis, evaluation, integration, testing and acceptance phases (IV&V and DT&E). Applies higher-level business or technical principles and methods to very difficult technical problems to arrive at automated engineering solution.

4.8 Systems Engineer – Associate

Description: Under direct supervision assists in performing systems analysis, evaluation, design, integration, documentation, and implementation of applications that require comprehensive knowledge and technical skills.

4.9 Network Engineer – Senior

Description: Under general direction, installs, configures, and supports an organization's local area network (LAN), wide area network (WAN), Agency Internet Network (AIN), Intranet and Internet, and other data communications systems or a segment of a network system; maintains network hardware and software; monitors network to ensure network availability to all system users and perform necessary maintenance to support network availability; may supervise other network support and client server specialists and plan, coordinate, and implement network security measures; and will provide leadership/mentorship to junior & mid-level network engineers. Oversees network control center; provides support to projects that involve networks; performs a full range of complex network designs encompassing multiple technologies within a single network; evaluates new network technologies and makes recommendations to project managers regarding the integration of these technologies into the existing network; plans new configurations for integration into the network, using knowledge of the performance characteristics of the systems being added to the network and the specifications for network interfaces to insure effective integration and optimal network performance; ensures that adequate

and appropriate planning is provided for hardware and communications facilities to develop and implement methodologies for analysis, installation and support of voice communications systems; and provides support in the translation of business requirements into telecommunications (e.g., LAN, MAN, WAN, Voice, and Video) requirements, designs, and orders. The overarching INFOSEC and COMSEC security requirements for the Agency network add to the complexity of these positions.

4.10 Network Engineer – Intermediate

Description: Will complete tasks assigned by Senior Network Engineer. Under general supervision will install, configure, and support an organization's local area network (LAN), wide area network (WAN), Agency Internet Network (AIN), Intranet and Internet, and other data communications systems or a segment of a network system; maintain network hardware and software; monitors network to ensure network availability to all system users and perform necessary maintenance to support network availability; provides support to projects that involve networks; and provides support in the translation of business requirements into telecommunications (e.g., LAN, MAN, WAN, Voice, and Video) requirements, designs, and orders.

4.11 Network Engineer – Associate

Description: Will complete tasks assigned by Senior Network Engineer. Under direct supervision will install, configure, and support an organization's local area network (LAN), wide area network (WAN), Agency Internet Network (AIN), Intranet and Internet, and other data communications systems or a segment of a network system; maintain network hardware and software; monitors network to ensure network availability to all system users and perform necessary maintenance to support network availability; provides support to projects that involve networks; and provides support in the translation of business requirements into telecommunications (e.g., LAN, MAN, WAN, Voice, and Video) requirements, designs, and orders.

4.12 Managed System Engineer – Senior

Description: Under general direction, performs duties such as site surveys, architecture design, system evaluation, system analysis, and infrastructure assessment. The managed system engineer shall perform duties on tasks that require expertise in system/processor architecture, wired for management baseline, desktop management interface, SNMP, client/server architecture, operating systems, software applications, network protocols, routers, switches, remote access servers, and firewalls.

4.13 Managed Systems Engineer – Intermediate

Description: Under general supervision, performs duties such as site surveys, architecture design, system evaluation, system analysis, and infrastructure assessment. Performs duties on tasks that require expertise in system/processor architecture, wired for management baseline, desktop management interface, SNMP, client/server architecture, operating systems, software applications, network protocols, routers, switches, remote access servers, and firewalls.

4.14 Managed Systems Engineer – Associate

Description: Under direct supervision, assists in site surveys, architecture design, system evaluation, system analysis, and infrastructure assessment.

4.15 IT Functional Area Expert

Experience/Education: Minimum of 5 years of experience and BS degree
Description: Recognized for strong expertise in industry issues and trends. Utilizes functional area expertise gained through direct industry experience to assess the operational and functional baseline of an organization and its organizational components. Works with senior managers and executives to provide industry vision and strategic direction with regard to their enterprise. Guides the determination of information technology inadequacies and/or deficiencies that affect the functional area's ability to support/meet organizational goals. Generates functional area strategies for enhanced IT operations in a cross-functional area mode throughout the organization. Participates in account strategy sessions, strategic assessments, and design reviews to validate enterprise approach and associated work products. Provides guidance and direction to other professionals, acts in a consulting and/or advisory capacity; coordinates resolution of highly complex problems and tasks, and possesses ability to meet and operate under deadlines.

4.16 IT Subject Matter Expert

Experience/Education: Minimum of 5 years of experience and a BA/BS or MA/MS degree
Description: Executes tasks and projects relevant to subject matter. Reduces issues to practical recommended options. Explains recommendation to decision-makers in terms that permit decisions. Performs studies and analyses on subjects within the technical scope of work. Develops requirements from a project's inception to its conclusion for a particular IT subject matter area (i.e., simple to complex systems). Assists other project members with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; communications protocols; risk management/electronic analysis; software; lifecycle management; software development methodologies; and modeling and simulation. Recognized at the industry level in a technical field or specialized engineering or technology area and is proficient in relevant engineering principles and practices. Applies experience, skills, and expert knowledge within an engineering discipline to complex assignments. Generates unique concepts as evidenced by synthesis of new products or processes. Creates or uses engineering/scientific tools to solve technical problems. Utilizes and develops tools, techniques, processes, and/or facilities such as state-of-the-art simulation environments, laboratories, and test facilities. Provides leadership for engineering activities in a specialized engineering or technology subject area. Serves as a major contributor to technical planning process and for providing technical management and guidance.

5. Application Systems

SOC No. 15-1130, Software Developers and Programmers
SOC No. 15-1131, System Programmers, Computer Language Coders
SOC No. 15-1132, Software Applications Developer, Software Applications Engineer
SOC No. 15-1133, Software Systems Developer, Embedded Systems Software Developer, Software Systems Engineer
SOC No. 15-1121, Information Systems Analyst
SOC No. 15-2031, Process, Procedure Analyst
SOC No. 17-2199, Engineer, all others

5.1 Applications Systems Analyst – Senior
Description: Under general direction, formulates/defines system scope and objectives based on user needs. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time and form of desired results. Prepares detailed specifications from which programs will be written. Analyzes and revises existing system logic difficulties and documentation as necessary. Competent to work at the highest technical level of all phases of applications systems analysis activities. May use Computer-aided software engineering (CASE) tools.

5.2 Applications Systems Analyst – Intermediate
Description: Under general supervision, formulates and defines system scope and objectives through research and fact-finding to develop or modify moderately complex information systems. Prepares detailed specifications from which programs will be written. Analyzes and revises existing system logic difficulties and documentation as necessary. Competent to work on most phases of applications systems analysis activities, but requires instruction and guidance in other phases. May use CASE tools.

5.3 Applications Systems Analyst – Associate
Description: Under immediate supervision, assists in research and fact-finding to develop or modify information systems. Assists in preparing detailed specifications from which programs will be written. Analyzes and revises existing system logic difficulties and documentation as necessary. May use CASE tools.

5.4 Software Engineer – Senior
Description: Under general direction, conducts or participates in multidisciplinary research and collaborates with equipment designers and/or hardware engineers in the planning, design, development, and utilization of electronic data processing systems software. Determines computer user needs; advises hardware designers on machine characteristics that affect software systems such as storage capacity, processing speed, and input/output requirements; designs and develops compilers and assemblers, utility programs, and operating systems.

5.5 Software Engineer – Intermediate
Description: Under general supervision, conducts or participates in multidisciplinary research and collaborates with equipment designers and/or hardware engineers in the planning, design, development, and utilization of electronic data processing systems software. Determines computer user needs; advises hardware designers on machine characteristics that affect software systems such as storage capacity, processing speed, and input/output requirements; designs and develops compilers and assemblers, utility programs, and operating systems.

5.6 Software Engineer – Associate
Description: Under direct supervision, assists in designing and developing compilers and assemblers, utility programs, and operating systems.

5.7 Applications Programmer – Senior
Description: Under general direction, devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time and form of desired

results. Designs, codes, tests, debugs and documents those programs. Competent to work at the highest technical level of all phases of applications programming activities. Note: This position does not perform systems analysis functions.

5.8 Applications Programmer – Intermediate

Description: Under general supervision, modifies moderately complex applications programs from detailed specification. Codes, tests, debugs, and documents and maintains those programs. Competent to work on most phases of applications programming activities, but requires instruction and guidance in phases. Note: This position does not perform systems analysis functions.

5.9 Applications Programmer – Associate

Description: Under immediate supervision, modifies applications programs from detailed specifications. Codes, tests, debugs, documents and maintains those programs. This level is staffed by beginners who have had sufficient educational background and/or experience to qualify them to start in applications programming. Note: This position does not perform systems analysis functions.

5.10 IT Certified Professional – Senior

Description: Under general direction, responsible for the most complex testing and analysis of all elements of the network facilities including: power, software, communications devices, lines, modems and terminals. Monitors and controls the performance and status of the network resources. May function in a lead capacity within the department. Provides guidance and direction for less experienced personnel.

5.11 IT Certified Professional – Intermediate

Description: Under general supervision, responsible for moderately complex tasks typically relating to network monitoring, operations, installation or maintenance. Handles routine network activities and identifies and resolves routine network problems.

5.12 IT Certified Professional – Associate

Description: Under direct supervision, assists in monitoring and responding to technical control facility hardware and software problems utilizing hardware and software testing tools and techniques. May provide LAN server support. May assist installing terminals and associated hardware. Requires knowledge of data scopes, patch panels, modems, concentrators, and associated terminal and network management software.

5.13 DevOps Engineer – Intermediate

Description: A DevOps engineer introduces processes, tools, and methodologies to balance needs throughout the software development life cycle, from coding and deployment, to maintenance and updates.

5.14 DevSecOps Engineer – Intermediate

Description: DevSecOps is short for development, security, and operations. The DevSecOps Engineer automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery.

5.15 Full Stack Developer – Associate

Description: A full-stack developer is a programmer who works within software development and is knowledgeable in both the front end and back end of an application. They work to create a seamless user experience through their diverse skill set. They're also well-versed in databases, server configuration, user interface and more.

5.16 Continuous Integration, Continuous Delivery or Deployment (CI/CD) Engineer – Intermediate

Description: In software engineering, CI/CD or CICD generally refers to the combined practices of continuous integration and either continuous delivery or continuous deployment. CI/CD bridges the gaps between development and operation activities and teams by enforcing automation in building, testing and deployment of applications. Modern day DevOps practices involve continuous development, continuous testing, continuous integration, continuous deployment and continuous monitoring of software applications throughout its development life cycle. The main concepts attributed to CI/CD are continuous integration, continuous delivery, and continuous deployment. Responsible for improving and managing the productivity of technology processes by creating automated workflows to replace the manual ones.

6. Operations and Logistics

SOC No. 11-1071, Logistics Manager
SOC No. 11-3021, Computer and Information Systems Manager
SOC No. 43-9011, Computer Operators
SOC No. 43-5071, Shipping, Receiving, and Expediting Clerks
SOC No. 43-5081, Stock Clerks and Order Fillers
SOC No. 13-1081, Logistician, Logistician Analyst, Logistics Planner, Logistics Specialist

6.1 Seat Management Administrator

Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: The seat management administrator shall perform duties such as configuration management, infrastructure management, asset management, help desk, system analysis, and infrastructure assessment. The seat management administrator shall perform duties on tasks that require expertise in system/processor architecture, wired for management baseline, desktop management interface, SNMP, client/server architecture, operating systems, software applications, network protocols, routers, switches, remote access servers, and firewalls.

6.2 Configuration Management (CM) Specialist – Senior

Description: Under general direction, responsible for effectively tracking, logging, categorizing, and maintaining changes made against the accepted Army baseline(s) standards. Develops, distributes, and tracks all change packages resulting from approved Configuration Control Board action. Trains personnel by conducting workshops and seminars on the proper methodology to maintain a proactive CM program. Provides daily support and direction to staff as to change status requirements, deadlines, and problems.

6.3 Configuration Management (CM) Specialist – Intermediate

Description: Under immediate supervision, responsible for effectively tracking, logging, categorizing, and maintaining changes made against the accepted Army baseline(s) standards.

Develops, distributes, and tracks all change packages resulting from approved Configuration Control Board action.

6.4 Configuration Management (CM) Specialist – Associate

Description: Under immediate supervision, distributes and tracks all change packages resulting from approved Configuration Control Board action. Provides daily support to staff as to change status requirements, deadlines, and problems.

6.5 Computer Operator – Senior

Description: Under general direction, monitors and controls one or more servers by operating the central console or on-line terminals. Studies program operating instruction sheets to determine equipment setup and run operations. Continuously observes the operation of the console panel, storage devices, and printers to monitor the system and determine the point of equipment or program failure. Manipulates controls in accordance with standard procedures to rearrange sequence of job steps to continue operations when individual units of the system malfunction. Confers with software systems engineering or applications programming personnel in the event errors require a change of instructions or sequence of operations. Maintains operating records such as machine performance and production reports. Competent to work at the highest level of all computer operations phases.

6.6 Computer Operator – Intermediate

Description: Under general supervision, monitors and controls a computer by operating the central console or on-line terminals. May operate auxiliary equipment directly associated with the computer. May maintain records regarding output units and supply inventories. May assist in manipulating controls to rearrange sequence of job steps to continue operations when individual units of the system malfunction. Competent to work on most phases of computer operations, but still may require some instruction and guidance for other phases.

6.7 Computer Operator – Associate

Description: Under immediate supervision, assists in performing routine tasks associated with operating a computer in accordance with detailed instructions.

6.8 Distribution Operations Specialist – Senior

Description: Under indirect supervision, responsible for review/develop/modify/test procedures and systems requirements to manage property book requirements directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Train internal and external customers regarding procedures/processes and software applications. Conduct internal audits and development/review of corrective action plans. Negotiate supplier agreements and service contracts as required by job. Have knowledge of capital procurement processes. Perform duties and responsibilities as the lead on process improvement teams. Coordinate workflow and material movement to meet program and customer delivery requirements.

6.9 Distribution Operations Specialist – Intermediate

Description: Under general direction, responsible for review/develop/modify/test procedures and systems requirements to manage property book requirements directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Train internal and external customers regarding procedures/processes and software applications. Conduct internal audits and

development/review of corrective action plans. Negotiate supplier agreements and service contracts as required by job. Have knowledge of capital procurement processes. Perform duties and responsibilities as the lead on process improvement teams. Coordinate workflow and material movement to meet program and customer delivery requirements.

6.10 Distribution Operations Specialist – Associate

Description: Under immediate supervision, responsible for review/develop/modify/test procedures and systems requirements to manage property book requirements directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Train internal and external customers regarding procedures/processes and software applications. Conduct internal audits and development/review of corrective action plans. Negotiate supplier agreements and service contracts as required by job. Have knowledge of capital procurement processes. Perform duties and responsibilities as the lead on process improvement teams. Coordinate workflow and material movement to meet program and customer delivery requirements.

7. Cybersecurity

SOC No. 15-1142, Network Security Administrator
SOC No. 15-1141, Database Security Administrator
SOC No. 11-3021, Computer and Information Systems Manager
SOC No. 15-1122, Computer Security Specialist
SOC No. 15-1121, Computer Systems Analyst
SOC No. 15-1120, Computer and Information Analyst
SOC No. 17-2061, Computer Hardware Engineer
SOC No. 15-1133, Software Systems Engineer
SOC No. 17-2199, Engineer, all others

7.1 Information Assurance Engineer – Senior

Description: Under general direction, responsible for all activities relating to information assurance procedures and systems. Develops information systems assurance programs and control guidelines. Confers with and advises subordinates on administrative policies and procedures and resolving technical problems, priorities, and methods. Consults with and advises other sections regarding internal controls and security procedures. Prepares activity and progress reports relating to the information systems audit function.

7.2 Information Assurance Engineer – Intermediate

Description: Under general supervision, develops information systems assurance programs and control guidelines, assists in resolving technical problems, priorities, and methods.

7.3 Information Assurance Engineer – Associate

Description: Under general supervision, audits new and existing information systems applications to ensure that appropriate controls exist, that processing is efficient and accurate, and that systems procedures are in compliance with corporate standards

7.4 Information Systems Auditor – Senior

Description: Under general direction, audits the most complex new and existing information

systems applications to ensure that appropriate controls exist, that processing is efficient and accurate, and that information systems procedures are in compliance with corporate standards. Competent to work at the highest level of all phases of information systems auditing.

7.5 Information Systems Auditor – Intermediate

Description: Under general supervision, audits moderately complex new and existing information systems applications to ensure that appropriate controls exist, that processing is efficient and accurate, and that systems and procedures are in compliance with corporate standards. Competent to work on most phases of information systems auditing.

7.6 Information Systems Auditor – Associate

Description: Under direct supervision, carries out routine phases of the systems audit function. Assists in the auditing of new and existing information systems applications to ensure that appropriate controls exist, that processing is efficient and accurate, and that systems and procedures are in compliance with corporate standards. Staffed by skilled employees who have had sufficient educational background and/or experience in information systems auditing.

7.7 Data Security Analyst – Senior

Description: Under general direction, performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. May require familiarity with domain structures, user authentication, and digital signatures. Conducts accurate evaluation of the level of security required. May require understanding of firewall theory and configuration. Must be able to weigh business needs against security concerns and articulate issues to management.

7.8 Data Security Analyst – Intermediate

Description: Under general supervision, performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. May require familiarity with domain structures, user authentication, and digital signatures. Conducts accurate evaluation of the level of security required. May require understanding of firewall theory and configuration. Frequently reports to a Senior Data Security Analyst.

7.9 Data Security Analyst – Associate

Description: Under direct supervision, performs all procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports. Frequently reports to an Intermediate Data Security Analyst.

7.10 Disaster Recovery/COOP/Contingency Administrator

Experience/Education: Minimum of 10 years of experience and MS/PhD degree
Description: Responsible for preparing contingency plans for system software, hardware, and applications for the organization. Implements procedures to ensure business applications continue to function through disruptive incidents within an organization. Develops and maintains various security controls to protect technology assets from internal or inadvertent modification, disclosure or destruction. Provides reports to supervisors regarding effectiveness of data security and make recommendations for the adoption of new procedures. Oversees and facilitates the preparation of an organization-wide business resumption plan. Responsible for ensuring the business resumption plan adequately addresses the organization's requirements and established timeframes. Responsible for day-to-day security administration of the organization's data systems and data networks including systems access administration.

7.11 Information Security Specialist – Senior
Description: Under general direction, uses current information security technology disciplines and practices to ensure the confidentiality, integrity, and availability of corporate information assets in accordance with established standards and procedures. Develops and maintains knowledgebase on changing regulatory, threat, and technology landscapes to continually develop or maintain security policies and standards, and ensure compliance throughout the organization.

7.12 Information Security Specialist – Intermediate
Description: Under general supervision, uses current information security technology disciplines and practices to ensure the confidentiality, integrity, and availability of corporate information assets in accordance with established standards and procedures. Develops and maintains knowledgebase on changing regulatory, threat, and technology landscapes to continually develop or maintain security policies and standards, and ensure compliance throughout the organization.

7.13 Information Security Specialist – Associate
Description: Under direct supervision, assists in developing and maintaining knowledgebase on changing regulatory, threat, and technology landscapes to continually develop or maintain security policies and standards, and ensure compliance throughout the organization.

7.14 IA Policy and Compliance Certified Professional – Senior
Description: Under general direction, performs and leads support of Certification and Accreditation (C&A) or other IA/CND Compliance and Auditing processes and inspections for all enterprise systems and networks; ensures validity and accuracy review of all associated documentation. Leads and performs compliance reviews of computer security plans, performs risk assessments, and validates and performs security test evaluations and audits. Analyzes and defines security requirements for information protection for enterprise systems and networks. Assists in the development of security policies. Analyzes the sensitivity of information and performs vulnerability and risk assessments on the basis of defined sensitivity and information flow. Professionally certified as Technical Level III as defined by DODI 8570 is a requirement.

7.15 IA Policy and Compliance Certified Professional – Intermediate
Description: Under general supervision, performs Certification and Accreditation (C&A) or other IA/CND Compliance and Auditing processes and inspections for all enterprise systems and networks; ensures validity and accuracy review of all associated documentation. Performs compliance reviews of computer security plans, performs risk assessments, and performs

security test evaluations and audits. Analyzes security requirements for information protection for enterprise systems and networks. Assists in the development of security policies. Analyzes the sensitivity of information and performs vulnerability and risk assessments on the basis of defined sensitivity and information flow. Professionally certified as Technical Level II as defined by DODI 8570 is a requirement.

7.16 IA Policy and Compliance Certified Professional – Associate
Description: Under general supervision, assists in the support of Certification and Accreditation (C&A) or other IA/CND Compliance and Auditing processes and inspections for all enterprise systems and networks; assists in the development of all associated documentation. Assists in the compliance reviews of computer security plans, performs risk assessments, and assists in security test evaluations and audits. Analyzes security requirements for information protection for enterprise systems and networks. Professionally certified as Technical Level I as defined by DODI 8570 is a requirement.

7.17 Cyber Operations Research Analyst – Senior
Description: Under general direction, leads and participates in analysis of actual and predictable interacting operational activities of business to obtain a quantitative, rational basis for decision making through the application of logic and scientific or economic disciplines and techniques. Ability to devise modeling and measuring techniques; utilizes mathematics, statistical methods, engineering methods, operational mathematics techniques (linear programming, game theory, probability theory, symbolic language, etc.), and other principles and laws of scientific and economic disciplines. Ability to demonstrate a complete understanding and wide application of technical principles, theories, and concepts within the Cyber Research field and provide consultation to technical solutions over a wide range of complex difficult problems in which proposed solutions are imaginative, thorough, practicable, and consistent with organization objectives. Professionally certified as Technical Level III as defined by DODI 8570 is a requirement.

7.18 Cyber Operations Research Analyst – Intermediate
Description: Under general supervision, participates in analysis of actual and predictable interacting operational activities of business to obtain a quantitative, rational basis for decision making through the application of logic and scientific or economic disciplines and techniques. Assists in devising models and measuring techniques; utilizes mathematics, statistical methods, engineering methods, operational mathematics techniques (linear programming, game theory, probability theory, symbolic language, etc.), and other principles and laws of scientific and economic disciplines. Ability to demonstrate a thorough understanding and ability to apply technical principles, theories, and concepts within the Cyber Research field and provide consultation to technical solutions over a wide range of complex difficult problems in which proposed solutions are imaginative, thorough, practicable, and consistent with organization objectives. Professionally certified as Technical Level II as defined by DODI 8570 is a requirement.

7.19 Cyber Operations Research Analyst – Associate
Description: Under general supervision, assists in analysis of actual and predictable interacting operational activities of business to obtain a quantitative, rational basis for decision making through the application of logic and scientific or economic disciplines and techniques. Assists

with devising models and measuring techniques; utilizes mathematics, statistical methods, engineering methods, operational mathematics techniques (linear programming, game theory, probability theory, symbolic language, etc.), and other principles and laws of scientific and economic disciplines. Ability to demonstrate an understanding and ability to apply technical principles, theories, and concepts within the Cyber Research field and assists in providing consultation to technical solutions over a wide range of complex difficult problems in which proposed solutions are imaginative, thorough, practicable, and consistent with organization objectives. Professionally certified as Technical Level I as defined by DODI 8570 is a requirement.

7.20 Cyber Operations Malware Analyst – Senior

Description: Under general direction, leads and participates in the evaluation and analysis of complex malicious code through the utilization of tools, including dissemblers, debuggers, hex editors, un-packers, virtual machines, and network sniffers. Responsible for providing findings in a technical report with details of the malware, identification parameters, advanced capabilities, and mitigation strategies. Conducts research in the area of malicious software, vulnerabilities, and exploitation tactics. Requires experience with application security, network security, reverse engineering, or malware. Requires strong knowledge of worms, viruses, Trojans, rootkits, botnets, Windows internals, and the Win32 API. Extensive experience required in programming (assembly and web) and system analysis with various tools, including IDA Pro, Ollydbg, PCAP tools, or TCP Dump. Professionally certified, within a Computer Network Defense (CND) discipline, as Technical Level III as defined by DODI 8570 is a requirement.

7.21 Cyber Operations Malware Analyst – Intermediate

Description: Under general supervision, participates in the evaluation and analysis of complex malicious code through the utilization of tools, including dissemblers, debuggers, hex editors, un-packers, virtual machines, and network sniffers. Responsible for providing findings in a technical report with details of the malware, identification parameters, advanced capabilities, and mitigation strategies. Conducts research in the area of malicious software, vulnerabilities, and exploitation tactics. Requires experience with application security, network security, reverse engineering, or malware. Requires thorough knowledge of worms, viruses, Trojans, rootkits, botnets, Windows internals, and the Win32 API. Additional experience required in programming (assembly and web) and system analysis with various tools, including IDA Pro, Ollydbg, PCAP tools, or TCP Dump. Professionally certified, within a CND discipline, as Technical Level II as defined by DODI 8570 is a requirement.

7.22 Cyber Operations Malware Analyst – Associate

Description: Under general supervision, assists in the evaluation and analysis of complex malicious code through the utilization of tools, including dissemblers, debuggers, hex editors, un-packers, virtual machines, and network sniffers. Assists with providing findings in a technical report with details of the malware, identification parameters, advanced capabilities, and mitigation strategies. Provides research assistance in the area of malicious software, vulnerabilities, and exploitation tactics. Requires experience with application security, network security, reverse engineering, or malware. Requires knowledge of worms, viruses, Trojans, rootkits, botnets, Windows internals, and the Win32 API. Additional experience required in programming (assembly and web) and system analysis with various tools, including IDA Pro, Ollydbg, PCAP tools, or TCP Dump. Professionally certified, within a CND discipline, as

Technical Level I as defined by DODI 8570 is a requirement.

7.23 Cyber Watch Operations Certified Analyst – Senior

Description: Under general direction, leads security event monitoring and correlation within a tiered Security Operations Center. Proven experience and ability to leverage CND analyst toolsets to detect and respond to IT security incidents. Ability to implement standard procedures for incident response interfacing with Information Security Officer and IT staff. Conducts research and document threats and their behavior to include monitoring external CSIRTs/CERTs. Provide recommendations to threat mitigation strategies. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Perform routine event reporting over time including trend reporting and analysis. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on design/Implementation/Administration role. Demonstrates in-depth knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection. Professionally certified, within a CND discipline, as Technical Level III as defined by DODI 8570 is a requirement.

7.24 Cyber Watch Operations Certified Analyst – Intermediate

Description: Under general supervision, participates in security event monitoring and correlation within a tiered Security Operations Center. Proven experience and ability to leverage CND analyst toolsets to detect and respond to IT security incidents. Conducts research and document threats and their behavior to include monitoring external CSIRTs/CERTs. Assist in providing recommendations to threat mitigation strategies. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Perform routine event reporting over time including trend reporting and analysis. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on Implementation or Administration role. Demonstrates thorough knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection. Professionally certified, within a CND discipline, as Technical Level II as defined by DODI 8570 is a requirement.

7.25 Cyber Watch Operations Certified Analyst – Associate

Description: Under general supervision, assists with security event monitoring, correlation, and daily event reporting within a tiered Security Operations Center. Experience with CND analyst toolsets to detect and respond to IT security incidents. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on Administration role. Demonstrates knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection. Professionally certified, within a CND discipline, as Technical Level I as defined by DODI 8570 is a requirement.

7.26 Cyber Security Architect (Alternate job titles: Cyber Security Systems Designer, IT Security Architect) - Intermediate

Description: Cyber Security Architects are responsible for the overall maintenance of an organization's information technology security systems and protocols. They design and implement security measures for hardware, software, and network platforms to ensure protection

from cyber-attacks and any other possible harmful intrusions that could compromise or damage an organization's data and network infrastructure. These architects assess existing cybersecurity systems and protocols and design and implement upgrades to existing measures as well as implementing new procedures.

8. System Administration

SOC No. 15-1142, Network Administrator
SOC No. 15-1141, Database Administrator
SOC No. 11-3021, Computer and Information Systems Manager

8.1 Systems Administrator – Senior

Description: Under general direction, responsible for activities related to system administration. Assigns personnel to various projects, directs their activities, and evaluates their work. Ensures long-term requirements of systems operations and administration are included in the overall information systems planning of the organization. Responsible for the installation, maintenance, configuration, and integrity of computer software. Implements operating system enhancements that will improve the reliability and performance of the system.

8.2 Systems Administrator – Intermediate

Description: Under general supervision, responsible for installing, configuring, and maintaining operating system workstations and servers, including web servers, in support of business processing requirements. Performs software installations and upgrades to operating systems and layered software packages. Schedules installations and upgrades and maintains them in accordance with established IT policies and procedures. Monitors and tunes the system to achieve optimum performance levels. Ensures workstation/server data integrity by evaluating, implementing, and managing appropriate software and hardware solutions. Ensures data/media recoverability by implementing a schedule of system backups and database archive operations. Supports media management through internal methods and procedures or through offsite storage and retrieval services. Develops and promotes standard operating procedures. Conducts routine hardware and software audits of workstations and servers to ensure compliance with established standards, policies, and configuration guidelines. Develops and maintains a comprehensive operating system hardware and software configuration database/library of all supporting documentation.

8.3 Systems Administrator – Associate

Description: Under direct supervision, maintains integrity of the operating system environment. Performs system software upgrades including planning and scheduling, testing, and coordination. Performs workstation and server administration setup. Coordinates disk space planning and management. Maintains growth statistics, space forecasts, tape libraries, and software and hardware inventories. Performs data backups and recoveries. Monitors and maintains continuity with system software licensing and maintenance agreements. Provides recommendations regarding hardware and system software planning and budgeting. Maintains production change control schedule and participates in change control.

9. Data Administration

SOC No. 15-1141, Database Administrator, Database Management System Specialist, Database Security Administrator
SOC No. 15-1132, Database Developer
SOC No. 11-3021, Computer and Information Systems Manager

9.1 Database Administrator

Experience/Education: Minimum of 10 years of experience and MS/PhD degree
Description: Participates in the design, creation, and maintenance of computerized databases. Responsible for the quality control and auditing of databases to ensure accurate and appropriate use of data. Works with management to develop database strategies to support organization requirements. Consults with and advises users on access to various databases. Works directly with users to resolve data conflicts and inappropriate data usage. Directs the maintenance and use of the corporate data dictionary.

9.2 Database Analyst/Programmer – Senior

Description: Under general direction, designs, implements and maintains complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Includes maintenance of database dictionaries, overall monitoring of standards and procedures, and integration of systems through database design. Competent to work at the highest level of all phases of database management.

9.3 Database Analyst/Programmer – Intermediate

Description: Under general supervision, designs, implements, and maintains moderately complex databases. Includes maintenance of database dictionaries and integration of systems through database design. Competent to work on most phases of database administration, but may require some instruction and guidance in other phases.

9.4 Database Analyst/Programmer – Associate

Description: Under direct supervision, assists in the implementation and maintenance of databases.

9.5 Advanced Database Analyst/Programmer – Senior

Description: Under general direction, leads and participates in the development and maintenance of Cyber and IA database systems while also offering database development resource to the development team. Required to review and provide technical solutions to projects which may be in different stages of the development life cycle. Requires knowledge and experience with Oracle or MS SQL Server DBMS, SQL Language, Unix/Linux including basic shell commands, data warehousing, report generation, job scheduling and monitoring tools, XML, HTML, open source development, and technical documenting skills (Windows Office/Visio/Cvs, etc.). Advanced Oracle or Microsoft SQL Server certification is required. Professionally certified as Technical Level III as defined by DODI 8570 is a requirement.

9.6 Advanced Database Analyst/Programmer – Intermediate

Description: Under general supervision, participates in the development and maintenance of Cyber and IA database systems while also offering database development resource to the development team. Required to review and provide technical solutions to projects which may be in different stages of the development life cycle. Requires knowledge and experience with Oracle or MS SQL Server DBMS, SQL Language, Unix/Linux including basic shell commands, data warehousing, report generation, job scheduling and monitoring tools, XML, HTML, open source development, and technical documenting skills (Windows Office/Visio/Cvs, etc.). Oracle or Microsoft SQL Server certification is required. Professionally certified as Technical Level II as defined by DODI 8570 is a requirement.

9.7 Advanced Database Analyst/Programmer – Associate

Description: Under general supervision, assists in the development and maintenance of Cyber and IA database systems while also offering database development resource to the development team. Assists with reviews and provides technical solutions to projects which may be in different stages of the development life cycle. Requires knowledge and experience with Oracle or MS SQL Server DBMS, SQL Language, Unix/Linux including basic shell commands, data warehousing, report generation, job scheduling and monitoring tools, XML, HTML, open source development, and technical documenting skills (Windows Office/Visio/Cvs, etc.). Oracle or Microsoft SQL Server certification is required. Professionally certified as Technical Level I as defined by DODI 8570 is a requirement.

9.8 Database Librarian

Experience/Education: Minimum less than 5 years of experience and BS degree
Description: Under general supervision, enters and maintains data dictionary information, data keyword lists, and dictionary forms. Reviews all information to be entered into the dictionary to assure adherence to standards and to ensure that all requirements are met. Maintains current library of each processing system's information recorded in the dictionary.

10. Data Warehousing

SOC No. 15-1141, Database Administrator, Database Management System Specialist, Database Security Administrator
SOC No. 15-1132, Database Developer
SOC No. 11-3021, Computer and Information Systems Manager
SOC No. 43-4171, Information Clerk
SOC No. 43-2021, Information Operator

10.1 Data Warehousing Project Manager

Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Works in a data warehouse environment that includes data design, database architecture, metadata and repository creation. Responsible for leading data warehouse team in development and enhancements of the data warehouse user interface. Establishes user requirements. Creates new standards and procedures related to end user and internal interface development. Works with Data Architect on technical issues and system architecture definition. Translates high-level work plans and converts to detailed assignments for team members. Monitors status of assignments and reviews work for completion/quality.

10.2 Data Architect
Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Works in a data warehouse environment that includes data design, database architecture, metadata and repository creation. Translates business needs into long-term architecture solutions. Defines, designs, and builds dimensional databases. Responsible for developing data warehousing blueprints, evaluating hardware and software platforms, and integrating systems. Evaluates reusability of current data for additional analyses. Conducts data cleaning to rid the system of old, unused, or duplicate data. Reviews object and data models and the metadata repository to structure the data for better management and quicker access.

10.3 Data Warehouse Analyst
Experience/Education: Minimum of 5 years of experience and BA/BS degree
Description: Works in a data warehouse environment that includes data design, database architecture, metadata and repository creation. Reviews data loaded into the data warehouse for accuracy. Responsible for the development, maintenance and support of an enterprise data warehouse system and corresponding data marts. Troubleshoots and tunes existing data warehouse applications. Conducts research into new data warehouse applications and determines viability for adoption. Assists in establishing development standards. Evaluates existing subject areas stored in the data warehouse. Incorporated existing subject areas into an enterprise model. Creates new or enhanced components of the data warehouse.

10.4 Data Warehousing Programmer
Experience/Education: Minimum of 5 years of experience and BA/BS degree
Description: Under general supervision, responsible for product support and maintenance of the data warehouse. Performs data warehouse design and construction. Codes and documents scripts and stored procedures. Designs and implements data strategy methods. Develops appropriate programs and systems documentation. Assists with metadata repository management. Prepares and implements data verification and testing methods for the data warehouse. Creates index and view scripts.

10.5 Data Warehousing Administrator
Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Under general supervision, coordinates the data administration technical function for both data warehouse development and maintenance. Plans and oversees the technical transitions between development, testing, and production phases of the workplace. Facilitates change control, problem management, and communication among data architects, programmers, analysts, and engineers. Establishes and enforces processes to ensure a consistent, well managed, and well-integrated data warehouse infrastructure. Expands and improves data warehouse to include data from all functions of the organization using data manipulation, transformation, and cleansing tools.

11. Help Desk/End User Support

SOC No. 11-3021, Computer and Information Systems Manager
SOC No. 15-1142, Computer Systems Administrator

SOC No. 15-1121, Computer Systems Analyst
SOC No. 15-1120, Computer and Information Analyst
SOC No. 15-1151, Help Desk Technician
SOC No. 15-1152, Computer User Support Specialist, Computer Network Support Specialist

11.1 Help Desk Coordinator
Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Responsible for ensuring the timely process through which problems are controlled, including problem recognition, research, isolation, resolution and follow-up steps. Requires experience and understanding of MIS environment. Is able to resolve less complex problems immediately, while more complex problems are assigned to second level support or supervisor. Typically involves use of problem management database and help desk system. May provide guidance/training for less experienced personnel.

11.2 Help Desk Support Service Specialist – Senior
Description: Under general direction, provides second-tier support to end-users for PC, server, mainframe applications, and hardware. Handles problems that the first-tier of help desk support is unable to resolve. May interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user problems. Maintains currency and highest level of technical skill in field of expertise.

11.3 Help Desk Support Service Specialist – Intermediate
Description: Under general supervision, provides second-tier support to end-users for PC, server, mainframe applications and hardware. Handles problems that the first-tier of help desk support is unable to resolve. May interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user problems. Maintains currency and high level of technical skill in field of expertise. Escalates more complex problems to Senior level.

11.4 Help Desk Support Service Specialist – Associate
Description: Under direct supervision, provides support to end-users for PC, server or mainframe applications, and hardware. May interact with network services, software systems engineering and/or applications development to restore service and/or identify and correct core problems. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user problems. Refers more complex problems to Intermediate and/or Senior level.

11.5 PC Support Manager
Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Responsible for overall personal computer activity. Establishes and implements PC policies, procedures and standards, and ensures their conformance with information systems goals and procedures. Studies and projects PC resource requirements including personnel, software, equipment and facilities, and makes recommendations to management. Maintains currency in new developments and technology. Provides for the training of department staff and

end users. Directs setup and maintenance of library and materials for end user reference and reviews department staff. Ensures that security procedures are implemented and enforced. Provides leadership in the effective use of internal data processing, automated office systems and data communications. May also manage LAN services.

11.6 PC Systems Specialist

Experience/Education: Minimum of 5 years of experience and BA/BS degree
Description: Under general supervision, performs analytical, technical and administrative work in the planning, design and installation of new and existing personal computer systems. Works on moderately complex applications. Confers with end users to determine types of hardware and software required. Writes programs to fulfill requirements or selects appropriate off-the-shelf software and modifies to suit. May maintain or utilize telecommunications protocols. Installs new hardware and maintains existing hardware. Trains end users in use of equipment and software.

11.7 PC Maintenance Technician

Experience/Education: Minimum less than 5 years of experience and BS degree
Description: Under direct supervision, performs general maintenance tasks, troubleshoots and repairs computer systems and peripheral equipment located throughout the organization. Maintains an adequate spare parts inventory of systems, subsystems, and component parts used in repair work. Prepares progress reports for all work performed. Receives work direction from supervisor on work priorities and daily assignments. Frequently reports to a PC Support Manager.

12. Internet/Web Operations

SOC No. 11-3021, Computer and Information Systems Manager
SOC No. 15-1143, Web Designer, Web Developer
SOC No, 15-1134, Internet Developer
SOC No. 15-1122, Internet Security Specialist

12.1 Web Project Manager

Experience/Education: Minimum of 10 years of experience and MS/PhD degree
Description: Responsible for web strategy and operations. Develops business plan and annual budget for website function. Accountable for budget, staff planning, management, and products and service delivery. Oversees operational activities of the website(s) with specific attention aimed at content creation and website maintenance.

12.2 Web Designer – Senior

Description: Under general direction, designs and builds web pages using a variety of graphics software applications, techniques, and tools. Designs and develops user interface features, site animation, and special-effects elements. Contributes to the design group's efforts to enhance the look and feel of the organization's online offerings. Designs the website to support the organization's strategies and goals relative to external communications. Requires understanding of web-based technologies and thorough knowledge of HTML, PhotoShop, Illustrator, and/or other design-related applications.

12.3 Web Designer – Intermediate
Description: Under general supervision, designs and develops user interface features, site animation, and special-effects elements. Contributes to the design group's efforts to enhance the look and feel of the organization's online offerings. Designs the website to support the organization's strategies and goals relative to external communications. Develops applications based on current, new, and future net-based applications. Requires significant graphics and design experience as well as HTML knowledge.

12.4 Web Designer – Associate
Description: Under direct supervision assists in designing and developing user interface features, site animation, and special-effects elements. Assists in designing the website to support the organization's strategies and goals relative to external communications. Requires graphics and design experience as well as HTML knowledge.

12.5 Web Software Developer – Senior
Description: Under general direction, designs, develops, troubleshoots, debugs, and implements software code (such as HTML, CGI, and JavaScript) for a component of the website. Works with graphic designers and other members of a project team to develop the site concept, interface design, and architecture of the website. Responsible for interface implementation. Integrates web applications with backend databases. Deploys large web-based transaction systems using application servers. Researches, tests, builds, and coordinates the integration of new products per production and client requirements. Requires strong navigation and site-design instincts.

12.6 Web Software Developer – Intermediate
Description: Under general supervision, develops, codes, tests, and debugs new software and enhancements to existing web software. Competent to work on fairly complex programs with guidance. Works with technical staff to understand problems with web software and resolve them.

12.7 Web Software Developer – Associate
Description: Under direct supervision, assists in developing, coding, testing, and debugging new software and enhancements to existing web software.

12.8 Web Technical Administrator
Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: In role of onsite administrator, responsible for achieving overall technical integrity of organization's website. Maintains and upgrades hardware and software including website technical architecture related to hardware and telecommunication connectivity. Administers e-mail, chat, and FTP services. Communicates router configuration changes and troubleshoots system errors and bugs. Maintains servers, creates monitoring reports and logs, and ensures functionality of links. Monitors site for acceptable performance and user accessibility. Establishes backups and monitors site security.

12.9 Web Content Administrator
Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Responsible for developing and providing content that will motivate and entertain

users so that they regularly access the website and utilize it as a major source for information and decision-making. Responsible for managing/performing website editorial activities including gathering and researching information that enhances the value of the site. Locates, negotiates, and pursues content. Seeks out customers to gather feedback for website improvement and enhancements. Requires experience in production management, web page design, HTML, and web graphics types and standards.

13. Network Administration/Support

SOC No. 15-1142, Network and Computer System Administrator, Network Coordinator
SOC No. 15-1152, Network Technician, Network Support Technician, Network Diagnostic Support Technician

13.1 Network Administrator – Senior

Description: Under general direction, responsible for the acquisition, installation, maintenance and usage of the company's local area network. Studies contractor products to determine those which best meet company needs; assists in presentation of information to management resulting in purchase and installation of hardware, software, and telecommunication equipment. Manages network performance and maintains network security. Ensures that security procedures are implemented and enforced. Installs all network software. Evaluates, develops and maintains telecommunications systems. Troubleshoots network problems. Establishes and implements network policies, procedures and standards and ensures their conformance with information systems and company's objectives. Trains users on network operation.

13.2 Network Administrator – Intermediate

Description: Under general supervision, responsible for the acquisition, installation, maintenance, and usage of the organization's local area network. Manages network performance and maintains network security. Ensures that security procedures are implemented and enforced. Installs all network software. Evaluates, develops and maintains telecommunications systems. Troubleshoots network problems. Establishes and implements network policies, procedures, and standards and ensures their conformance with information systems and organization objectives. Trains users on network operation. Frequently reports to a PC support manager or Senior Network Administrator.

13.3 Network Administrator – Associate

Description: Under direct supervision, assists in the installation, maintenance, and usage of the organization's local area network. Assists in the establishment of network procedures regarding access methods and time, security validation checks, and documentation. Maintains network software and hardware inventories. Researches software and hardware issues regarding the network. Inform users when there are network problems. Monitors and maintains continuity with software licensing and maintenance agreements. Troubleshoots network problems. Frequently reports to a PC Support Manager or Senior Network Administrator

13.4 Network Support Technician – Senior

Description: Under general direction, monitors and responds to complex technical control facility

hardware and software problems utilizing a variety of hardware and software testing tools and techniques. Provides primary interface with contractor support service groups or provides internal analysis and support to ensure proper escalation during outages or periods of degraded system performance. May provide network server support. Requires extensive knowledge of PC/network communications hardware/software in a multi-protocol environment, and network management software. May function as lead providing guidance and training for less experienced technicians.

13.5 Network Support Technician – Intermediate
Description: Under general supervision, monitors and responds to technical control facility hardware and software problems utilizing hardware and software testing tools and techniques. May interface with contractor support service groups to ensure proper escalation during outages or period of degraded system performance. May assist with installation of terminals and associated hardware. May provide network server support. Requires strong knowledge of PC/Network communications hardware/software, in a multi-protocol environment, and network management software.

13.6 Network Support Technician – Associate
Description: Under direct supervision, assists in monitoring and responding to technical control facility hardware and software problems utilizing hardware and software testing tools and techniques. May provide network server support. May assist with installation of terminals and associated hardware. Requires knowledge of data scopes, patch panels, modems, concentrators, and associated terminals and network management software.

14. Documentation

SOC No. 27-3041, Technical Editor
SOC No. 27-3042, Technical Writer, Documentation Writer
SOC No. 17-3010, Drafters
SOC No. 17-3019, Drafter, All Others
SOC No. 27-1024, Graphics Artist, Graphics Designer

14.1 Documentation Specialist – Senior
Description: Under general direction, is responsible for preparing and/or maintaining systems, programming, and operations documentation, procedures, and methods including user manuals and reference manuals. Maintains a current internal documentation library. Provides or coordinates special documentation services as required. Competent to work at the highest level of all phases of documentation. May act as project leader for large jobs.

14.2 Documentation Specialist – Intermediate
Description: Under general supervision, prepares and/or maintains systems, programming, and operations documentation, including user manuals. Maintains a current internal documentation library. Competent to work on most phases of documentation.

14.3 Documentation Specialist – Associate
Description: Under direct supervision, prepares and/or maintains systems, programming and

operations documentation, including user manuals. Maintains a current internal documentation library.

14.4 Technical Editor

Experience/Education: Minimum of 10 years of experience and MA/MS degree
Description: Responsible for content of technical documentation. Checks author's document for spelling, grammar, and content problems (e.g., missing instructions or sections; redundant or unnecessary sections). Accuracy of content may fall under this position or the programmer, depending on the expertise of the editor. Ensures that documents follow the style laid out in the organization's style guide. May also be responsible for maintaining the style guide. Suggests revisions to the style guide as appropriate. Editor is often a technical writer who has moved to this position.

14.5 CAD Specialist

Experience/Education: Minimum of 5 years of experience and BA/BS degree
Description: Ability to prepare various drawings that communicate engineering ideas, designs, and information in support of engineering functions directly supporting infostructure IT goals and projects. Drawings consist of parts and assemblies including sectional profiles, irregular or reverse curves, hidden lines, and small or intricate details. Requires experience in current conventional computer-aided design drafting techniques and application programs.

14.6 Graphics Specialist

Experience/Education: Minimum of 5 years of experience and BA/BS degree
Description: Responsible for graphics design and use, operation and setup of computer graphic systems for business communications. Executes graphic projects and assists in coordination of all graphic production scheduling; coordinates production support with outside contractors, as needed. Ensures that graphic projects are completed on time, within budget and to user’s satisfaction. Interfaces with users to determine scope of project and best graphic medium. Trains other personnel in proper use of computer graphic equipment. Troubleshoots computer equipment problems and performs minor preventive maintenance.

14.7 Draftsman – Senior

Description: Under indirect supervision, responsible for preparing various drawings that communicate engineering ideas, designs, and information in support of engineering functions directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Drawings consist of parts and assemblies including sectional profiles, irregular or reverse curves, hidden lines, and small or intricate details. Requires experience in current conventional computer-aided design drafting techniques and application programs.

14.8 Draftsman – Intermediate

Description: Under general direction, responsible for preparing various drawings that communicate engineering ideas, designs, and information in support of engineering functions directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Drawings consist of parts and assemblies including sectional profiles, irregular or reverse curves, hidden lines, and small or intricate details. Requires experience in current conventional computer-aided design drafting techniques and application programs.

14.9 Draftsman – Associate

Description: Under immediate supervision, responsible for preparing various drawings that communicate engineering ideas, designs, and information in support of engineering functions directly supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Drawings consist of parts and assemblies including sectional profiles, irregular or reverse curves, hidden lines, and small or intricate details. Requires experience in current conventional computer-aided design drafting techniques and application programs.

15. Enterprise Resource Planning (ERP)/Business Process Development

SOC No. 13-2031, Budget Analyst, Cost Analyst
SOC No. 13-1111, Business Management Analyst, Management Analyst
SOC No. 13-1081, Logistics Analyst
SOC No. 15-1121, Data Processing Systems Analyst, Computer Systems Analyst, Information Systems Analyst
SOC No. 15-1122, Network Security Analyst
SOC No. 15-2031, Operations Analyst, Operations Research Analyst, Procedure Analyst, Process Analyst
SOC No. 15-2041, Statistical Analyst

15.1 ERP Business Analyst – Senior

Description: Under general direction, serves as senior subject matter expert associated with content, processes and procedures associated with ERP. Defines the detailed requirements, analyzes the business needs, and validates solutions with the client. Details requirements through the product development and other functions to support the project team. Monitors other business analysts in software development methods and processes and implementation of those methods. Evaluates development projects and assists in tailoring the development process to meet the project needs.

15.2 ERP Business Analyst – Intermediate

Description: Under general supervision, serves as subject matter expert associated with content, processes, and procedures associated with enterprise applications. Applies functional knowledge to design and customization of workflow systems that provide seamless integration for client/server applications. Writes functional requirements, develops test plans, and works with production issues.

15.3 ERP Business Analyst – Associate

Description: Under direct supervision, serves as subject matter expert associated with content, processes and procedures associated with enterprise applications. Applies functional knowledge to design and customization of workflow systems that provide seamless integration for client/server applications. Writes functional requirements, develops test plans, and works with production issues.

15.4 Business Systems Analyst – Senior

Description: Under general direction, formulates and defines systems scope and objectives based on both user needs and a good understanding of applicable business systems and industry

requirements. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time, and form of desired results. Includes analysis of business and user needs, documentation of requirements, and translation into proper system requirement specifications. Guides and advises less experienced Business Systems Analysts. Competent to work at the highest technical level of most phases of systems analysis while considering the business implications of the application of technology to the current and future business environment.

15.5 Business Systems Analyst – Intermediate

Description: Under general supervision, formulates and defines systems scope and objectives through research and fact-finding combined with an understanding of applicable business systems and industry requirements. With this knowledge, develops or modifies moderately complex information systems. Includes analysis of business and user needs, documenting requirements, and revising existing system logic difficulties as necessary. Guides and advises less experienced Business Systems Analysts. Competent to work in some phases of systems analysis and considers the business implications of the application of technology to the current business environment.

15.6 Business Systems Analyst – Associate

Description: Under direct supervision, assists in formulating and defining systems scope and objectives through research and fact-finding combined with a basic understanding of business systems and industry requirements. Includes analysis of business and user needs, documenting requirements, and revising existing system logic difficulties as necessary under direction of experienced Business System Analysts. Competent to consider most business implications of the application of technology to the current business environment.

16. Information Systems Training

SOC No. 13-1151, Corporate Trainers, Training Specialists, Training and Development Specialists
SOC No. 11-3131, Training Managers, Training and Development Managers

16.1 Information Systems Training Manager

Experience/Education: Minimum of 10 years of experience and MS/PhD degree
Description: Responsible for all activities associated with education programs for both the information technology and end-user/PC personnel. Advises on administrative policies and procedures, technical problems, priorities, and methods. Assigns personnel to the various training tasks and directs their activities, reviews and evaluates their work, conducts performance appraisals, and makes decisions on personnel.

16.2 Information Systems Training Specialist – Senior

Description: Under general direction, organizes, prepares, and conducts complex training and educational programs for information systems or user personnel. May design and develop in-house programs. Maintains records of training activities, employee progress, and program effectiveness. Competent to work at the highest level of all phases of information systems training.

16.3 Information Systems Training Specialist – Intermediate
Description: Under general supervision, organizes and conducts moderately complex training and educational programs for information systems or user personnel. Maintains records of training activities, employee progress, and program effectiveness. Competent to work on most phases of information systems training.

16.4 Information Systems Training Specialist – Associate
Description: Under direct supervision, organizes and conducts basic training and educational programs for information systems or user personnel. Maintains record of training activities, employee progress, and program effectiveness.

16.5 Instructor Technical Training – Senior
Description: Under indirect supervision, responsible for provides technical expertise and instruction according to customer specifications and standards (operate, maintain, and repair in classroom or laboratory settings) supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Analyzes System and Network related information and interprets it into useable instruction/training for intended audience. Develops courseware/content in specific technical subject matter area. Provides advice to customers in system design and optimal configuration. Provides technical telephone support to customers with hardware and software problems. Also, provides technical and training input for development of training proposals. May be required to deploy and train US Forces in CONUS or OCONUS field locations.

16.6 Instructor Technical Training – Intermediate
Description: Under general direction, responsible for provides technical expertise and instruction according to customer specifications and standards (operate, maintain, and repair in classroom or laboratory settings) supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Analyzes System and Network related information and interprets it into useable instruction/training for intended audience. Develops courseware/content in specific technical subject matter area. Provides advice to customers in system design and optimal configuration. Provides technical telephone support to customers with hardware and software problems. Also, provides technical and training input for development of training proposals. May be required to deploy and train US Forces in CONUS or OCONUS field locations.

16.7 Instructor Technical Training – Associate
Description: Under immediate supervision, responsible for provides technical expertise and instruction according to customer specifications and standards (operate, maintain, and repair in classroom or laboratory settings) supporting DoD Enterprise infrastructure and infostructure IT goals and projects. Analyzes System and Network related information and interprets it into useable instruction/training for intended audience. Develops courseware/content in specific technical subject matter area. Provides advice to customers in system design and optimal configuration. Provides technical telephone support to customers with hardware and software problems. Also, provides technical and training input for development of training proposals. May be required to deploy and train US Forces in CONUS or OCONUS field locations.

17. Audio Visual

SOC No. 17-2061, Computer Hardware Engineer
SOC No. 17-2199, Engineer, all others
SOC No. 15-1130, Software Developers and Programmers
SOC No. 15-1131, System Programmers, Computer Language Coders

17.1 Audio Visual Fabrication Engineer – Senior
Description: Under indirect supervision, installs, pulls, terminates, and tests all audio visual (AV) type cables, connectors, and interfaces. Ability to install projections screens, plasma TVs and different types of speakers. Installation of AV systems on client sites. Read blueprints and wire AV racks. Manage AV projects with various models and makes of equipment. Has a thorough understanding and working knowledge of testing, analyses, and corrective action on systems, networks, hardware, and software in a Professional Audio/Video environment. Knows and understands all wire and connector types on all AV related cable.

17.2 Audio Visual Fabrication Engineer – Intermediate
Description: Under general direction, installs, pulls, terminates, and tests all audio visual (AV) type cables, connectors, and interfaces. Ability to install projections screens, plasma TVs and different types of speakers. Installation of AV systems on client sites. Read blueprints and wire AV racks. Manage AV projects with various models and makes of equipment. Has a thorough understanding and working knowledge of testing, analyses, and corrective action on systems, networks, hardware, and software in a Professional Audio/Video environment. Knows and understands all wire and connector types on all AV related cable.

17.3 Audio Visual Fabrication Engineer – Associate
Description: Under immediate supervision, installs, pulls, terminates, and tests all audio visual (AV) type cables, connectors, and interfaces. Ability to install projections screens, plasma TVs and different types of speakers. Installation of AV systems on client sites. Read blueprints and wire AV racks. Manage AV projects with various models and makes of equipment. Has a thorough understanding and working knowledge of testing, analyses, and corrective action on systems, networks, hardware, and software in a Professional Audio/Video environment. Knows and understands all wire and connector types on all AV related cable.

17.4 Audio Visual Programmer – Senior
Description: Under indirect supervision, designs and programs control interface touch panels for audio visual systems. Works with Design Engineer and Contracting Officer's Technical Representative to ensure a user-friendly operating environment for controlling audio/visual equipment. Provide training to users to ensure proper use and care.

17.5 Audio Visual Programmer – Intermediate
Description: Under general direction, designs and programs control interface touch panels for audio visual systems. Works with Design Engineer and Contracting Officer's Technical Representative to ensure a user-friendly operating environment for controlling audio/visual equipment. Provide training to users to ensure proper use and care.

17.6 Audio Visual Programmer – Associate
Description: Under immediate supervision, designs and programs control interface touch panels

for audio visual systems. Works with Design Engineer and Contracting Officer's Technical Representative to ensure a user-friendly operating environment for controlling audio/visual equipment. Provide training to users to ensure proper use and care.

18. Intelligent Automation [Artificial Intelligence (AI)/Robotic Process Automation (RPA)]

Robotic Process Automation (RPA) is an emerging technology area that has not been officially defined by NIST but is being promoted as a commercial solution.

18.1 Artificial Intelligence (AI) Engineer – Intermediate

Description: An artificial intelligence engineer is an individual who works with traditional machine learning techniques like natural language processing and neural networks to build models that power AI-based applications. An artificial intelligence programmer helps develop operating software that can be used for robots, artificial intelligence programs or other artificial intelligence applications. They may work closely with electrical engineers or robotics engineers and others in order to produce systems that utilize artificial intelligence. This is the capability of adapting or changing based on adding data. It may also mean programming a system to look for or seek out specific conditions and respond based on those factors. Candidates should possess excellent math, science, and analytical skills necessary to solve complex problems and find efficient solutions.

18.2 Machine Learning Engineer – Intermediate

Description: Machine learning is a form of AI that enables a system to learn from data rather than through explicit programming. Once an ML program is written, it must be "trained" before it is deployed in its intended use. Training is the process by which the machine learns. The programming utilizes algorithms that ingest training data supplied by a machine learning engineer, making it possible to produce more precise models based on that data.

18.3 Machine Learning (Data) Scientist – Senior

Description: Data science can be described as the description, prediction, and causal inference from both structured and unstructured data. This discipline helps individuals and enterprises make better business decisions. It's also a study of where data originates, what it represents, and how it could be transformed into a valuable resource. To achieve the latter, a massive amount of data has to be mined to identify patterns to help businesses. The field of data science employs computer science disciplines like mathematics and statistics and incorporates techniques like data mining, cluster analysis, visualization, and machine learning.

19. Cloud Services

19.1 Cloud Architect – Intermediate

Description: A cloud architect, or cloud computing architect, is responsible for setting up all of the components required for successful cloud computing. A cloud computing network, as opposed to a more traditional computer network, involves storing and managing data across a number of remotely located servers, rather than a local server. Cloud architects are in charge of creating these cloud networks by connecting remotely located servers. This involves setting up front- and back-end platforms and developing an operational cloud based delivery system. A strong background in

scripting and programming languages. Cloud architects combine a technical education background with a number of years of work experience in the field of computing and technology.

19.2 Cloud Developer – Associate
Description: A professional Cloud Developer builds scalable and highly available applications using virtual systems, practices, and tools. They design and implement cloud infrastructures, and ensure the effective design of business processes in the cloud. They have a deep understanding of cloud provider architectures and are able to monitor cloud maintenance, planning, security and usage across the company.

19.3 Cloud DevOps Engineer – Intermediate
Description: A DevOps engineer is an IT professional who is responsible for bridging software development, engineering, and management to make the software development process faster. A DevOps engineer introduces processes, tools, and methodologies to balance needs throughout the software development life cycle, from coding and deployment, to maintenance and updates.

19.4 Cloud Engineer – Senior
Description: Under general supervision, has duties of instructing, directing, and checking the work of other project engineers. Responsible for the completion of assigned engineering projects within budgetary and scheduling guidelines. Leads a group of engineers, analysts, and/or technicians assigned for the duration of a project or may function as ongoing lead within a group of engineers associated with one or more technical areas within the telecom function (such as, but not limited to, network design, engineering, implementation, or operations/user support). Does not have formal supervisory responsibilities, although may provide input for (project) team member performance appraisals.

19.5 Cloud Engineer – Intermediate
Description: A cloud engineer is an IT expert responsible for the design, planning, management, maintenance, and support, and any other technological duties associated with an organization's cloud computing environment. Cloud operations engineers specialize in creating and implementing cloud-based solutions such as Software as a Service (SaaS) and Platform as a Service (PaaS).

19.6 Cloud Network Engineer – Intermediate
Description: Cloud network engineering roles assess an organization's technology infrastructure and explore options for moving to the cloud. If the organization elects to move to the cloud, a cloud engineer is responsible for overseeing the process, referred to as migration, and maintaining the new system. Job Duties: Implement, support, maintain, and optimize the network hardware, software, and communications links of the company's cloud infrastructure.

19.7 Cloud Security Engineer – Intermediate
Description: Cloud security engineers specialize in providing security systems and tools management related to the cloud technologies and playing a vital role in protecting an organization's data. A cloud security engineer specializes in providing security for cloud-based digital platforms and plays an integral role in protecting an organization's data. This may involve analyzing existing cloud structures and creating new and enhanced security methods. They often serve as part of a larger team dedicated to cloud-based management and security. Cloud security engineers usually work full-time in an office environment, with some positions requiring personnel to respond to after-hours emergencies.

19.8 Platform Engineer – Intermediate
Description: Platform engineers enable application developers to put software into the hands of users in an easier manner. This is the case when there is integration between on premise systems and cloud services. Platform engineers build systems that allow teams to build on. A platform engineer writes code that bridges the gap between software and hardware and tests the system so that it runs effectively and smoothly.

19.9 Test Engineer – Intermediate
Description: A test engineer is a professional who determines how to create a process that would best test a particular product in manufacturing and related disciplines, in order to assure that the product meets applicable specifications. Test engineers are also responsible for determining the best way a test can be performed in order to achieve adequate test coverage.

19.10 User Interface, User Experience (UI/UX) Designer – Associate
Description: UI Designer/Developer III designs web pages and develops web-based technical solutions that engage users and meet business requirements. Handles projects from conceptualization through delivery. A UI Designer/Developer III develops and applies creative designs, ensuring that content meets brand standards and targets the intended audience.

20. Data Services

20.1 Data Architect – Senior
Description: Data architects focus on how information moves across the system from one application to another. Demonstrated expertise in requirements engineering, software architecture, software testing, and software deployment including understanding how the software interacts with the technical architecture. Data architects allow a company to easily publish and share their data with others in the industry, data architects design database systems. By creating the system according to industry standards, they also help a business accurately report information to the necessary bureaus. First, the architect may review any data architecture already in place, while also determining the specifications for the size of the new system. The databases they create organize large bits of information, such as company spending. Additionally, they design with growth in mind, allowing for future modifications to the database as the company develops.

20.2 Data Engineer – Intermediate
Description: Under general supervision, carries out procedures to ensure that all information systems products and services meet minimum organization standards and end-user requirements. Thoroughly tests software to ensure proper operation and freedom from defects. Documents and works to resolve all problems. Reports progress on problem resolution to management. Devises improvements to current procedures and develops models of possible future configurations. Performs workflow analysis and recommends quality improvements.

20.3 Data Labeler – Intermediate
Description: Data labeling is the manual curation of data by humans on machine learning and AI applications. Data Steward coordinates an organization's quality, security, and maintenance of data. Defines data elements and establishes policies and procedures related to the collection and accuracy

of data, and performs tests on data systems. Being a Data Steward ensures sufficient data quality is maintained so that the data can effectively support the business process.

20.4 Data Scientist – Senior

Description: Data Scientists build analytics tools that utilize the data pipeline to provide actionable insights into customer acquisition, operational efficiency and other key business performance metrics. Create data tools for analytics and data scientist team members that assist them in building and optimizing products. Communicate effectively through listening, documentation and presentations, especially using compelling visualization tools to share analysis and interpretation of data.

20.5 Operations Research and Systems Analyst (ORSA) – Intermediate

Description: Operations research analysts use advanced mathematical and analytical methods to help solve complex issues.

APPENDIX 3: GOVERNMENT AND CONTRACTOR FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

1. Government Furnished Property, Equipment, and Services

1.1 Services
The Government may provide Government Furnished Services which will be stipulated in each individual task order.

1.2 Facilities
The Government may provide Government Furnished Equipment which will be stipulated in each individual task order.

1.3 Utilities
The Government may provide Government Furnished Utilities which will be stipulated in each individual task order. The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

1.4 Equipment
The Government may provide Government Furnished Equipment which will be stipulated in each individual task order.

1.5 Materials
The Government may provide Government Furnished Materials which will be stipulated in each individual task order.

2. Contractor Furnished Items and Responsibilities

2.1 General
The contractor may have to furnish all supplies, equipment, facilities, and services required to perform work under this contract that are not listed under Appendix 3 of this PWS. This will be stipulated in each individual task order.

2.2 Facility Clearance
The contractor may need to possess and maintain security clearances of at least Secret and up to Top Secret, Specialized Compartmentalized Information from the Defense Security Service. The contractor's employees, performing work in support of this contract may have been granted a security clearance from the Defense Industrial Security Clearance Office. This will be specified on each individual task order and in each individual DD254.

APPENDIX 4: DIRECTIVES, POLICIES, STANDARDS & GUIDELINES

APPLICABLE RESOURCES

The contractor must abide by all applicable regulations, publications, manuals, Security Technical Implementation Guides (STIGs) and local policies and procedures.

The following specifications, standards, policies and procedures represent the constraints placed on this acquisition. All documents listed are mandatory, as applicable. Applicability is as defined in the document. The most current version of the document at the time of task order issuance will take precedence. The list is not all-inclusive. Other documents required for execution of tasks issued under ITES-3S will be cited in the relevant task order.

DoD Instruction 8010.01, Department of Defense Information Network (DoDIN) Transport, September 10, 2018

This issuance establishes policy, assigns responsibilities, and provides procedures for DODIN transport and the life-cycle management of: Connection and interconnection of information systems (e.g., applications, enclaves, or outsourced processes); Unified capabilities (UC) products (including data, voice, and video); Access to information services (including data, voice, video, and cross domain (CD)) transmitted over the DODIN transport.

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf

Department of Defense Instruction 8500.01E Change 1, Cybersecurity, 7 October 2019

a. Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).

b. Incorporates and cancels DoDI 8500.02 (Reference (c)), DoDD C-5200.19 (Reference (d)), DoDI 8552.01 (Reference (e)), Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (DoD CIO) Memorandums (References (f) through (k)), and Directive-type Memorandum 08-060 (Reference (l)).

c. Establishes the positions of DoD principal authorizing official (PAO) and the DoD Senior Information Security Officer (SISO) and continues the DoD Information Security Risk Management Committee (DoD ISRMC).

d. Adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (m)) to be used throughout DoD instead of the term "information assurance (IA)."

https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

DoD Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014 (Incorporating Change 3, December 29, 2020)

The DoD will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoD mission areas (Mas).

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=qEE2HGN_HE4Blu7161t1TQ%3D%3D

Department of Defense Cloud Strategy, December 2018

The strategy drives implementation toward the enterprise cloud environment, an ecosystem composed of a General Purpose and Fit For Purpose clouds. It focuses implementation activities on two fundamental types of work: first is the stand up of cloud platforms ready to receive data and applications, and second is the ongoing work to migrate existing applications and to develop new applications in the cloud.

https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF

The Army Cloud Plan 2020

The Army Cloud Plan lays out the following six strategic objectives: Accelerate Data Driven Decisions, Decrease Time to Field software, Optimize the Security Accreditation Process, Establish Cloud Design, Software Development and Data Engineering as a Core Competency, Design Software to Adapt to an Unpredictable World, and Provide IT Asset/Cost Transparency and Accountability.

https://api.army.mil/e2/c/downloads/2020/09/11/81bb912e/the-army-cloud-plan-2020-final2.pdf

Defense Standardization Program

Standardization documents are developed and used for products, materials, and processes that have multiple applications to promote commonality and interoperability among the Military Departments and the Defense Agencies and between the United States and its allies, and to limit the variety of items in the military supply system. The Acquisition Streamlining and Standardization Information System (ASSIST) database identifies approved defense and federal standardization documents, adopted non-government standards (NGS), and U.S. ratified materiel International Standardization Agreements (ISAs).
https://www.dsp.dla.mil/Specs-Standards/

DoD Enterprise Software Initiative (DoD ESI). Overview & History, September 23, 2016 (Updated 02/02/21)

DoD Enterprise Software Initiative (DoD ESI) is an official DoD initiative sponsored by the DoD Chief Information Officer (CIO) to lead in the establishment and management of enterprise COTS IT agreements, assets, and policies. DoD ESI lowers the total cost of ownership across the DoD, Coast Guard and Intelligence Communities for commercial software, IT hardware, and services.
Link to DoD ESI Agreements:

https://www.esi.mil/default.aspx
https://www.esi.mil/AgreementList.aspx?type=0

DoD Memo, "Category Management Purchasing Solutions for Commodity Laptops and Desktops", November 24, 2020

The Department of Defense Chief Information Officer (DoD CIO) promotes the use of Information Technology Category Management (ITCM) "Best-in-Class" (BIC) solutions for commodity laptop and desktop computer purchases to maximize asset value through demand management, volume discounts, and streamlined procurement processes. This memo designates BIC solutions for DoD enterprise use. DoD ordering activities must first consider these BIC solutions to fulfill commodity purchasing requirements.

https://www.esi.mil/download.aspx?id=8275

DoD Memo "Department of Defense Software Lifecycle Maintenance", July 9, 2020 (Updated 11/24/20)

The Department of Defense Software Lifecycle Maintenance Memorandum, released 14 May 2020 by the DoD Chief Information Officer, covers current critical Cybersecurity vulnerability concerns associated with installed commercial software on Government Information Systems and servers not being properly maintained or supported. It gives guidance on how DoD Components, to include owners of Programs of Record and Weapon Systems, must mitigate this and provides attached Vendor Software Lifecycle Maintenance Schedules, Support Policies, Lifecycle Changes, and other resources for various software.

https://www.esi.mil/download.aspx?id=8157

Army Regulation 25-1, Information Management Army Information Technology, 07/15/2019

This regulation establishes policies and assigns responsibilities for in-formation management and information technology. It applies to information technology contained in both business systems and national security systems (except as noted) developed for or purchased by the Department of Army. It addresses the management of information as an Army resource, the technology supporting information requirements, and the resources supporting information technology. This regulation implements Title 40, United States Code, Subtitle III (40 USC, Subtitle III); 44 USC, Chapters 35 and 36; 10 USC 2223 and 3014; and DODD 8000.01. It establishes the Army's Chief Information Officer and the full scope of the Army Chief Information Officer's responsibilities and management processes. These processes

involve strategic planning, capital planning, business process analysis and improvement, assessment of proposed systems, information resource management (to include investment strategy), performance measurements, acquisition, and training.

https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1004709

Army Regulation 25-2, Information Management: Cybersecurity, 4 April 2019

This regulation establishes the Army Cybersecurity Program and sets forth the mission, responsibilities, and policies to ensure uniform implementation of public law and Office of Management and Budget, Committee on National Security Systems, and Department of Defense issuances for protecting and safeguarding Army information technology, to include the Army managed portion of the Department of Defense Information Network, (hereafter referred to as information technology) and information in electronic format (hereafter referred to as information). Information technology includes infrastructure, services, and applications used directly by the Army or for the Army by legal agreements or other binding contracts.
https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1002626

Army Network Enterprise Technology Command (NETCOM) Technical Authority (TA) for Implementation of Army End-User Computing Environment Version 7.0, 13 March 2020

This Technical Authority (TA) document identifies the recommended hardware, operating systems (OSs), applications, and configurations necessary to establish a secure, standardized baseline end-user computing environment for use throughout the Army. This TA defines the end-user computing system baselines established as the Army's portion of the Department of Defense Information Network (DoDIN-A) Configuration Items (CIs) managed by the DoDIN-A Change Advisory Board (CAB) via the Change Management (ChM) process. End-user computing environments include the use of Microsoft Windows in physical desktop (mobile ruggedized laptops, tablets, and stationary desktop systems) and virtual computing environments.

Department of Defense (DoD) Unified Capabilities Requirements (UCR) 2013 Change 2, September 2017

The Department of Defense (DoD) Unified Capabilities Requirements (UCR) 2013 specifies the technical requirements for certification of approved commercial products to be used in DoD networks to provide end-to-end Unified Capabilities (UC), so that all components of the network are connected and working together.

https://aplits.disa.mil/docs/UCR-2013-Change2.pdf

The Department of Defense Information Network (DoDIN) Approved Products List (APL)

The Department of Defense Information Network (DoDIN) Approved Products List (APL) is the single consolidated list of products that have completed Cybersecurity (CS) and Interoperability (IO) certification.

https://aplits.disa.mil/processAPList

DOD Information Technology Standards Registry (DISR)

The DISR is the single, unifying DoD registry for approved information technology (IT) and national security systems (NSS) standards and standards profiles that is managed by the Defense Information Systems Agency (DISA). The DISR Baseline lists IT Standards that are mandated for use in the DoD Acquisition process. The DISR is the standards data source that is used to populate and develop Standards Technical Profiles (StdV) that are required artifacts in Information Support Plans (ISP). The complete DISR can be accessed at https://gtg.csd.disa.mil/disr/dashboard.html with a DoD Computer Access Card (CAC) and an account.

https://www.dsp.dla.mil/Specs-Standards/List-of-DISR-documents/

Energy Star

ENERGY STAR® is the government-backed symbol for energy efficiency, providing simple, credible, and unbiased information that consumers and businesses rely on to make well-informed decisions. Thousands of industrial, commercial, utility, state, and local organizations—including about 40% of the Fortune 500®—partner with the U.S. Environmental Protection Agency (EPA) to deliver cost-saving energy efficiency solutions that improve air quality and protect the climate. Since 1992, ENERGY STAR and its partners helped American families and businesses save more than 4 trillion kilowatt-hours of electricity and achieve over 3.5 billion metric tons of greenhouse gas reductions, equivalent to the annual emissions of more than 750 million cars. In 2018 alone, ENERGY STAR and its partners helped Americans avoid $35 billion in energy costs.

https://www.energystar.gov/about?s=mega

Statutory Authority for ENERGY STAR

The ENERGY STAR program was established by EPA in 1992, under the authority of the Clean Air Act Section 103(g).
Federal Law

Section103(g) of the Clean Air Act directs EPA to "develop, evaluate, and demonstrate non-regulatory strategies and technologies for air pollution prevention… with opportunities for participation by [stakeholders]… including SOx, NOx… CO2… including end-use efficiency, and fuel-switching to cleaner fuels." (42 USC Section 7403g)

In 2005, Congress enacted the Energy Policy Act. Section 131 of the Act amends Section 324 of the Energy Policy and Conservation Act, and directed the Environmental Protection Agency and the

Department of Energy to implement "a voluntary program to identify and promote energy–efficient products and buildings in order to reduce energy consumption, improve energy security, and reduce pollution through voluntary labeling of or other forms of communication about products and buildings that meet the highest energy efficiency standards." The Act further directs EPA and DOE to work jointly to "(1) promote ENERGY STAR compliant technologies as the preferred technologies in the marketplace for (A) achieving energy efficiency; (B) and reducing pollution; (2) work to enhance public awareness of the ENERGY STAR label, including providing special outreach to small businesses; (3) preserve the integrity of the ENERGY STAR label; (4) regularly update Energy Star product criteria for product categories;" and to solicit comments from interested parties prior to establishing/revising ENERGY STAR product categories, specifications, or criterion. (42 USC Section 6294a)

https://www.energystar.gov/about/origins_mission/epas_role_energy_star/epa%E2%80%99s_statutory_authority_energy_star

Energy Star Product Specifications

Category: Data Center Equipment – Data Center Storage, Enterprise Servers, Large Network Equipment, Small Network Equipment, Uninterruptable Power supplies.
Category: Electronics and Office Equipment – Audio/Video, Computers, Displays, Imaging Equipment, Televisions

https://www.energystar.gov/products/spec?s=mega

Green Electronics Council (GEC) Electronic Product Environmental Assessment Tool (EPEAT) Registry

The EPEAT registry provides a list of electronic devices that have met energy and environmental criteria established by the GEC. Devices are registered as Bronze, Silver, or Gold, depending on their compliance level.

https://epeat.net/

President Issues Executive Order Regarding Energy-Efficient Use of Power Devices in Federal Facilities, 7/31/2001

Executive Order 13221 - Defines the policy for use of Energy Star devices within Federal Facilities. The Executive Order required that when Federal organizations purchase commercially available, off-the-shelf products that use external standby power devices, or that contain an internal standby power function, that the purchase products use no more than one watt in their standby power-consuming mode. If such products are not available, agencies shall purchase products with the lowest standby power wattage while in their standby power-consuming mode.

http://www.gsa.gov/graphics/fas/Buying_Energy_Efficient_Products.pdf

Section 508

Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires federal agencies to develop, procure, maintain and use information and communications technology (ICT) that is accessible to people with disabilities - regardless of whether or not they work for the federal government. The US Access Board established the Section 508 standards that implement the law and provides the requirements for accessibility.

https://www.epa.gov/accessibility/what-section-508

US Access Board ICT - Revised Section 508 Standards and 255 Guidelines website

http://go.usa.gov/x7VUs

Federal Identity, Credential, and Access Management (FICAM)

FICAM is the Federal Government's implementation of Identity, Credential, and Access Management (ICAM). ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives.

https://playbooks.idmanagement.gov/arch/intro-arch/

Enabling Mission Delivery through Improved Identity, Credential, and Access Management

A federal enterprise identity is the unique representation of an employee, contractor, or enterprise user, which could be a mission or business partner, or even a device or technology managed by a Federal agency to achieve its mission and business goals (OMB Memorandum 19-17).

https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

Standards and Policies

Review the federal policies and standards that impact and shape the implementations of ICAM programs and systems.

https://playbooks.idmanagement.gov/arch/standards/

DoD Manual 4140.01, Volume 7, "DoD Supply Chain Materiel Management Procedures: Supporting Technologies,", April 18, 2019

Assistant Secretary of Defense for Sustainment supports the development and application of advances in logistics technology that strengthen the capabilities of the DoD supply chain.

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/414001m/414001m_vol07.PDF?ver=aXy98hp6g9fZxjy0cHrY7A%3d%3d

Automatic Identification Technology (AIT)

The Office of the Under Secretary of Defense (Supply Chain Integration) is responsible for leading the implementation of a modern and integrated materiel supply chain process that fully supports military operational requirements. The end goal of this initiative is to promote customer confidence in the DoD logistics process by building a responsive, cost-effective capacity to provide required products and services to the Warfighter.

https://www.acq.osd.mil/log/SCI/AIT.html

Department of Defense Standard Practice - Military Marking For Shipment and Storage (MIL STD 129-R Change 2), 27 SEP 2019

This standard provides the minimum requirements for uniform military marking for shipment and storage. Additional markings may be required by the contract or the cognizant activity.

https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=35520

Army Regulation 700-145 Logistics Item Unique Identification, 18 FEB 2016

This regulation implements key provisions of DODI 8320.03, DODI8320.04, and DFARS 211.274–5. It prescribes Department of the Army policy and responsibilities for item unique identification that includes planning, acquiring, and sustaining item unique identification for Army managed items.

DoDD 8320.03: Unique Identification (UID) Standards for a Net-Centric Department of Defense Establishes policy and prescribes the criteria for creation, maintenance, and dissemination of UID data standards for discrete entities; Establishes policy and assigns responsibilities for the establishment of the Department's enterprise-wide UID strategy and for the development, management, and use of unique identifiers and their associated authoritative data source in a manner that precludes redundancy.

http://www.dtic.mil/whs/directives/corres/pdf/832003p.pdf

Department of Defense Standard Practice - Identification Marking of US Military Property (MIL-STD-130N Notice 1, 26 AUG 2019)

This standard provides the item marking criteria for development of specific marking requirements and methods for identification of items of military property produced, stocked, stored, and issued by or for the Department of Defense (DoD). This standard addresses criteria and data content for both free text and machine-readable information (MRI) applications for identification marking of U.S. military property.

https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=35521

Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG) (DOD Directive 8100.02), 4/14/2004 (Certified Current as of April 23, 2007)

Establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DOD Global Information Grid (GIG).

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/810002p.pdf

Security Requirements for Cryptographic Modules (FIPS PUB 140-3), 22 MAR 2019

The selective application of technological and related procedural safeguards is an important responsibility of every federal organization in providing adequate security in its computer and telecommunication systems. This standard is applicable to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106 and the Federal Information Security Management Act of 2002, Public Law 107-347.

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List

Website provides listing of NIST certified cryptographic modules that are compliant with FIPS 140-1 and FIPS 140-2 security requirements.

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

APPENDIX 5: REQUIRED REPORTS

1. General Information (applies to all reports)

CHESS Manages Data by Contract:
Reports must be submitted and managed by contract. Vendors with more than one contract with CHESS must maintain contract data integrity by submitting and managing separate reports for each contract. CHESS will not accept mixed contract data submitted in the same report.

Report Format:
All reports shall be submitted using either Microsoft Excel version 97-2007 .xls format or .xlxs format. The spreadsheets shall contain text and number values with two decimals for money columns only. **The spreadsheets shall not contain formatting; rounding of number/dollar values, hard line returns, or other embedded special characters. An exception to the formatting includes yellow highlighting for new/edited fields, and column formatting of data types.** All reports contain data fields that are optional. If there is no data to report in these fields, the field must be left empty. (No spaces, returns, tabs, etc.)

Report Delivery:
All reports shall be submitted on the CHESS Portal or as per most recent direction from CHESS. When a file reaches 10Mb, the vendor will begin another cumulative file.

Reports are due as follows:
In accordance with this document as indicated for each report.

Negative Reports:
Revision is required for negative CHESS reports.

Rejection of reports:
Vendor reports will be loaded via an automated process. Therefore, CHESS reserves the right to reject reports submitted by the vendor if necessary. Possible reasons for rejection are missing information or formatting issues. Report submissions must meet the formatting guidelines provided in this document. Each report will be checked by CHESS for content as well as formatting. If CHESS rejects a report, the report will be returned to the vendor with an explanation identifying the problem(s). The vendor must make the necessary corrections and **resubmit the report in its entirety within three (3) business days from the day the report was returned**. CHESS will advise the vendor within 5 working days of receipt of a revised report whether the revised report is accepted. If the revised file still contains errors it will be rejected and returned to the vendor for correction. Subsequent reports will NOT be accepted by CHESS until all the required corrections have been made and CHESS has notified the vendor that the revised report is accepted.

Common Rejection Reasons:

Formatting Issues

- File not in Excel Spreadsheet (Version 97-2007) .xls or .xlxs format
- Missing Columns
- Incorrect naming convention of the OT Report
- Missing Column Headings
- Spreadsheet contains Macros, links, etc.

Data Issues

- Missing "Required" data (Ex. Contract Number)
- Data type is incorrect for the column. (Ex. A column for numeric data has text)
- Data exceeds maximum length acceptable for column(s)
- Date is presented in the incorrect format
- Numbers within the report contain more than 2 decimal places.
- The Order/Mod total does not match the sum of the items being reported
- Invalid Service Agency, Army Activity, State or Country Code
- No Formatting, hard line returns, embedded special characters or word wrapping within a column
- Missing or Invalid UNSPSC
- "Duplicate Orders" (Order with different transaction dates and no Mod associated with it or two rows containing all of the same data)

Revised Reports:
Revised reports must be submitted as a complete file (i.e. make changes/corrections to the original file and resubmit the entire file, not just what was changed). The file name format when submitting revised files must follow the file name format stipulated for each report (Order Transaction, Vendor Status, Product Attributes) with the addition of (Rev) immediately preceding the file extension .xls. For example, the first revision of a cum-1 OT report would be named: ContractNumber_OT_yyyy_mm_dd_cum-1(Rev1).xls. Subsequent revisions to the same file should indicate the revision number (e.g. Rev2, Rev3, etc.).

File Names:
File names must not exceed 50 characters. The date in the file name should be the submission date and should not indicate the end or start dates of data within the report.

2. Order Transaction (OT) report

The OT report shall be submitted monthly and is due by close of business (COB) on the 15th of each month. If the 15th falls on a weekend or Government holiday, the OT report shall be due the next business day immediately following the 15th. An e-mail response is required for negative reports (no transactions to report). The file name format for the first OT report is: ContractNumber_OT_yyyy_mm_dd_cum-1.xls. Due to the limitations of Excel, a mutually agreeable cut-off date for the cum-1 report will be determined, or if the file reaches 10Mb. Subsequent files shall only contain data not already reported in cum-1. Subsequent files shall be named: ContractNumber_OT_yyyy_mm_dd_cum-2.xls, cum-3, cum-4, etc. No extra spaces, commas, or ampersands allowed in the spreadsheet. Dashes are allowed. Leading zeros are allowed to be dropped in order to avoid leading apostrophes which violate formatting rules. The

OT report is cumulative in nature. Each report shall include *all* transactions from contract inception up to the Saturday preceding the submission date of the file. All columns are required, even when there is no data for a specific column. All new entries or changes must be identified by highlighting in yellow the line number and the data in the line that has changed or been added. The email message that includes the submitted OT report must contain the following:

1. any changes to the report since the last report and include the line number and the type of transaction (i.e., award, cancellation, de-obligation, etc.)
2. the total dollar value of the cumulative OT report being submitted in the email message.

The value stated in the email message will be used by CHESS to match the sales dollars in OTSIII after the load process. ***If the total dollar value stated in the forwarding email message does not match the total dollars of the OT report being submitted, the report will be rejected and returned to the vendor for correction.*** If an RFP number is missing (Col D), or if the RFP number does not match an *IT e-mart* RFP number, then the file in its entirety will be rejected. Task Order type (Col K) should reflect one of the abbreviations provided below. If a task has multiple types, use the predominant type.

Abbreviation Long Description
CPAF Cost Plus Award Fee
CPFF Cost Plus Fixed Fee
CR Cost – Reimbursable
CT Cost – Cost Type Contract
FP Fixed Price
FFP Firm Fixed Price
LH Labor Hours
T&M Time-and-Materials

The dollar amount reflected in Column R (Dollar amount of Transaction) must match the total order/mod value. Entries for column "AD" (Country) must come from the CHESS "Country List" found at https://chess.army.mil/Static/SRV_CONCOD. Entries for columns "AG" and "AH" must come from the CHESS "Service/Agency" found at https://chess.army.mil/Static/SRV_ARMY_ACT. Column J must contain a United Nations Products and Services Code for each CLIN. If a transaction contains a mixture of items shown above, the UNSPSC for that item should identify the dominant item provided under the transaction. Since the OT report is cumulative, vendors may correct previously reported information in subsequent reports (see Section 1. General Information, Revised Reports) such as:

Removing a cancelled order or an order/mod previously reported in error.
Correcting dollar amounts previously reported by an order/mod.
Correcting items ordered previously reported for an order/mod.

3. Monthly Task Order Status Report (MTOSR)

The MTOSR report shall be submitted monthly and is due by close of business (COB) on the 15th of each month. If the 15th falls on a weekend or Government holiday, the MTOSR report shall be due the next business day immediately following the 15th. An e-mail response is required for negative reports (no transactions to report). The file name format for the MTOSR report is "contractnumber_MTOSR_yyyy_mm.xls".

4. Small Business Participation Report (SBPR)

The SBPR report shall be submitted monthly and is due by close of business (COB) on the 15th of each month. If the 15th falls on a weekend or Government holiday, the SBPR report shall be due the next business day immediately following the 15th. The file name format for the SBPR report is "contractnumber_SBPR_yyyy_mm.xls".

5. Product Attribute (PA) Report

Product Attribute reports are due no later than 10 days from when:

- Labor rates have changed or
- New labor categories are added to the catalog

The file name format for the Product Attribute report is "contractnumber_PA_yyyy_mm_dd.xls".
The Product Attribute report must be a full replacement. CHESS will replace the vendors' existing Product Attribute file with the most recent submission. Partial updates are not permitted. Each Product Attribute report may contain only one worksheet. Each item in the Product Attribute report must provide, in column N (Description), an easy-to-understand description of the labor category. Each item in the Product Attribute report is limited to one row of the spreadsheet, and must have a unique item number which must be consistent throughout the lifecycle of that item. Each row must also have a unique price associated with the item.

6. Performance-based Progress Report (PBPR)

The Contractor shall provide a report on a quarterly basis to report the performance-based aspects (proposed measures/metrics and incentives/disincentives). Submission of this report will commence at least within six months after receipt of initial task order. The report shall be submitted by the 15th of the month following the end of a quarter.

Additional reports shall be provided as required in individual orders.