Statement of Work (SOW)
Project: {GLOBAL Twins}

GENERAL INFORMATION

Description of Services/Introduction:

The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform support and materials to the NSC TRADOC SO, at Fort Leavenworth, KS, and the Logistics Exercise & Simulations Division at Fort Lee, VA, and Fort Hood, TX as defined in this PWS except for those items specified as government furnished property (GFP) and services. The Contractor shall perform to the standards in this TO.

Background:

NSC, as the leader of the Army simulation community, provides Soldiers, leaders, and units the tools they need to train everyday by developing and championing capabilities for the Synthetic and Training Environment (STE), Virtual-Gaming-Constructive Training Environments. NSC functions as the Executive Agent responsible for the Army Mission Command Training Support Program (MCTSP); providing direct support to training exercises and experiments for Joint National Training Capability (JNTC) through support to the Mission Command Training Program (MCTP) and support to Home Station Training (HST) through the Regional Simulation Center (RSC). NSC houses and manages the Combined Arms Center – Training Innovation Facility (CAC-TIF); deliver interim solutions to capability gaps, while simultaneously providing valuable user feedback to STE-IS and provides Senior Leaders with situational awareness through hands on demonstrations.

Objectives:

To successfully achieve the NSC missions the following tasks shall be executed:

- Capability Development
- Assistance to the Materiel Developer in fielding capabilities across the Army
- Define and coordinate facilities, manpower, network, and sustainment costs necessary for Army Commands to properly use MCTSP
- Provide direct exercise and user support
- Support Home Station Training (HST) through the GSC/RSC
- Verification, Validation and Accreditation (VV&A) testing and certification of products developed by the Materiel Developer
- Support to the MCTP WFX Program
- Innovation, bridging strategies and strategic messaging within the CAC-TIF

Scope:

To successfully achieve the NSC missions the following tasks shall be executed:, Technology assessments and evaluations; VV&A testing and certification of products developed by the Materiel Developer; Assist the Materiel Developer in the fielding of capability across the Army; Support and resourcing for evaluation, integration, testing, and proof of principle studies in regard to emerging Commercial and Government off the shelf (COTS/GOTS) technologies; MCTSP capability development to include defining and coordinating the facilities, manpower, network and sustainment costs necessary for Army Commands to properly use the capability; Provide direct exercise support to MCTP; and Support HST through the RSC; and Innovation and experimentation within the CAC-TIF.

Special Qualifications:

All personnel shall comply with and meet Information Assurance Technician Level II (IAT II) Certification requirements as specified in 05-PR-M-0002, Information Assurance Best Business Practice (IA BBP), Information Assurance (IA) training and certification, as updated, i.e. Security + and complete Computing Environment (CE) certification and/or provide proof of completion of training for their primary area of support, (e.g. Cisco, Linux, Microsoft, VMware, etc., prior to working these tasks or gaining access to the NSC Simulation Network (SIMNET), JLCCTC systems, and/or external connections - Global Simulation Center Network (GSCNet), the Joint Testing and Experimentation Network (JTEN) or other such dedicated or direct tunnel, extant, or future.

Global Twins Graduate Medical Education and Simulation Key Personnel

Contractor's Key Personnel: {Describe positions which are considered key to successful performance of the contract and the information required to support key personnel qualifications, e.g., experience which correlates to SOW requirements, education, and past performance on similar projects. Specify if resumes are required and provide resume format if appropriate.}

Global Twins Graduate Medical Education and Simulation (GTGMES) Technical Control Forward (TCF) Lead. Contractor TCF manager(s) shall have 3 years' experience in modeling and simulation. JLCCTC technical, functional, and operational competencies including experience in configuring/setting up JLCCTC remote site systems, the TCF manager(s) shall identify and troubleshoot problems with models, interfaces, and networks at remote site locations. The TCF manager(s) shall have 3 years' experience and shall possess skills and experience in C2/MCiS architecture and technical functions to include the JLCCTC systems.

Global Twins Database Lead

The Database manager(s) shall possess 3 years' experience in building JLCCTC Database and have experience leading a JLCCTC Database development team. The Database manager(s) shall provide JLCCTC tools, interfaces, and processes used to build database products. The Database

manager(s) shall have 3 years' experience in military unit structures and/or researching unit compositions and structure (i.e. FMS Web). The Database manager(s) shall respond to GSC or Unit requests to change, in a timely manner, layouts and structures. Additionally, The Database manager(s) shall have the knowledge and experience to advise the GSC or training audience on executive-level-realistic configuration of NATO, ABCANZ, Opposing Force (OPFOR), Situational Forces (SITFOR) and other units in the database to ensure credible performance in JLCCTC models.

Cybersecurity Program Analyst:

Cybersecurity Program Analyst shall have 3 years' experience and be knowledgeable in Department of Defense (DoD) cybersecurity requirements and accreditation procedures. The Cybersecurity Program Analyst shall possess a DoD approved IAM Level II certification (CASP, GSLC, CISM or CISSP).

Database Developer:

Database Developer shall have minimum of 5 years' experience in relational database and Graphical User Interface (GUI) development. Familiar with implementing relational databases on a Structured Query Language (SQL) server within a secure DoD cloud Computing Environment (CE).

MUSE/BVT Lead:

The MUSE/BVT Lead shall have at least five (5) years' experience in the technical, functional and operational knowledge of all MUSE / BV systems and software. The Lead shall be a subject matter expert, with skills and experience training unit personnel in MUSE/BV operation and personnel network and setup of systems. Additionally, the Lead shall have skills and experience and be well-versed in real world MUSE/UAS systems and operations. The Lead shall have at least five (5) years of skills and experience with MUSE/BV.

Global Twins Key Personnel

Cybersecurity Program Analyst Lead:

The Cybersecurity Program Analyst Lead shall have a minimum of a bachelor's degree, and a minimum of five (5) years of relevant experience. The Cybersecurity Program Analyst Lead shall have knowledge in Department of Defense (DoD) cybersecurity requirements and accreditation procedures. The Cybersecurity Program Analyst Lead shall possess a DoD approved Information Assurance Manager (IAM) Level II certification [CompTIA Advanced Security Practitioner (CASP), GIAC Security Leadership Certification (GSLC), Certified Information Security Manager (CISM) or Certified Information Systems Security Professional (CISSP)].

Database Developer:

Extremely proficient in relational database development and GUI with a minimum of five (5) years of relevant experience. Familiar with implementing relational databases on a SQL server within a secure DoD cloud CE. Possesses capability to work independently within the boundaries of a supervisor's guidance and direction, think critically, with an emphasis on attention to detail. Possesses and can maintain a Secret clearance. Possesses required CE, Cyber Security/Information Assurance Technical Level, and web/application development certifications to perform database development with a GUI accessible to users within a secure DoD cloud CE; examples include but not limited to: Microsoft SQL Database Development and Comptia Security +. Possesses working knowledge of hardening database(s) utilizing Security Technical Implementation Guides (STIGs) and familiarity operating under National Institute of Standards and Technology (NIST) Security Controls that will impact database implementation. Executes Nondisclosure Agreement to ensure that sensitive financial data is protected and not shared with unauthorized individuals. - Possesses experience developing database(s) with Data Transformation Services (DTS).

TPO Constructive Key Personnel

JLCCTC Technical Team Lead:

The JLCCTC Technical Team Lead shall have: A minimum of three (3) years of experience as a simulation technician. JLCCTC Technical Team Lead shall have experience leading technical teams and Army training simulation exercise design and management; knowledge in JLCCTC software development, VV&A, networking, Microsoft Windows, Linux family of operating systems, and virtualization. JLCCTC Technical Team Lead shall have knowledge in setting up and operating JLCCTC software testing, analysis, troubleshooting, test writing, Problem Tracking Report (PTR) writing, technical analysis, help desk support, demonstrated problem solving capability, briefing technical status and issues. JLCCTC Technical Team Lead shall have experience in linkages with other services simulations and federations (JLVC, IEWTPT, JTTI+K, AWSIM, etc.); and a Bachelor's degree from an accredited institution in a technical discipline.

WARSIM Simulation Specialist:

The WARSIM Simulation Specialist shall have: A minimum of three (3) years recent experience with WARSIM in a JLCCTC environment. Expert knowledge is defined as experience and appropriate certification in JLCCTC capability development, VV&A, and user support. Expert knowledge in all functional aspects of WARSIM and its interaction with other JLCCTC federates and other federations that JLCCTC links to for exercises. WARSIM Simulation Specialist shall have knowledge of JLCCTC database administration. WARSIM Simulation Specialist shall have knowledge in planning and executing Army training exercises using training simulations. WARSIM Simulation Specialist shall have experience in developing & executing functional vignettes and planning and executing OREs for validation events. WARSIM Simulation Specialist shall exhibit knowledge in all aspects of military doctrine at the Battalion through Army level operations and command and staff training at those levels. WARSIM Simulation

Specialist shall have knowledge of joint and coalition operations, training management, and capability development. WARSIM Simulation Specialist shall have a bachelor's degree from an accredited university. Master's degree preferred.

MCS SME:

The MCS SME shall have a minimum of four (4) years' experience with MCS in a variety of environments. The MCS SME shall have experience in providing simulation-stimulation-MCS advice to support capability development, exercise support/construct and demonstrated expertise in capability development, VV&A, and user support. The MCS SME shall have Expert knowledge in all aspects of MCS – technical, functional, and database. The MCS SME shall have expert knowledge of MCS database administration in all Battle Functional Areas. The MCS SME shall have experience in developing & executing functional vignettes for test events and planning and executing OREs. The MCS SME shall exhibit knowledge in all aspects of Corps through BN level operations and provide expert advice on all aspects of MCS. The MCS SME shall have an Engineering Bachelor's degree and experience requirements describe above. In lieu of a Bachelor degree, the SME can have six (6) years MCS experience.

WIM Technical Team Lead:

The WIM Technical Lead shall have four (4) years of recent experience (within the past 7 years) with WIM (all enclaves) leading technical teams in JLCCTC VV&A activities, WIM software development, and networking experience. The WIM Technical Lead shall have experience with Microsoft Windows, Linux, and Solaris families of operating systems. The WIM Technical Lead shall have experience in setting up and operating WIM in the JLCCTC capability. The WIM Technical Lead shall have experience in use of Radiant Mercury and the Tactical Control Support Processor in a JLCCTC Architecture. The WIM Technical Lead shall have experience in software testing, analysis, troubleshooting, and writing Problem Trouble Reports. The WIM Technical Lead shall have experience in managing/providing help desk support, rendering technical advice, and offering WIM functional assistance. The WIM Technical Lead shall have experience in problem solving abilities. The WIM Technical Lead shall have a current SSBI and access to TS SCI.

TPO Virtual Gaming Key Personnel

Senior Hardware Software Engineer (Gaming Technologies):
Four (4) years of experience in leading technical teams in capability development, verification, validation and accreditation, software development and computer programming simulation integration. Four (4) years of experience in hardware and software standards and protocols, the ability to apply architectures to real-world requirements, and an understanding of communications systems and networks. Four (4) years' experience in modifying existing gaming software, game design, action-script programming and developing special purpose

software components to ensure efficiency and integrity between systems and applications. Experience with networking services such as Play Station Network (PSN), Xbox Live or Stream. Experience in writing programs using C++, MFC, C#, Python, Perl, Visual Basic, JAVA, XML, database programming. Experience in implementing, testing, debugging and maintaining engine and game play code. Experience in military doctrine and training management and capability development preferred. Master's degree or experience equivalent in technical disciplines such as engineering, mathematics, statistics, game development and related computer sciences in performing capability development and Research and Management R&M tasks.

HW/SW Engineer:

Candidate shall have four (4) years' experience in software development, simulation integration within the Microsoft Windows and Linux family of operating systems; to include expertise in hardware and software standards and protocols; ability to apply architectures to real world requirements utilizing current LVC&G platforms. Two (2) years of experience in software testing, analysis, troubleshooting, problem trouble reports development, management and documentation (PTRs), and operating current gaming suite toolkit (available at https://Milgaming.army.mil). Employee shall have the ability to write programs using C++, MFC, C#, Visual Basic, JAVA, XML, scripting languages, X programming and libraries and shall integrate networking packet protocols into simulation environments

HW/SW Engineer 3D Modeler:

Four years' experience in game design and development, 3D model development, and 3D programming by integrating 3D Models into game-based synthetic environments within the current gaming suite of tools. Background in the production and editing of game-based terrain databases from real terrain source databases; assist in integration efforts of game-based products to current Army simulation. Utilizing electronic file formats to include but not limited to Virtual Battlespace 3 (VBS3) .p3d & 3D Studio Max or MAYA 3D electronic file formats.

HW/SW Engineer LAB Configuration:

Four (4) Years' experience in the Information Technology / Telecommunications, Modeling & Simulations field. Knowledge in the planning, development, installation/maintenance and troubleshooting of LAN/WANS and cable systems. Experience in computer systems engineering and network specifications as they are related to product testing and evaluation. Experience with network products to include but not limited to Cisco, Nortel, DLINK and Lucent and LVC-G and STE technologies.

Systems Integrations Technician/Engineer:

Four (4) Years' experience in the Information Technology/Computer Science, C4I and C2 Systems and Systems Integrations. Knowledge in the development, installation, integration and

evaluation of all Battle and Mission Command Systems including but not limited to FBCB2, DXTRS, JCR, FIRESIM, SIMPLE, AFATDS, CPOF, JADOCS, AMDWS to COTS and GOTS simulations to including but not limited to VBS3 and other game based technologies.

TPO Synthetic Training Environment Key Personnel

Senior Hardware Software Engineer (Gaming Technologies):

Four (4) years of experience in leading technical teams in capability development, verification, validation and accreditation, software development and computer programming simulation integration. Four (4) years of experience in hardware and software standards and protocols, the ability to apply architectures to real-world requirements, and an understanding of communications systems and networks. Four (4) years' experience in modifying existing gaming software, game design, action-script programming and developing special purpose software components to ensure efficiency and integrity between systems and applications. Experience with networking services such as Play Station Network (PSN), Xbox Live or Stream. Experience in writing programs using C++, MFC, C#, Python, Perl, Visual Basic, JAVA, XML, database programming. Experience in implementing, testing, debugging and maintaining engine and game play code. Experience in military doctrine and training management and capability development preferred. Master's degree or experience equivalent in technical disciplines such as engineering, mathematics, statistics, game development and related computer sciences in performing capability development and Research and Management R&M tasks.

HW/SW Engineer:

Candidate shall have four (4) years' experience in software development, simulation integration within the Microsoft Windows and Linux family of operating systems; to include expertise in hardware and software standards and protocols; ability to apply architectures to real world requirements utilizing current LVC&G platforms. Two (2) years of experience in software testing, analysis, troubleshooting, problem trouble reports development, management and documentation (PTRs), and operating current gaming suite toolkit (available at https://Milgaming.army.mil). Employee shall have the ability to write programs using C++, MFC, C#, Visual Basic, JAVA, XML, scripting languages, X programming and libraries and shall integrate networking packet protocols into simulation environments

HW/SW Engineer 3D Modeler:

Four years' experience in game design and development, 3D model development, and 3D programming by integrating 3D Models into game-based synthetic environments within the current gaming suite of tools. Background in the production and editing of game-based terrain databases from real terrain source databases; assist in integration efforts of game-based products

to current Army simulation. Utilizing electronic file formats to include but not limited to Virtual Battlespace 3 (VBS3) .p3d & 3D Studio Max or MAYA 3D electronic file formats.

HW/SW Engineer LAB Configuration:

Four (4) Years' experience in the Information Technology / Telecommunications, Modeling & Simulations field. Knowledge in the planning, development, installation/maintenance and troubleshooting of LAN/WANS and cable systems. Experience in computer systems engineering and network specifications as they are related to product testing and evaluation. Experience with network products to include but not limited to Cisco, Nortel, DLINK and Lucent and LVC-G and STE technologies.

Systems Integrations Technician/Engineer:

Four (4) Years' experience in the Information Technology/Computer Science, C4I and C2 Systems and Systems Integrations. Knowledge in the development, installation, integration and evaluation of all Battle and Mission Command Systems including but not limited to FBCB2, DXTRS, JCR, FIRESIM, SIMPLE, AFATDS, CPOF, JADOCS, AMDWS to COTS and GOTS simulations to including but not limited to VBS3 and other game-based technologies.

CAC-TIF Key Scrum Team Skillsets

Programming and Game Integrated Development Environment (IDE) Development:
Support scripting using, but not limited to, C++, C#, Python, JAVA, XML, Unreal, Unity, Lumberyard, Microsoft Visual Studio, BiFrost, CyberBoss, and LUA Scripting Languages. Programmers shall be familiar with conventional design patterns (i.e. Command, Singleton, etc). Version control software (I.e. Git and/or Plastic) shall be utilized to enable collaboration on projects between multiple parties, including government design teams. The Contractor shall perform software analysis program scripting, testing, debugging and simulation integration to include recommended modifications of existing Virtual and Gaming game design, action-script programming, AR, VR and MR hardware and software integration and special purpose software components to ensure efficiency and integrity between systems and applications. The Contractor shall integrate COTS and GOTS hardware and software integration across simulator and simulation platforms. Support will include testing and modification of software code and script between multiple devices to enable the display, interaction, and resolution of effects generated by the simulations modeled behaviors. Additionally, the contractor will provide written documentation releasable to the force on the integration of hardware and software enabling simulations and simulators the ability to add peripherals to the currently configured baseline.

3D Modeling, Texturing, and Animation:

Provide texture, rigging, animation, integration, testing and validation of 3d models utilizing various platforms to include but not limited Synthetic Training Environment (STE) product line accepted software, Autodesk 3D Studio Max, Maya, Substance Painter, Quixel Suite, Marmoset

Toolbag, Adobe Creative Cloud, and Adobe Photoshop. 3D models shall include a high polygon model (20,000+ polygons), a mobile ready model (<5,000 polygons). Producing functional and static models per sprint that include but are not limited to visual components and scripted functionality to commercial industry standard using Government provided software (3D Studio Max, MAYA or similar industry standard software). Models shall be 100% functional, reflect equipment specific characteristics and provide an accurate visual, physical and performance representation of the modeled equipment and/or person

User Experience and Interface Design Requirements:

Design and shape unique, user-centric products and experiences. Able to make deliberate design decisions and to translate any given user-experience journey into a smooth and intuitive interaction. Conduct industry research and stay up to date on best practices, competitor UI designs and emerging technologies. The Contractor shall make strategic design and user-experience decisions related to core, and new, functions and features, and identify design problems and devise innovative solutions. Research and showcase relevant trends and technologies from industry. Additionally, understand UX design best practices to design solutions, capable of supporting multimodal design, mobile-first and responsive design. Create, improve, and use wireframes, prototypes, style guides, user flows, and effectively communicate interaction ideas using any of these methods. The Contractor shall use common UI design deliverables (Sitemaps, user flows, wireframes, lo-fi and hi-fi layouts, prototypes). Manage design libraries and design systems with adherence to product branding requirements. The Contractor shall clearly and effectively communicate design processes, ideas, and solutions to teams and clients. Iterate designs and solutions efficiently and intelligently. The Contractor shall use industry tools for User Interface and User Experience design including but not limited to Photoshop, Sketch, Illustrator, InVision, UXPin, Quartz, InDesign, Axure, Balsamiq, Framer Basic, and Omnigraffle. Able to code using basic front-end languages including but not limited to HTML, HTML5, CSS3, and Javascript.

Multiplayer Networking:

The Contractor shall be capable of taking multiplayer game mode features from concept through to delivery by iterating, experimenting, and exploring various multiplayer feature designs; define and drive the design, requirements, and priorities; create and maintain quality design documentation. Capable of innovating in areas that push the boundaries of existing and nascent software as well as develop, improve, optimize and support core technologies. The contractor shall work with stakeholders on software teams to gather and incorporate feedback, needs, align expectations, support and educate in the use of shared technology and ultimately help realize their vision. Identify and address software shortfalls and improvements as well as creating tools / utilities to aid in usage / debugging / optimization. Profile and optimize existing systems. Work closely with other programming disciplines to achieve great multiplayer experiences in different software environments and modalities. Refactor and consolidate existing solutions, often developed within Scrum Teams, to enable them to be more broadly deployed. Strong programming skills in C++ and strong software engineering and debugging skills. Experience with TCP & UDP network protocols, familiar with NAT traversal, packet routing, OSI model.

Understand the mechanics of gameplay and the requirements of game engines. Integrate gameplay code with server engineering. Network programmers talk to gameplay programmers about delivering network functionality. They also work with platform holders and hosting providers. Design, develop and maintain libraries that facilitate multiuser features. Give work estimates and prioritize tasks in collaboration with peers and project management and complete all work in a timely basis. Capable of supporting multiengine, multiplatform and multi modal development.

Extended Reality Development:

The Contractor shall assess and evaluate the efficacy of virtual 2D and 3D model development, modification, and transferability between simulations, versions of simulations, and simulation modalities. Support will include coding, scripting, rendering, transferring, and modifying virtual content within, across, and between simulations and modalities. The Contractor shall research and implement the best XR platforms and tools needed for multimodal experiences across platforms. Develop realistic and immersive multimodal experiences, leveraging a variety of software platforms. Create experiences using dynamic gameplay-related systems. The Contractor shall support development using industry standard software and programing languages including but not limited to C++, Blueprint, Unity, Unreal Engine, SQL, Python, and JAVA. The Contractor shall support debugging and optimizing code on assigned projects. The Contract shall utilize 3D capture technology such as 3D scanning and photogrammetry. The Contractor shall build out large-scale user interfaces in industry standard programs in a scalable way. Develop custom training simulation software allowing people to train effectively, affordably, and safely within a multimodal environment. The Contractor shall support innovation through the creation of extended reality experiences, apps, and projects to create new knowledge and technology-rich experiential learning opportunities. The Contractor shall consult with faculty and students to help troubleshoot project challenges and provide recommendations and training on specific extended reality hardware, software, and experiences. The Contractor shall provide feedback on potential XR projects and collaborate with research teams on prototyping and project development. Implement sustainable infrastructure, including documentation and versioning for ongoing XR projects. Provide input on technology purchases and refresh cycles.

General Graphic, Audio, Video Design:

The Contractor with support every CAC-TIF project with media design packages; to include but not limited to Technical Design Drawings, Instructional Manuals, Diagrams, Production Documents, Slides, Signs, Animations, and Mobile Uploads. Products will range in complexity from full color single page to technical drawings and animated visual instructions that will be uploaded to various DoD and commercial websites. Complex products are normally completed within 16 hours of effort. The contractor shall incorporate 2d, 3d, and Mixed Reality imagery and simulations into video format supported by Audio/Video development and editing.

Security Management.

Security Requirements, Compliance and Support to JLCCTC cybersecurity. The Contractor shall comply with Intelligence Community (IC), DoD, Defense Intelligence Agency (DIA), DA, and local cybersecurity-related directives, instructions, and regulations. The Contractor shall meet the information system security requirements prescribed by AR 25-2 and the JLCCTC system security plans for SECRET and below systems and Director of National Intelligence (DNI) Intelligence Community Directive (ICD) 503 (ICD 503) and ICD 705-series for TS SCI systems. Ensure 100% compliance with requirement as described. Provide Microsoft Word document to the Government reporting when training has been completed, NLT 30 Sep, annually.

All contractor personnel requiring access to classified information/areas under this contract shall possess a personal security clearance equal to the level of classified information revealed. The contractor shall not release any classified information to unauthorized personnel. All personnel requiring access to classified information under this contract shall possess a final adjudicated security clearance and be a U.S. Citizen. Waivers may be granted by the MTC Director, on a case by case basis. Per AR 25-2 paragraph 4.14.2.a and table 4-2, individuals needing privileged level access to classified systems and devices are required to possess & maintain at least a favorable Single Scope Background Investigation (SSBI). The contract is for operational services and equipment operation on equipment that may contain classified information up to Top Secret (TS- SCI). The security requirements are in accordance with the attached DD Form 254. As required by the Risk Management Framework (RMF) & the National Industrial Security Program Operating Manual (DoD 5220.22-M), the contracted organization must implement an insider threat program that includes a cross- discipline insider threat incident handling team; insider threat incidents must be reported to the Information System Security Manager (ISSM) and the Security Manager.

1.1. **Access to a U.S. Classified Facility/Systems.** The contractor shall possess and maintain a SECRET facility clearance from the Defense Security Service. All contract employees, requiring access and performing work in support of this contract shall possess a minimum SECRET security clearance with US ACCESS from the Defense Industrial Security Clearance Office and verified through Defense Information System for Security (DISS). The company will have a law enforcement background check completed for all employees who will be entering Army- controlled installations or facilities. Documentation of these checks will be made available to the COR upon request. The company will submit a DISS visitor's request for MTC Directors approval seven days in advance of an event in accordance with MTC RMF policies and procedures, for all visiting contractor personnel. All non-U.S. citizens will not be granted access and will be escorted by cleared personnel at all times if entering Army-controlled installations or facilities.

1.2. **DD Form 254.** A Contract Security Classification Specification, DD Form 254, is specified for this task order and is incorporated as an attachment.

1.3. **Classified Disposition.** On final delivery of goods or services, or on completion or termination of the task order, the contractor shall return to the Government all classified material received or generated under the task order or destroy all classified material unless the KO authorizes in writing retention for a specific period. The COR must have knowledge of all classified material received or generated by the contractor under the task order.

1.4. **Simulation System Classification.** All simulations systems may operate in a classified mode based on customer requirements. Army Mission Command Systems (MCS) are classified systems, and all personnel require a current and valid security clearance at the SECRET Level. The Government retains the right to deny access to contract personnel that fail to obtain or maintain required security clearances. Failure to maintain a valid security clearance shall result in the contractor employee not being allowed to perform on this task order. Such failure of an employee does not relieve the contractor from timely performance of the task order requirements.

1.5. **Sensitive Compartmented Information (SCI) Access.** The contractor shall establish an Army Centralized Contracts and Security (ACCS) portal account with Intelligence and Security Command (INSCOM) by emailing cseoperations@mi.army.mil. The contractor shall insure the accurate CAGE codes registration with ACCS. The Contractor shall nominate personnel to receive SCI Indoctrination based on their duties and place of work; the Government SCI contract monitor will be the final approving authority regarding SCI indoctrinations.

1.6. **Access and handling of Classified Material.** The contractor shall comply with Federal Acquisition Regulation (FAR) 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with (1) the Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M), and (2) any revisions to DoD 5220.22-M, notice of which the Government will furnish to the contractor after contract award.

1.7. **Physical Security.** The contractor shall provide a Security Manager and Assistant Security Manager to perform physical security and access control at each MTC facility and campus operated by the contractor. The contractor shall adhere to all established DoD, Army, and local installation regulations, as well as Governmental Standard Operating Procedures (SOP) pertaining to physical security and access control and establish a system of accounting for all keys issued to contractors. Physical security includes but is not limited to the following activities: DISS qualified with a valid Personnel Security System Access Request (PSSAR), and letter of appointment, provide physical access to all MTC facilities for all scheduled training/non-training activities; briefing guards during training events; ensuring personnel granted access are not violating SOPs and DOD regulations during the conduct of training/non-training events; ensuring MTC facilities are properly secured during training/non-training events IAW Government SOPs and DOD regulations; correct when possible or report all violations as soon as they are found to the security manager and COR. Access control includes but is not limited to the following: verify clearances through DISS of all individuals requiring access to MTC facilities requiring a valid clearance; issue badges IAW MTC Physical Security SOP; provide access to facilities; monitor who was granted access to MTC facilities and their clearance levels, and maintain HPCON and FPCON procedures as directed.

1.7.1. The contractor shall maintain facility access/visitor control logs and maintain them in a single government accessible location in accordance with RMF policies and procedures.

1.7.2. The contractor shall be responsible for safeguarding all Government equipment, information and property provided for contractor use in accordance with MTC Physical

Security SOP and applicable Army Regulations. At the close of each work period, Government facilities, equipment, and materials shall be secured.

1.8. **Facility Access.** The contractor shall have access to the facilities required for the accomplishment of the training during normal operating hours and during designated exercise hours. Off duty contractor personnel shall not be present in the MTC facilities. Contractor access at other than above designated times requires the MTC Director approval. Any external (NonMTC) contractor visits will be coordinated with the Government prior to the visit for approval and routed through the MTC Security Manager.

1.8.1. The Assistant Security Manager shall administer and manage the Electronic Security System (ESS). The ESS is comprised of 2 sub-systems. The Access Control System (ACS) and the Closed-Circuit Television (CCTV). This function is a system administrator (IATII Certification) position and must comply with DoD and Army training requirements in DoD 8140.01, DoD 8570.01-M, and AR 25-2.

1.9. **Key Control.** Government will issue keys to contract personnel. Contractors will account for Government issued keys IAW procedures outline in AR 190-11, chapter 3-8. NOTE: All references to keys include key cards. Keys issued to the contractor by the Government shall not be duplicated. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Government representative. The contractor shall prohibit the use of Government-issued keys/key cards by any persons other than the contractor's employees specifically performing under this task order unless directed by Government personnel. The contractor shall prohibit the opening of locked areas by contractor employees to permit entrance of persons other than contractor employees specifically engaged in the performance of assigned work in those areas, or personnel authorized.

1.10. **Secure cabinet combinations.** The contractor shall establish and implement methods of ensuring that all lock combinations on current and any future locking devices are not revealed to unauthorized persons. The contractor shall ensure that the Government representative is aware when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the contractor's Quality Control Plan.

1.11. **Operational Security (OPSEC).** Per AR 530-1, Operations Security, The Contractor shall comply with all applicable Department of Defense (DoD), Department of the Army, and local security regulations and procedures during the performance of this TO. The Contractor shall not disclose, and must safeguard, procurement sensitive information, computer systems and data, Privacy Act data, and Government personnel work products that are obtained or generated in the performance of this TO. New contractor employees must complete Level I OPSEC training within 30 calendar days of reporting for duty. This training is Online and is accessed by URL: https://iatraining.us.army.mil/. This training normally takes less than one (1) hour to complete. Neither the Contractor nor any of its contract service providers shall disclose or cause to disseminate any information concerning operations of military activities to unauthorized personnel. Such action(s) could result in violation of the contract and possible legal actions. Questions concerning OPSEC should be directed to the requiring activity OPSEC Officer.

1.11.1. iWATCH Training. The Contractor The contractor and all associated subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award with the results reported to the COR NLT 30 calendar days after contract award. New employees commencing performance after contract award must complete iWATCH Training within 30 calendar days.

1.11.2. Eligibility Verification for Employment. E-Verify is an Internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data from U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility. The U.S. Department of Homeland Security is working to stop unauthorized employment. By using E-Verify to determine the employment eligibility of their employees, companies become part of the solution in addressing this problem. All U.S. employers must complete and retain a Form I-9 for everyone they hire for employment in the United States. This includes citizens and noncitizens. On the form, the employer must examine the employment eligibility and identity document(s) an employee presents to determine whether the document(s) reasonably appear to be genuine and relate to the individual and record the document information on the Form I-9. The list of acceptable documents can be found on the last page of the form. E-Verify is mandatory for employers with federal contracts or subcontracts that contain the Federal Acquisition Regulation E-Verify clause.

1.12. **Personnel Requirements.**

1.13. **Special Qualifications**. For Information Assurance (IA)/Information Technology (IT) Training. All contractor employees and associated subcontractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working in IA/IT functions must comply with DoD and Army training requirements in DoD 8140.01, DoD 8570.01-M, and AR 25-2. The following qualifications/certifications are required to perform under this task order for all personnel serving as systems administrators (SA), network administrators (NA), and managers of personnel serving as SA and NA:

- Information Assurance Technology Level 1 (IATI) Baseline and Computing Environment certifications
- Information Assurance Technology Level 2 (IATII) Baseline and Computing Environment certifications
- Information Assurance Management Level 1 (IAMI) Baseline certifications.
- Information Assurance Management Level 2 (IAMII) Baseline certifications

1.14. **Computing Environment.** In accordance with DoD 8570.01-M, contractors shall obtain the appropriate DoD-approved IA baseline certification prior to being hired. No exceptions to this requirement will be given. The Government will consider the designated position unfilled until the individual has met baseline certification requirements for his/her position. The contractor shall ensure appropriate contractor personnel have baseline and computing environment certifications for IATI, IATII, IAMI, AND IAMII. Contractors are

granted six months from date of employment to obtain computing environment certifications. IATs must obtain appropriate Computing Environment (CE) certifications for the components, devices and operating system(s) they support as required by the task order.

1.15. **Information Assurance (IA) Awareness.** All contractor employees and associated subcontractor employees must complete the DoD Cyber Awareness Challenge Training and read/sign a computer Acceptable Use Policy Agreement before issuance of network access and annually thereafter.

1.16. **Army Training Certification Tracking System (ATCTS) Registration.** All contractor employees with access to a government information system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services. The contractor shall register, update, and maintain the following information for all employees registered in ATCTS:

- Username that includes AKO and Enterprise
- User's Supervisor
- Contract number and expiration
- Personnel Security Clearance
- Personnel Security Standard Code
- Profile assignment
- Position as defined by AR25-2
- DoD Cyber Workforce Framework (DCWF) Work Role (s) assigned
- Privileged Access Agreement signature date
- Duty appointment letter signature date
- Acceptable Use Policy signature date
- SAAR /DD2875 signature date
- DOD Baseline certification
- Computing Requirement certification

When training is identified due to equipment/system fielding that is not related to baseline IA certification, but is required to accomplish PWS tasks, the Government will provide the training.

1.1.1. The contractor is responsible for in-processing, out-processing, and management of the required certification documentation, appointment orders, and privileged access agreements of their employees on the Army's ATCTS database. The contractor will assist the MTC ISSM in validating contractor positions requiring privileged level access to an information system, quarterly.

1.17. **Government Required Training.** The contractor shall ensure contract staff attends/or takes online courses for required Army training provided on each installation. This training includes but is not limited to Anti- Terrorism Training, TARP/OPSEC training, and Information Assurance (IA) Awareness.

1.18. **Personnel Qualifications.** Contractor employees working under this task order shall be able to fluently speak, read, understand, and write the English language. The contractor shall maintain records of employees' qualifications, certifications, and licenses. The contractor personnel must meet the conditions contained in AR 25-2 and AR 380-67 in relationship to

obtaining access to Automated Information Systems (AIS) processing of classified information to fulfill their duties.

1.19. **Conduct of Contractor Personnel**. The contractor shall be responsible for the performance and always conduct of contractor and subcontractor employees. Personnel employed by the contractor in the performance of this task order or any representative of the contractor entering the Installation shall abide by the security regulations listed in the base contract and this task order and shall be subject to such checks by the Government as deemed necessary. Contractor ensures all personnel adhere to standards of behavior that reflect favorably on their employer and the federal government.

1.19.1. The contractor is responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity. Contractor will be held responsible for taking disciplinary action with respect to their employees as necessary.

1.19.2. The contractor shall present itself, and conduct all training, in a professional manner as to bring credit to the Government and contractor organization. The contractor shall ensure that all contractor employees working under the task order maintain a neat, well-groomed appearance always while on duty about the immediate task at hand. The wearing of military uniform items by contractor employees at any time while working under the task order is prohibited.

Information Assurance Security Management.

The Contractor shall perform vulnerability assessments using the Government provided Army approved tools, Security Technical Implementation Guides (STIG), checks, and Government provided baseline compliance tools to create and maintain artifacts to demonstrate baseline compliance and complete the Body of Evidence (BoE), which includes creation and maintenance of artifacts. TPO C Systems fall under Configuration Management (CM). System vulnerabilities or security findings are addressed within the CM Plan. If the Contractor identifies an issue that requires system changes, he or she shall complete a Problem Trouble Report (PTR) detailing the issues, submit the PTR to the system site Government lead for review. Vulnerability details must be protected at the system classification level. The Contractor shall submit the written reports to the Government ISSM. SAs shall perform vulnerability assessments and IA support activities, using Government provided Army approved tools under direction of an ISSO in support of VV&A, Maintenance Release and User Assessment events and to maintain JLCCTC systems IAW their approved baselines. The number of specific systems to be assessed varies but shall average approximately 30; vulnerability assessments shall include the JLCCTC, OneSAF, and DXTRS and take place within the NSC. Contractor initiated system functional and/or configuration changes and/or modifications are not authorized. Support twelve (12) vulnerability assessment reports (either for each event or once per month) in accordance with system classification. Provide two (2) written reports per vulnerability assessment. The first report is an unclassified executive summary that tallies the total numbers of high, medium, and low vulnerabilities discovered during the vulnerability assessment without detailing the vulnerability to the system. The second report is a classified (at the level of the tested system) technical report that includes specific details of the individual vulnerabilities on each system identifying each system assessed. Format for both reports

are IAW the Government provided Army approved tool used. Both reports are due to the system Government lead or system ISSM NLT one (1) business day after completion of the vulnerability assessment.

1. The Contractor shall perform IA and configuration management CM support activities, and security audit collection and provide the records of such activities (including audit archives, vulnerability assessment reports, etc.) on TPO-C JLCCTC simulation systems, to the Government ISSM as artifacts in the system BoE. Conduct IA and CM support activities to support VV&A, Maintenance Release, and User Assessment events. Provide associated reports. Submit IA and CM reports to the TPO-C Government ISSM using the Government-provided tools NLT 2 business days after event completion. Conduct monthly security audit log collection, archived on removable optical media (e.g., DVD), and provided to the TPO-C Government ISSM.

2. The Contractor shall maintain current copies of JLCCTC related Assessment and Authorization (A&A) documents such as current ATOs, RMF Assess Only Approval and IA-related documents on the NSC SharePoint. Maintain copies of the RMF/ICD 503 authorization decisions (e.g., ATO) for the JLCCTC systems, 'Friend of the Family' simulations, and associated networks. Archive documents on the TPO-C SharePoint Site and notify the appointed the TPO-C Government ISSM via e-mail when documents are filed. Archive documents NLT two (2) business days of dated receipt of document.

3. The Contractor shall support the Government-provided plan for Information Assurance Vulnerability Management (IAVM) dissemination, reporting, and compliance procedures. The Contractor shall conduct vulnerability assessments IAW AR 25-2 for each VV&A and test event to enable the TPO-C ISM to properly analyze the risks to IS and determine compliance with the approved baseline. Provide IAVM, vulnerability assessment support for Verification, Validation and Validation, and Accreditation, Maintenance Release and User Assessment Events.

4. The Contractor shall support the TPO-C Government ISSM in identifying unauthorized access to information, any system failure, and any suspected defect that could lead to an unauthorized disclosure, loss of integrity, or unavailability of system information. Provide Incident Report for each security or Information Assurance violation immediately to Government appointed lead. The Contractor shall report incidents within the NSC to the ISSM and or NSC Security Manager upon discovery and within the terms of the NSC Security SOP.

5. The Contractor shall support and assist in the management of Contractor Employees' Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS) accounts for the TPO-C area of responsibility. Support shall include providing information on employees requesting access to SIPRNET and JWICS to the NSC Information Management Officer (IMO) and training the new SIPRNET and/or JWICS users. Deliver written requests for access to SIPRNET and/or JWICS. Products shall be 100% factual concerning requesting individuals and contain no more than two (2) typographical errors about other information. Provide technical assistance to the requesting individual in

the proper access and navigation of the SIPRNET and JWICS IAW the standards taught in the training, ensure each requesting individual can access and navigate the systems without assistance, and assure the individuals' sign the SIPRNET and JWICS Acceptable Use Policies (AUPs) and DD Form 2875, as applicable. Compliance with AUPs and DD Form 2875 is 100%. Using a government-provided format, provide a Microsoft Word document to the NSC Information Management Office (IMO). Provide AUPs signed by requesting individuals to the NSC IMO. Notify NSC IMO via e-mail when training is complete for each individual and NLT five (5) business days after the request made by the individual is initiated.

6. The Contractor shall provide Contractor a Special Security Monitor (CSSM) for each shift and the Contractor shall determine the number of shifts. The CSSM, is responsible for shift security management and implementation of SCI security and administrative instructions for the NSC Sensitive Compartmented Information Facility (SCIF). The CSSM will be appropriately SCI-indoctrinated, appropriately trained as an SSR, and appointed on orders.

7. Contractor shall be 100% compliance with the following requirements. There shall be no loss or misuse of SCI materials, combinations, Information System (IS) passwords, equipment, and facilities. There shall be no SCI security violations. The Contractor shall support ten (10) VV&A, Maintenance Release, or User Assessments events. To ensure the Contractor meets these requirements, the Government will observe, review, and inspect the Contractor, as required for each event and occasionally during daily maintenance and training activities.

8. The Contractor shall provide shift/duty CSSMs. The CSSM, is responsible for shift security management and implementation of SCI security and administrative instructions for the NSC SCIF.

9. The Contractor shall assist the Special Security Representative (SSR) to maintain applicable SCI directives, regulations, manuals, SOP, and guidelines to adequately discharge SSR duties and responsibilities.

10. The Contractor shall ensure SCI is properly accounted for, controlled, transmitted, transported, packaged, and safeguarded.

11. The Contractor shall ensure SCI is disseminated only to persons authorized access to the material and having an established need-to-know.

12. The Contractor shall serve as the official channel for certifying and receiving SCI visitor clearances/ accesses. When a CSSM is on duty and no Government SSR is on duty, CSSM only allows access to those with proper security clearances and access. CSSM shall use the Government provided access roster.

13. The Contractor shall complete continuing SCI security education training and awareness program to keep apprised of the requirements and guidelines for protecting SCI. The Contractor shall ensure 100% compliance with requirement. The Contractor shall complete annual SCI training NLT 30 Sep, and complete periodic CSSM training and information

sessions as required by the Government and the SSO. All these training requirements shall use Government-provided materials. The Contractor shall complete periodic SSR training as required for each event and occasionally for daily maintenance activities.

14. The Contractor shall ensure accreditation documentation is available for the NSC SCIF and the communications/automated information systems under the organizations security cognizance. Contractor shall ensure 100% compliance with requirement. During the shift, the Contractor shall ensure that there is no loss or misuse of SCI materials, combinations, IS passwords, equipment, and facilities for contractor personnel on shift. Contractor shall ensure there are no SCI-related security violations. Contractor shall support ten (10) VV&A, Maintenance Release, or User Assessments events. To ensure the Contractor meets these requirements, the Government will observe, review, and inspect as required for each event, and occasionally during daily maintenance and training activities.

15. The Contractor shall maintain continuing liaison as required with non-SCI security officials such as the NSC security officers. The Contractor shall ensure 100% compliance with requirement. The Contractor shall ensure that there is no loss or misuse of SCI materials, combinations, IS passwords, equipment, and facilities by Contractor personnel on shift. The Contractor shall ensure there are no SCI-related security violations. The Contractor shall support ten (10) VV&A, Maintenance Release, or User Assessments events. To ensure the Contractor meets these requirements, the Government will observe, review, and inspect the Contractor as required for each event, and occasionally during daily maintenance and training activities. To ensure the Contractor meets these requirements, the Government will observe, review, and inspect the Contractor as required for each event, and occasionally during daily maintenance and training activities.

16. The Contractor shall provide a Test Team within the NSC to evaluate JLCCTC capabilities, selected partner system simulations, and user recommended simulations, for inclusion into the JLCCTC architecture prior to JLCCTC training WFX and CPX3 exercises and events. The scope of the support shall include planning, suite construction and execution of complete end-to-end testing and connectivity from the Simulation to the MCS. Plan and Execute six (6) JLCCTC test events per year. Support &/or testing shall be conducted IAW NSC Test planning. Provide input to Event Lead describing any Simulation to MCS issues, PTRs, and availability. Provide daily updates on issues being worked/solved. At the conclusion of the event provide the JLCCTC Government Lead a report in MS Word format with less than four errors. Report is due NLT the 5th business day after the event.

17. The Contractor shall build & sustain the DXTRS terrain loads. This includes but not limited to DTED & CADRG Maps and Maneuver Networks to support the TRADOC CoEs/Schools and other users. Build & sustain the DXTRS terrain loads. Plan on up to ten (10) complete terrain packs and maintain the loads as part of the GST base or on SharePoint. The Contractor shall have up to thirty (30) days to build DXTRS Terrain Load with less than 10% errors. Provide weekly updates on issues being worked/solved. At the conclusion of the load provide the DXTRS Government Lead a report in MS Word format with less than four errors. As requested by the user and approved by the DXTRS Government lead.

Data Rights: {If data is to be produced, furnished, acquired, or used in meeting contract requirements, delineate the respective rights and obligations of the government and the contractor regarding the use, production, and disclosure of that data.}

Section 508 – Electronic and Information Technology Standards: {When information technology is to be acquired, include language describing Section 508 requirements.} **Attachment:** {If applicable, include an Attachment stating Evaluation Factors and significant Subfactors representing the key areas of importance and emphasis to be considered in the source selection decision}

About the ICT Accessibility 508 Standards and 255 Guidelines

These standards address access to information and communication technology (ICT) under Section 508 of the Rehabilitation Act and Section 255 of the Communications Act. Section 508 of the Rehabilitation Act charges the Access Board with developing and promulgating this rule. The statute also charges the Access Board with providing Technical Assistance on Section 508, which is provided through webinars, trainings, and in close collaboration with GSA and materials available from Section508.gov.

Section 508 requires access to ICT developed, procured, maintained, or used by federal agencies. Examples include computers, telecommunications equipment, multifunction office machines such as copiers that also operate as printers, software, websites, information kiosks and transaction machines, and electronic documents. The Section 508 Standards, which are part of the Federal Acquisition Regulation, ensure access for people with physical, sensory, or cognitive disabilities.

The Section 255 Guidelines cover telecommunications equipment and customer-premises equipment — such as telephones, cell phones, routers, set-top boxes, and computers with modems, interconnected Voice over Internet Protocol products, and software integral to the operation of telecommunications function of such equipment.

Background

- February 3, 1998 – The Board publishes the original Telecommunications Act Accessibility Guidelines.
- December 21, 2000 – The Board issues the original Section 508 Standards.
- July 6, 2006 – The Board organizes TEITAC, the Telecommunications and Electronic and Information Technology Advisory Committee, to assist in updating the Section 508 Standards and Telecommunications Act Guidelines.
- April 3, 2008 – The Advisory Committee presents its final report to the Board.
- March 22, 2010 – The Board releases a draft proposed rule for public comment, docket ATBCB-2010-0001.
- December 8, 2011 – The Board issues a revised draft proposed rule for public comment, docket ATBCB-2011-0007.
- February 27, 2015 – The Board ICT proposed rule for public comment, docket ATBCB-2015-0002.
- January 18, 2017 – The Board issues the final rule, docket ATBCB-2015-0002-014.
- January 22, 2018 – The Board issues correction to the final rule to restore provisions for TTY access, docket document ATBCB-2015-0002-0146.

Additional Resources

- Section508.gov — GSA's Government-wide IT Accessibility Program
- Section 508 of the Rehabilitation Act (29 U.S.C. §794d)
- Final Regulatory Impact Analysis (FRIA)
- Comparison Table of WCAG 2.0 to Original 508 Standards
- Mapping of WCAG 2.0 to Functional Performance Criteria
- ICT Testing Baseline for Web Accessibility

Appendix A to Part 1194 – Section 508 of the Rehabilitation Act: Application and Scoping Requirements

508 Chapter 1: Application and Administration

E101 General

E101.1 Purpose

These Revised 508 Standards, which consist of 508 Chapters 1 and 2 (Appendix A), along with Chapters 3 through 7 (Appendix C), contain scoping and technical requirements for information and communication technology (ICT) to ensure accessibility and usability by individuals with disabilities. Compliance with these standards is mandatory for Federal agencies subject to Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d).

E101.2 Equivalent Facilitation

The use of an alternative design or technology that results in substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards is permitted. The functional performance criteria in Chapter 3 shall be used to determine whether substantially equivalent or greater accessibility and usability is provided to individuals with disabilities.

E101.3 Conventional Industry Tolerances

Dimensions are subject to conventional industry tolerances except where dimensions are stated as a range with specific minimum or maximum end points.

E101.4 Units of Measurement

Measurements are stated in metric and U.S. customary units. The values stated in each system (metric and U.S. customary units) may not be exact equivalents, and each system shall be used independently of the other.

E102 Referenced Standards

E102.1 Application

The specific editions of the standards listed in Chapter 7 are incorporated by reference into 508 Chapter 2 (Scoping Requirements) and Chapters 3 through 6 to the prescribed extent of each such reference. Where conflicts occur between the Revised 508 Standards and the referenced standards, these Revised 508 Standards apply.

E103 Definitions

E103.1 Terms Defined in Referenced Standards

Terms defined in referenced standards and not defined in E103.4 shall have the meaning as defined in the referenced standards.

E103.2 Undefined Terms

Any term not defined in E103.4 or in referenced standards shall be given its ordinarily accepted meaning in the sense that the context implies.

E103.3 Interchangeability

Words, terms, and phrases used in the singular include the plural and those used in the plural include the singular.

E103.4 Defined Terms

For the purpose of the Revised 508 Standards, the terms defined in E103.4 have the indicated meaning.

Agency

Any agency or department of the United States as defined in 44 U.S.C. 3502, and the United States Postal Service.

Alteration

A change to existing ICT that affects interoperability, the user interface, or access to information or data.

Application.

Software designed to perform, or to help the user to perform, a specific task or tasks.

Assistive Technology (AT)

Any item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities.

Audio Description.

Narration added to the soundtrack to describe important visual details that cannot be understood from the main soundtrack alone. Audio description is a means to inform individuals who are blind or who have low vision about visual content essential for comprehension. Audio description of video provides information about actions, characters, scene changes, on-screen text, and other visual content. Audio description supplements the regular audio track of a program. Audio description is usually added during existing pauses in dialogue. Audio description is also called “video description” and “descriptive narration”.

Authoring Tool

Any software, or collection of software components, that can be used by authors, alone or collaboratively, to create or modify content for use by others, including other authors.

Closed Functionality

Characteristics that limit functionality or prevent a user from attaching or installing assistive technology. Examples of ICT with closed functionality are self-service machines, information kiosks, set-top boxes, fax machines, calculators, and computers that are locked down so that users may not adjust settings due to a policy such as Desktop Core Configuration.

Content

Electronic information and data, as well as the encoding that defines its structure, presentation, and interactions.

Document

Logically distinct assembly of content (such as a file, set of files, or streamed media) that: functions as a single entity rather than a collection; is not part of software; and does not include its own software to retrieve and present content for users. Examples of

documents include, but are not limited to, letters, email messages, spreadsheets, presentations, podcasts, images, and movies.

Existing ICT

ICT that has been procured, maintained or used on or before January 18, 2018.

Hardware

A tangible device, equipment, or physical component of ICT, such as telephones, computers, multifunction copy machines, and keyboards.

Information Technology

Shall have the same meaning as the term "information technology" set forth in 40 U.S.C. 11101(6).

Information and Communication Technology (ICT)

Information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to: computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; Web sites; videos; and, electronic documents.

Keyboard

A set of systematically arranged alphanumeric keys or a control that generates alphanumeric input by which a machine or device is operated. A keyboard includes tactilely discernible keys used in conjunction with the alphanumeric keys if their function maps to keys on the keyboard interfaces.

Label

Text, or a component with a text alternative, that is presented to a user to identify content. A label is presented to all users, whereas a name may be hidden and only exposed by assistive technology. In many cases, the name and the label are the same.

Menu

A set of selectable options.

Name

Text by which software can identify a component to the user. A name may be hidden and only exposed by assistive technology, whereas a label is presented to all users. In many cases, the label and the name are the same. Name is unrelated to the name attribute in HTML.

Non-Web Document

A document that is not: a Web page, embedded in a Web page, or used in the rendering or functioning of Web pages.

Non-Web Software

Software that is not: a Web page, not embedded in a Web page, and not used in the rendering or functioning of Web pages.

Operable Part

Hardware-based user controls for activating, deactivating, or adjusting ICT.

Platform Accessibility Services

Services provided by a platform enabling interoperability with assistive technology. Examples are Application Programming Interfaces (API) and the Document Object

Model (DOM).

Platform Software

Software that interacts with hardware or provides services for other software. Platform software may run or host other software, and may isolate them from underlying software or hardware layers. A single software component may have both platform and non-platform aspects. Examples of platforms are: desktop operating systems; embedded operating systems, including mobile systems; Web browsers; plug-ins to Web browsers that render a particular media or format; and sets of components that allow other applications to execute, such as applications which support macros or scripting.

Programmatically Determinable

Ability to be determined by software from author-supplied data that is provided in a way that different user agents, including assistive technologies, can extract and present the information to users in different modalities.

Public Facing

Content made available by an agency to members of the general public. Examples include, but are not limited to, an agency Web site, blog post, or social media pages.

Real-Time Text (RTT)

Communications using the transmission of text by which characters are transmitted by a terminal as they are typed. Real-time text is used for conversational purposes. Real-time text also may be used in voicemail, interactive voice response systems, and other similar application.

Revised 508 Standards

The standards for ICT developed, procured, maintained, or used by agencies subject to Section 508 of the Rehabilitation Act as set forth in 508 Chapters 1 and 2 (36 CFR part 1194, Appendix A), and Chapters 3 through 7 (36 CFR part 1194, Appendix C).

Software

Programs, procedures, rules, and related data and documentation that direct the use and operation of ICT and instruct it to perform a given task or function. Software includes, but is not limited to, applications, non-Web software, and platform software.

Software Tools

Software for which the primary function is the development of other software. Software tools usually come in the form of an Integrated Development Environment (IDE) and are a suite of related products and utilities. Examples of IDEs include Microsoft® Visual Studio®, Apple® Xcode®, and Eclipse Foundation Eclipse®.

Telecommunications

The signal transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Terminal

Device or software with which the end user directly interacts and that provides the user interface. For some systems, the software that provides the user interface may reside on more than one device such as a telephone and a server.

Text

A sequence of characters that can be programmatically determined and that expresses

something in human language.

TTY

Equipment that enables interactive text based communications through the transmission of frequency-shift-keying audio tones across the public switched telephone network. TTYs include devices for real-time text communications and voice and text intermixed communications. Examples of intermixed communications are voice carry over and hearing carry over. One example of a TTY is a computer with TTY emulating software and modem.

Variable Message Signs (VMS)

Non-interactive electronic signs with scrolling, streaming, or paging-down capability. An example of a VMS is an electronic message board at a transit station that displays the gate and time information associated with the next train arrival.

Voice over Internet Protocol (VoIP)

A technology that provides real-time voice communications. VoIP requires a broadband connection from the user's location and customer premises equipment compatible with Internet protocol.

Web page

A non-embedded resource obtained from a single Universal Resource Identifier (URI) using HyperText Transfer Protocol (HTTP) plus any other resources that are provided for the rendering, retrieval, and presentation of content.