INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEM-VI (ICIDS-VI) PRODUCTION

STATEMENT OF WORK

16 June 2022

Product Manager Force Protection Services (PM FPS)
5900 Putnam Road
Fort Belvoir, VA 22060-5420

Intentionally Left Blank

Table of Contents

SECTION C – STATEMENT OF WORK (SOW)

1. INTRODUCTION

The objective of this acquisition is to provide Integrated Commercial Intrusion Detection System-VI (ICIDS-VI) hardware and software for multiple Military Installations. ICIDS-VI provides intrusion detection capabilities for Installation Commanders to protect Government assets and information. ICIDS-VI consists of Commercial-Off-The-Shelf (COTS) equipment, interior and exterior sensors, Local Control Station Console (LCSC), System Administrator Station Console (SASC), Premise Control Unit (PCU), Closed Circuit Television (CCTV), and Entry Control Equipment (ECE).

1.1 ICIDS-VI Performance Capabilities

The Contractor shall install an ICIDS-VI System that integrates the Contractor Furnished Equipment (CFE) and existing Government Furnished Property (GFP) to meet the requirements of this SOW and System Performance Specification (SPS). This effort includes:

- Engineering Support Test Laboratory (ESTL)
- Intrusion Detection System (IDS) Site Survey (SS)
- Site Specific Engineering Design (SSD)
- Site Preparation to include Network connections
- Installation Materials
- One Year Warranty
- Operator, Systems Administrator, Sensitive Compartmented Information Facility (SCIF) and Maintainer Training
- System Performance Verification (SPV) and Government Endurance Testing (ET)
- Technical Manual (TM)

The system shall be a reliable, modular, scalable, open architecture for system and subsystem design supporting lifecycle supportability and capability growth. The ICIDS-VI solution shall be based on integrated system performance, industry best practices, long-term availability and supportability. The Contractor shall be responsible for maintenance and cybersecurity requirements for ICIDS-VI system.

1.2 Concept of Operations (CONOPS)

ICIDS VI is a System of Systems of complementary physical security capabilities fielded at Army/Joint installations. It provides physical security capabilities within Army/Joint Installation and monitored from a regional command and control station hosting multiple Army/ Joint installations. Figure 1 shows the notional regional monitoring concept. Figure 2 shows the notional ICIDS VI architecture within each Installation.

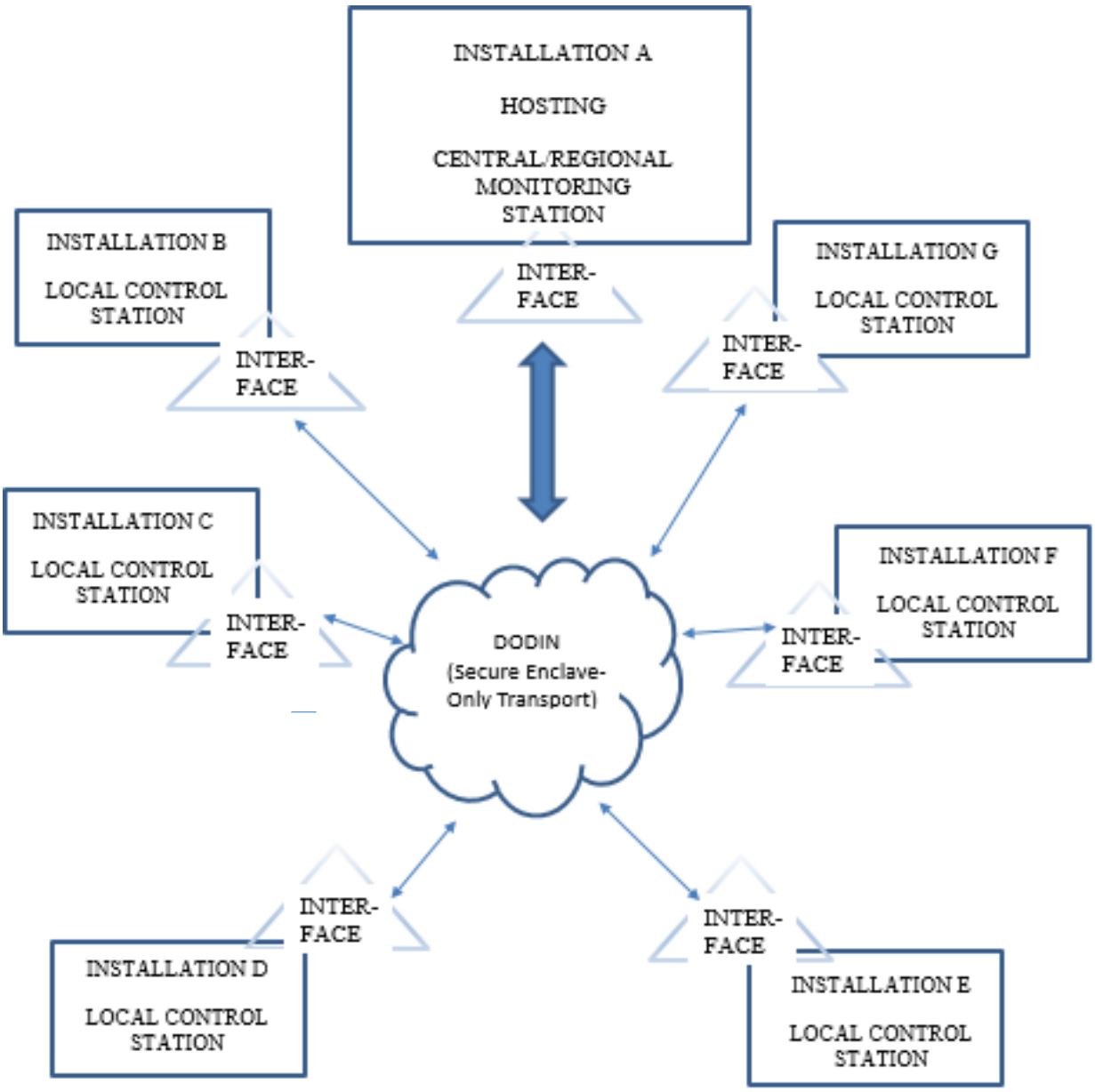

Figure 1. ICIDS Functional Architecture Central/Regional Monitoring Station.

NOTES:

1. Diagram describes functional requirements and is not a design constraint.
2. INTERFACE – interoperability and encryption capabilities between installation system and central monitoring system.

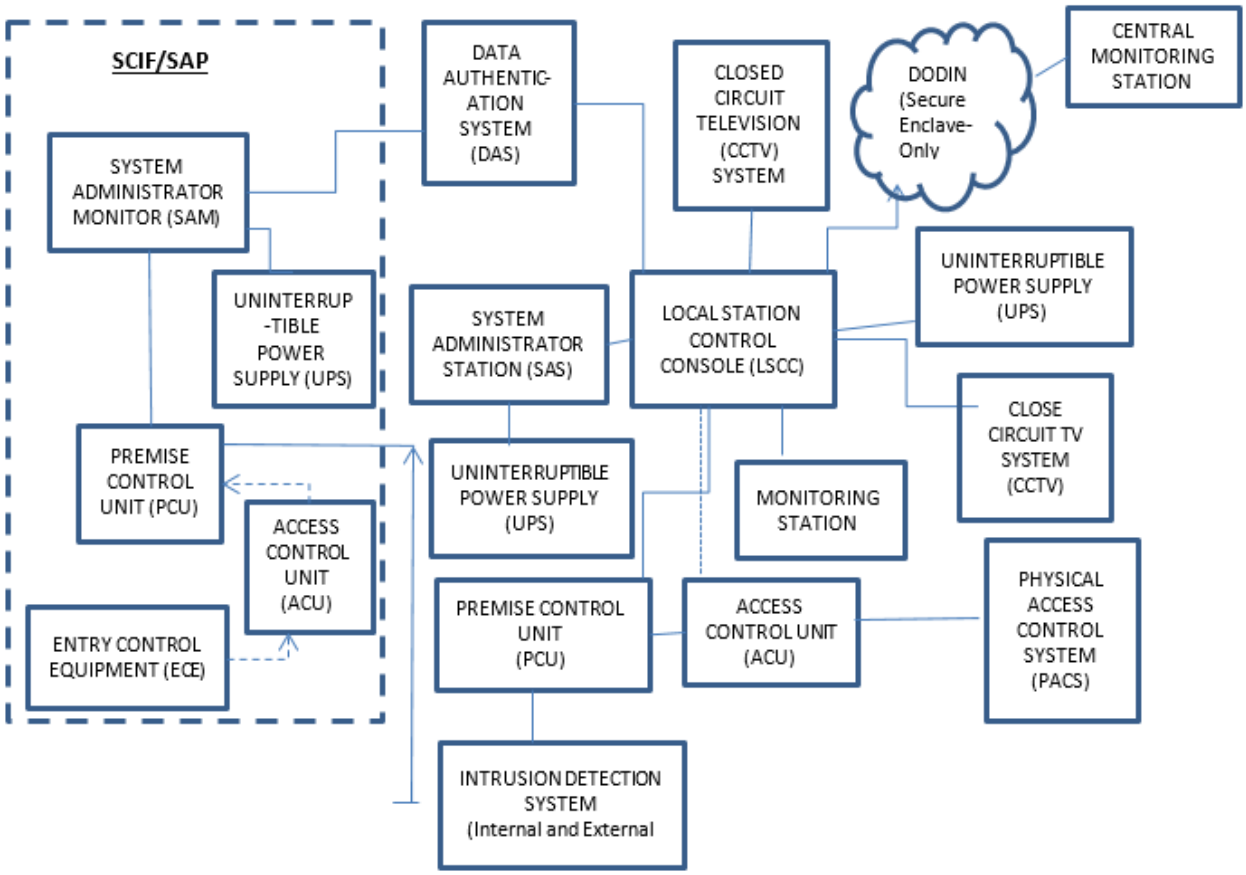

Figure 2. ICIDS Functional Architecture Local Control Station (LMS) at Installation.

NOTES:

1. Diagram describes functional requirements and is not a design constraint.
2. Quantities and types of components will vary with each installation.

1.3 ICIDS-VI Sites

ICIDS-VI shall be delivered and installed inside Continental United States (CONUS) or Outside Continental United States (OCONUS). ICIDS-VI Fielding Schedule is listed in Section J Attachment 0006, subject to funding and priority for execution. The Contractor shall coordinate theater clearance or Status of Forces Agreement (SOFA) requirements for OCONUS sites as necessary, see paragraph 7.0.

1.3.1 ICIDS-VI Delivery Order (DO)

The Contractor shall propose and execute individual DOs after contract award for support, to include but not limited to, management, survey, design, installation, testing, training, manuals, modifications, and requirements as requested by the Government.

2. APPLICABLE DOCUMENTS

References are shown in Section J Attachment 0004. If a document is referenced in this SOW without indicating any specific paragraph as applicable, entire document applies.

2.1 Order of Precedence

In event of a conflict between text and references, text of the SOW takes precedence followed by the SPS. This SOW does not supersede applicable laws and regulations.

3. REQUIREMENTS

3.1 General

The Contractor shall deliver fully functional ICIDS-VI Systems to designated Installations In Accordance With (IAW) the ICIDS-VI Contract and resulting DOs. The Contractor shall provide and maintain an ESTL.

3.2 Program Management

The Contractor shall implement, manage, update and maintain an Integrated Master Schedule (IMS). This information shall be presented for discussion at each Program Status Review (PSR) and delivered in the Contractor’s Progress, Status and Management Report (SMR) IAW Contract Data Requirements List (CDRL) A001. The Contractor shall produce and install ICIDS-VI IAW the Contractor's Government approved schedule. The schedule shall be used as a management tool to assess progress and status. The Contractor shall report on work in progress at the monthly PSR and in the SMR. The SMR shall provide the names, work location and current security clearance status of all personnel working on the contract, including training and certifications. The location for each PSR shall be at PM FPS, Ft. Belvoir, VA or the Contractor provided facilities.

The Contractor shall participate in a weekly meeting via telephone conference or in person with PM FPS to review status of cost, schedule and performance. The Contractor shall host a start of work meeting within 30 days after contract award. The Contractor shall provide the Government an agenda for approval seven calendar days prior to scheduled start of work meeting. The Contractor shall be responsible for recording the minutes of meetings conducted with the Government. The Contractor shall submit Report, Record of Meetings IAW CDRL A002.

3.3 ESTL

The Contractor shall establish, maintain and administer an ICIDS ESTL through end of the last warranty period. The Contractor shall provide space in ESTL for ICIDS-VI GFP. This equipment shall be installed, operated and maintained by the Contractor. The Government does not intend to provide any ICIDS-VI GFP for use in the ESTL. The Contractor shall use the ESTL for Performance Verification Test (PVT)-1 IAW paragraph 3.16.2. The ESTL will also be used for training, demonstration, validation and cyber security activities and assessment purposes IAW paragraph 3.13.6.2 Training Requirements, baseline validation and Cybersecurity assessment and updates and paragraph 3.13.6, Training and Training Support. The ESTL shall be used as a facility to test upgrades or modifications to the ICIDS prior to fielding changes at an operational site. The ESTL shall have a current baseline configuration to resolve issues that arise during fielding. The Contractor shall maintain the ICIDS-V baseline configuration at the ESTL (see Section J Attachment 0005 ESTL for ICIDS-V baseline). The ESTL shall be located not greater than a 30 miles radius from PM FPS, Fort Belvoir, VA. All component hardware, software, labor and facilities for the ESTL shall be provided by the Contractor. Upon completion of PVT-1, equipment shall remain for use in the ESTL for the life of the contract. The Government will take possession of ESTL equipment upon end of the last warranty period. The Government will witness all testing and evaluation as required.

3.4 Configuration Management (CM)

The Government is the CM decision authority. The Government will manage and chair the ICIDS-VI System Configuration Control Board (CCB) throughout its lifecycle. The Government will approve Class I or Class II designation for all changes. The Contractor shall participate, provide evidence/explicit explanation of changes and updates and support the CCB and conduct configuration control activities.

3.4.1 CM Requirements

The Contractor shall provide and execute an ICIDS-VI Configuration Management Plan IAW CDRL A003. The Contractor shall comply with the PM FPS CM procedures for all hardware, software and integration changes. The Contractor shall provide configuration item identification and control activities of all ICIDS-VI hardware and software as part of the CM process. All changes will be approved or disapproved by the CCB.

The initial configuration shall consist of materials as identified by the Contractor in the proposed solution. The Contractor shall notify the Contracting Officer (KO) within 60 days of product

availability changes, provide alternate courses of action and risk score if the old configuration will no longer be supportable. All recommended ICIDS-VI changes shall be submitted by Computer Software Product End Items, Software Upgrade, CDRL A004 or Commercial Drawings and Associated Lists, Hardware Upgrades, CDRL A005. Any request for change shall be accomplished with complete supporting documentation, including the need or reason for change and the price/schedule impact. Prior approval by the KO is required before any changes are implemented. If a reoccurring need is identified for a specific hardware and/or software item, the Contractor shall recommend the Government incorporate the item into the contract. The Government reserves the right to require the Contractor to provide additional supporting technical analysis and to specify additional testing to verify proposed change prior to approval. The price of configuration changes, other than hardware upgrades or those requested by the Government shall be the responsibility of the Contractor.

3.4.2 Physical Configuration Audit (PCA)

The PCA shall confirm proper execution of the Installation Engineering Plan (IEP), CDRL A006 and accuracy of the Commercial Drawings and Associated Lists, As-Built, CDRL A008. The Contractor shall provide and execute a Configuration Audit Plan – Physical Configuration Audit Plan, PCA IAW CDRL A009.

The Contractor shall conduct a PCA witnessed by the Government. The PCA shall be conducted after PVT-1, PVT-2, System Acceptance Testing (SAT) at Installations and any configuration changes. Upon completion of testing and correction of all failures, the system site configuration shall either confirm the baseline or identify corrections to the baseline for the ESTL and Installations. The results of the PCA shall be included in the Test Report for each testing event IAW CDRL A028 Test/Inspection Report, A034 Test/Inspection Report, and A040 Test/Inspection Report. The Contractor shall provide the PCA on 5% of installed PCU and 100% of the LSCC, Monitoring Stations and SAS.

3.4.3 Obsolescence/Diminishing Manufacturing Sources and Material Shortages (DMSMS)

The Contractor shall develop and implement an obsolescence/DMSMS Plan IAW CDRL A011. The Contractor shall conduct an obsolescence/DMSMS review that identifies and forecasts issues prior to installation. The Contractor shall provide recommendations on component replacements that provide equal or better performance. The Contractor shall prepare, maintain and deliver a listing of obsolete or DMSMS items.

3.5 Information System Security Engineering (ISSE)

The Contractor shall provide system level support IAW references, provisions of Department of Defense Instruction (DoDI) 8500.01, DoDI 8510.01, Army Regulation (AR) 25-1 and 25-2 (all sub applicable Department of the Army Pamphlets), Army Knowledge Management and Information Technology. The Contractor shall perform inputs for the ATO package utilizing eMASS portal.

The Contractor shall conduct Security Test and Evaluations (ST&Es) to assess the system's security posture in support of the Risk Management Framework (RMF) process or during major changes impacting computing environment or accreditation boundary. The ST&Es shall be conducted to uncover design, implementation and operational flaws that may affect the confidentiality, integrity and availability of the system. The Contractor shall support the Federal Information Security Management Act (FISMA) yearly assessments. The Contractor shall provide documents, data, certification tests results and access for major changes and re-certification.

The Contractor shall continuously assess and monitor security policies and procedures to incorporate an Information Assurance Vulnerability Management (IAVM) program as referenced under Cybersecurity Activities Support to DoD Information Network Operations dated 7 March 2016, and National Institute for Standards and Technology (NIST) SP800-40 Rev 4, Guide to Enterprise Patch Management Planning. The Contractor shall create Patch and Vulnerability Management plan and processes for the ICIDS-VI deployment and production environments IAW CDRL A012 Vulnerability Scan Compliance Report/DoD RMF Package Deliverables. The Contractor shall comply with the requirement for IA Vulnerability Alerts. The system is required to perform an end-to-end automated deployment of patches and updates to IT devices using enterprise patch management tools to include configuring access to the DoD Windows Server Update Services (WSUS) located on the DoD Patch Repository website. The Contractor shall deploy critical Microsoft patches within one week of notification publication by Microsoft and implement Microsoft System Center Configuration Manager (SCCM) to support deployment of updates that are not supported in WSUS. Any third party patches and software updates shall be coordinated by Contractor and applied within 30 days release of the version or update. The Contractor shall engineer and implement an automated, continuous on-line monitoring and audit trail creation capability with the ability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications. The capability shall be user configurable to automatically disable the system if serious IA or software violations are detected. The system shall employ an automated tool to review audit log records and reports. The system shall be designed with a hierarchical organizational unit (OU) structure that is adaptable and sustainable. The Contractor shall apply applicable DISA STIGs, checklists and along with that vendor security guidance, industry best practices and applicable vendor product security patches. The Contractor shall ensure applications are in compliance with DoD Instruction 8500.2 Information Assurance Implementation and DoDI 8551.1 Ports, Protocols and Services Management (PPSM). Contractor shall obtain DISA internet protocol address and register and get approval for Ports, Protocols and Services via Army PPSM office. The Contractor shall leverage automated tools to identify and remediate vulnerabilities or weaknesses in the application design or coding. The Contractor shall include in the CM plan how the ICIDS-VI systems delivered to the installations shall be updated as a result of changes to the baseline configuration.

The Contractor shall continuously maintain, review and assess the status of the system security and risk as it relates to Risk Management Framework Authority and Assess (A&A) process and DoD continues monitoring requirements, The Contractor shall identify any changes that would change the accreditation boundary, pose any risk impact current operation procedures, impact current content of technical manuals or require extended development or testing.

3.6 Information Assurance (IA)/Cybersecurity

The Contractor shall ensure ICIDS-VI obtains Army NETCOM Authority to Operate (ATO) for connection to an Installation's Virtual Local Area Network (VLAN) and any external network required to establish Central Monitoring concept of ICIDS VI.

The Contractor shall ensure that the ICIDS-VI System, if operational requirements arise, is capable of obtaining U.S Army Network Enterprise Technology Command (NETCOM) approvals to include but not limited to Authority to Connect (ATC), ATO, Request for Change to connect and Port, Protocol and Services (PPS) approvals for connection to an Installation's Non-secure Internet Protocol Router Network (NIPRNET) IAW NIST 800-53, NISTS 800-53A and CNSS instruction 1253, DoDI 8500.01, Cybersecurity DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), and Army NETCOM. The system shall be configured to comply with current and future Computer Network Defense directives (CND). The system shall be configured to comply with DoD Network and Cyber Security TASKORDs, OPORDS, FRAGOs, CTOs. The system shall be configured IAW DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling and Public Key Encryption, AR-2 to include applicable sub publications and other new Policy, Directive, Operational Orders, Cybersecurity Task Order and Publications. The Contractor should complete risk validation testing before A&A package is submitted for ATO approvals and continues monitoring. The Contractor shall implement and complete the comprehensive self-assessment with supporting system specific documentation upon receiving the Army's RMF policy guidance for operational testing approvals, Interim Authority to Test (IATT) and ATO approvals. The system shall utilize highest approved FIPS algorithm in place to encrypt all devices to include System logs. The Contractor shall account for and address all DoD IA Controls assigned to a designated categorization as High, Moderate or Low for each of the three security objectives Confidentiality, Integrity, Availability (CIA) Sensitive DoD IT system or the equivalent Risk Management Framework designation. The Contractor shall develop, track and resolve assigned IA controls including inherited controls Scorecard and IT Security Plan of Action and Milestone(s) (POA&M). The accreditation documentation shall be developed and delivered according to Information Systems Accreditation Documentation, CDRL A010, Information Systems Security Plan, Vulnerability Scan Compliance Report/ DOD Risk Management Framework (RMF) Package Deliverables, CDRL A012 and Information Assurance (IA) Design Review Information Package (DRIP) – Verification Matrix, CDRL A013. The plan(s) shall include the IA control implementation status, responsible entities, resources and the estimated completion date for each assigned IA control. Plan shall identify monthly requirements to ensure IA controls are corrected when new scans are run, how the updated baselines are sent to the field during the contract performance period as part of comprehensive and repeatable vulnerability requirements

The cybersecurity requirements for DoD IT shall be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37. All DoD Information Systems must be categorized IAW Committee on National Security Systems Instruction (CNSSI) 1253 and implement a corresponding set of security controls from NIST SP 800-53. The assessment procedures from NIST SP 800-53A and

DoD-specific assignment values, overlays, implementation guidance and assessment procedures shall be used. The Contractor shall be prepared to implement the Army's RMF processes and procedures upon receiving policy guidance.

The Contractor shall configure the ICIDS-VI IAW applicable Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs). STIGs should be identified for specific components, Operating System, Database, Metadata Technologies and document applicable DoD policies, security requirements, best practices and configuration guidelines. STIGs are associated with security controls through Control Correlation Identifiers (CCIs) which are decompositions of NIST SP 800-53 security controls into single, actionable and measurable items. Security Requirements Guides (SRGs) are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used. Control Correlation Identifiers (CCIs), RMF control family artifacts, scans, and STIGs shall be reviewed and updated at least annually as part of the Federal Information Security Management Act (FISMA) to ensure system security posture remains consistent with the accreditation baseline.

The Contractor shall use Security Content Automation Protocol (SCAP), appropriate and latest STIG and benchmarks, Security Readiness Review (SRR) scripts and Assured Compliance Assessment Solution (ACAS) is required to validate ICIDS-VI Baseline. STIG and SRG compliance results shall be provided in the form of STIG checklists as part of the Risk Management Framework (RMF) artifacts as required for the system lifecycle. This review ensures products will not introduce vulnerabilities into the hosting DoD Information System. The SCA's risk assessment will be used by the SCA to determine the level of overall system cybersecurity risk and a basis for recommendation of risk acceptance or denial to the Authorizing Official (AO), formerly the Designated Accrediting Authority (DAA). The SCA's risk assessment considers threats, vulnerabilities and potential impacts as well as existing and planned risk mitigation. The risk assessment will address all Non-Compliant (NC) controls and clearly communicate the SCA's conclusion on system cybersecurity risk and any recommendations for special instructions to accompany the authorization decision.

Actual results of the SCA's risk assessment are recorded in the SAR, formerly the DIACAP Scorecard and Plan of Action and Milestones (POA&M), as part of the security authorization package along with any artifacts produced during the assessment such as output from automated test tools or screen shots that depict aspects of system configuration.

Contractor shall submit for Government approval an overarching security plan IAW DoDI 8510.01 which describes their strategy for implementation, continues monitoring and maintenance of IA/Cybersecurity requirements throughout the life of the contract to include annual FISMA compliance. The security plan shall address the security controls described in NIST SP 800-53 and should be tailored in scope and depth appropriate to the effort and the specific unclassified DoD information. The Contractor shall include updates to all installed ICIDS-VI systems as a result of changes to the baseline configuration to support RMF through the end of the final warranty period.

The Contractor shall provide and execute an ICIDS-VI Information System Security Plan IAW CDRL A010. The plan provides an overview of security solutions for the system and describes security controls in place or planned. The security plan shall include implementation status, security control designation, responsible entities, resources and estimated completion dates. The security plan shall include a compiled list of system characteristics required for system registration and key security-related ICIDS-VI requirements unique to ICIDS-VI IAW NIST Risk Management Framework processes SP800-53 Rev 5, SP 53B, SP 80053A Rev 5 and SP800-53A Rev4. Government approval of the security plan, prior to implementation, also establishes the level of effort required to successfully complete the remainder of the steps in the RMF and provides the basis of the security specification for the acquisition of the system, subsystems or components. The AO's approval of the security plan must be documented in the security plan.

The Contractor shall deliver an ICIDS-VI solution and supporting artifacts that will achieve an Authority To Operate (ATO) accreditation decision for operation on a Army's LandWarNet which is based on achieving an ATO and maintaining an acceptable risk posture. The Contractor shall prepare and have the connection approvals ready for operational testing (IATT) if ATO is not ready and approved before operational testing. The ICIDS-VI shall be characterized as a "type authorization" which is used to deploy identical copies of a DoD Information System in specified environments. This method allows a single security authorization package to be developed for an archetype (common) version of a system. The system can then be deployed to multiple locations with a set of installation, security control and configuration requirements or operational security needs that will be provided by the hosting enclave.

The Contractor shall execute corrective actions to resolve or mitigate all security weaknesses identified during the Assess and Authorize (A&A) process associated with the design, engineering, integration, configuration, implementation and documentation of the ICIDS-VI solution. This information will be recorded and tracked in an IT Security POA&M. The Contractor shall prepare the POA&M based on the vulnerabilities identified during the security control assessment. Inherited vulnerabilities must be addressed in the POA&Ms. POA&Ms must be active throughout a system's lifecycle as vulnerabilities remain or are remediated. POA&M shall be updated as part of comprehensive vulnerability management as monthly, emergency out of cycle patches are tested, applied within 2 weeks of receiving the guidance, scans are produced and STIG checklists are updated monthly. Any required security controls that are not explicit in the contract or otherwise covered by a Service Level Agreement (SLA-inherited) must be assessed as NC. All such NC security controls must be documented in a POA&M with an explanation as to why accepting the risk of operating the system in a NC status is acceptable.

The Contractor shall continuously maintain, review and assess the status of the system as it relates to the A&A security posture. The Contractor shall adhere to IA controls that relate to configuration and vulnerability management, performance monitoring and implement capabilities to continuously monitor the system and information environment for security relevant events and configuration changes that negatively affect security posture. The system level continuous monitoring strategy must conform to all applicable published DoD enterprise level or Army continuous monitoring strategies. Contractor shall implement, manage and update as necessary Host Based Security System (HBSS) and Army Endpoint Security System (AESS)

to monitor system anomalies, correct them and remediate them. The HBSS agent with the current mandated modules will be installed on all windows machines as part of the delivery order baseline build. HBSS shall include applicable modules (currently DOD requirements but may change) HIPS, DLP, PA, RSD and ACCM add onto HBSS agent with anti-virus). The Contractor shall report significant changes in the security posture of the system, prepare Security Impact Analysis for approvals and recommended mitigations, immediately to the Government. At the direction of the SCA or AO, the Government may schedule a revalidation of any or all IA controls at any time. The system is subject to scheduled or unscheduled inspections from DISA, ARCYBER, and JFHQDODIN.

3.7 Site Survey (SS), Site Survey Design (SSD) and Installation

3.7.1 SS

a. PM FPS will provide the Contractor the following for each Installation

(1) List of zones

(2) List of remote areas currently installed with IDS

(3) List of remote areas that require IDS

(4) Installation drawings (if available)

(5) Contact information for the Government Installation Point Of Contact (POC)

Security Office POC for verifying security clearances of Contractor personnel

b. Government may provide information to the Contractor to develop the proposal for DO award. Upon receipt of the DO/Statement of Work, the Contractor shall submit a proposal with supporting rationale for the price and schedule to accomplish: SS, SSD including Design Review, network design, installation, material disposition, interface with GFP, training, testing, warranty, and timeline for scheduled maintenance at each Installation and travel for DO completion. Upon acceptance of the proposal, the KO will issue a DO and the Contractor shall proceed with schedule coordination for the site survey.

3.7.2 Performance of SS

The SS is the most critical factor for successful completion of ICIDS installation. The SS team shall be qualified in all aspects of the SS process including management, technical and previous IDS SS experience. The Contractor shall perform the SS and deliver a Site Survey Report (SSR), CDRL A015.

The Contractor shall conduct a SS using a Contractor checklist to determine equipment, quantities, network infrastructure and locations necessary for a complete ICIDS-VI installation. The SS shall identify Installation preparation requirements and define hardware/software interfaces with existing IDS or other security equipment. All Government provided Installation

documentation shall be verified with existing conditions. The Contractor shall verify availability and quality of any Government furnished Data Transmission Media (DTM), low voltage transmission lines and electrical grounding systems. All DTM and radio links shall be tested to determine suitability for use. The SS report shall document differing site conditions IAW FAR 52.236-3 Site Investigation and Conditions Affecting the Work and submit to the Government. If the SS identifies more or less zones than the Government provided information, the Contractor shall immediately notify the KO.

If authorized by the KO, the Contractor shall complete the SS of all zones identified and provide a revised proposal. The proposal shall provide supporting rationale for the changes, to include travel/subsistence to accomplish the SS. Upon Government approval of the proposal, the KO will issue a contract modification to adjust the price and scope of the DO.

Each Installation will provide the Contractor with suitable storage and office workspace IAW agreed terms and conditions set forth in the Memorandum of Notification (MON)/Material Fielding Agreement (MFA) between the PM FPS and the gaining Commander. If the Government cannot provide suitable storage and office space as determined prior to arrival of the SS Team, the Contractor shall identify and propose an alternate plan to include possible off site location. If directed by the Installation physical security office, the Contractor shall coordinate with the Installation public works activity manager to obtain approval from the Garrison Commander before facilities on a garrison are made available. This action is IAW AR 420-1 where contractors are required to have agreements with the Installation and the servicing utilities. The Contractor is responsible for daily clean up IAW FAR clause 52.236-12 and shall be in compliance with all safety regulations and codes.

3.7.3 Site Survey Report (SSR)

The Contractor shall deliver an SSR to report findings of the SS. Installation conditions, network readiness, new facilities or other changed requirements shall be documented in detail. Zone drawings, changed equipment layouts, revised block diagrams, preliminary price data for the equipment and installation and other data shall be included. The Contractor shall identify any environmental and network conditions that would hinder and exceed the operational limits of equipment to be installed. Contractor shall list all remediation items in result of SS to resolve them in a timely manner.

3.7.4 Site Preparation Requirements and Installation Plan (SPRIP)

The Contractor shall submit a SPRIP IAW CDRL A016. This document shall denote installation preparation requirements and required completion dates. The plan shall provide the results of DTM tests for use in ICIDS-VI. Should unsuitable DTM be identified, the plan shall make recommendations for using alternative DTM or re-conditioning/replacing existing DTM.

The SPRIP shall identify a schedule for installation, mobilization, facility access, planned utility interruptions, system startup, checkout, projected test schedules and other tasks required to accomplish the ICIDS-VI installation. The Installation will be responsible for site preparation. If the Installation cannot resolve site preparation issues, PM FPS will coordinate with the

Installation for resolution or provide a contract modification for the Contractor to provide required site preparation.

3.7.5 Site Specific Engineering Design (SSD)

The SSD shall provide a complete description of the ICIDS-VI Installation design IAW CDRL A006 Installation Engineering Plan (IEP) and drawing package IAW CDRL A007 Commercial Engineering Design Data and Associated Lists. The SSD shall include a narrative discussion of design philosophy, assumptions, reference sources and calculations for each site. Design documentation package shall include required drawings, design analysis, external, internal network data, requirements and other data required to support the design. Design shall include executive summary, site description, fielding schedule, building and utility system diagrams, Bill of Materials, drawings, Installation maps and system integration diagrams. System design shall include integration of system with Installation's network and existing Installation IDS.

Contractor shall conduct SSD review not later than 15 calendar days after receipt of Government comments on CDRLs A006 Installation Engineering Plan (IEP) and A007 Commercial Engineering Design Data and Associated Lists. The SSD review shall take place at the gaining Installation or via teleconference at the Government discretion. The Contractor shall discuss technical issues requiring Government guidance.

3.7.5.1 Design Review and Final Design Documentation

Upon Government review of design and completion of Design Review, the Contractor shall provide final IEP and SSD for Government approval IAW CDRLs A006 Installation Engineering Plan (IEP) and A007 Commercial Engineering Design Data and Associated Lists.

3.8 Site Installation

The date of installation initiation shall be determined by the Government upon final acceptance of the Contractor’s SSD and completion of any required site preparation. During installation, the existing IDS must remain operational for each zone until that zone is replaced. During transition of operations from existing IDS to ICIDS-VI, the Contractor shall not disrupt system operations for more than 24 hours. No more than 10 percent of the system shall be inoperable at any time. The Contractor shall maintain ICIDS-VI during transition until Government acceptance, at which time the warranty period will commence.

Installation shall be completed within the time set forth in the DO. ICIDS-VI shall be installed IAW the Government approved IEP and SSD. Prior to Government acceptance of the installed system, the Contractor shall revise SSD drawings to reflect actual installed design IAW CDRL A008. The drawings shall reflect all field changes. All interruptions of utility services shall be scheduled with the Government POC. The Contractor shall minimize interruption of services. The Contractor shall include OEM verification at each Installation for proper installation of ICIDS VI major components to include, but not limited to, PCU, door sensors, motion sensors, and enclosures. OEM verification shall be conducted during the PVT-2 phase and for every installation at the following intervals: beginning and at the end of the ICIDS VI installation.

OEM verification shall also be performed at the government's request to verify conformance with the manufacturers' specifications.

3.9 Equipment Delivery and Storage

The Contractor shall prepare and deliver required materials and equipment. The Contractor shall perform loading, unloading, packing, unpacking, inventory and inspection of equipment at each Installation. The Contractor shall ensure proper storage and security of materials and equipment during contract performance. If the Installation cannot provide storage, the Contractor shall include cost price in the final proposal.

3.10 Removal of Installation Debris

The Contractor shall ensure removal and disposal of all debris generated as a result of the installation including removed equipment IAW the DO.

3.11 Software Requirements

3.11.1 System Application Software

The Contractor shall provide system and application software. System software shall support application software programs IAW the SPS. If a software license is required, the Contractor shall provide Installation licenses to include initial, extended support, and reoccurring. If enterprise level licenses are required, the Contractor shall provide initial, extended support, and reoccurring.

3.11.2 Software Defect Corrections

Corrections to software defects shall be made available and installed at no change in contract price or Period of Performance (PoP) extension.

3.11.3 System Software

Upon successful completion of PVT and subsequent System Acceptance Test (SAT), paragraph 3.16.5, Contractor shall provide a copy of software and data installed at the Installation IAW Computer Software Product End Items, Software Installed IAW CDRL A017.

3.12 Documentation Requirements

3.12.1 Product Bulletins

The Contractor shall provide any product bulletins that impact ICIDS to the KO's Representative (COR).

3.13 Supportability

Contractor shall implement reliability and maintainability programs to ensure reliability requirements in the ICIDS-VI SPS are met.

The Contractor shall identify all failures, determine the causes of all failures, correct all failures and deliver to the Government a written report, Failure Summary and Analysis Report - Reliability IAW CDRL A018.

3.13.1 Contractor Logistics Support (CLS)

A one year warranty, beginning upon Government acceptance, including all parts and labor for all supplies delivered under this contract is required. Warranty shall include quarterly maintenance visits. The Contractor shall provide warranty response help desk service 24 hours per day, seven days per week during the Warranty PoP. Call response time will be less than 30 minutes. Maintenance Service (MS) Reports detailing maintenance problem(s) and corrective action(s) shall be delivered IAW CDRL A019.

a. Warranty Repair

The Contractor shall plan for repair actions on items that fail during one year warranty period. Specific tasks to be performed shall be provided in the Contractor Maintenance Support Plan (MSP), CDRL A020. The MSP shall define the process for documenting failed Contractor installed equipment, repair, replacement, modification and test and reporting corrective actions to PM FPS. The Contractor shall provide a timeline identifying when scheduled warranty maintenance will be performed at each Installation.

b. Warranty Repair Time

Contractor scheduled maintenance shall not interrupt system operations. Repair time for unscheduled warranty repair of an operational mission failure shall not exceed the time of eight or 24 hours as specified in the DO. An operational mission failure is defined as a malfunction of the system that results in loss of system performance requiring deployment of a guard force to 1/16th or greater of the protected zones. For other failures, response and repair time shall not exceed 24 hours. Warranty repair time for service calls is measured from the time Contractor is notified to the time Contractor’s work force has completed repair.

3.13.2 Requirements for Unique Item Identification (UID)

The Government does not anticipate any components to have UID requirements. However, if required, Contractor shall mark all contract deliverables IAW the following requirements.

a. UID Marking

Contractor shall apply UID markings to all other components identified by the Government in this contract as requiring UID markings. UID markings shall be IAW MIL-STD-130M.

b. Commercial Markings

All other components shall have acceptable commercial markings that meet guidelines in DoD Guide to Uniquely Identifying Items http://www.acq.osd.mil/dpap/UID/.

c. Permanency and Legibility

The UID marking and identification plates, tags, etching or labels when used on equipment, parts, assemblies, subassemblies, units, sets, groups or kits shall be as permanent as the normal life expectancy of the component and be capable of withstanding the environment, test, cleaning, repair and rebuild procedures specified for the item. Legibility shall be verified for ready readability per MIL-STD-130M.

d. Deleterious Effect

Marking of components shall be accomplished in a manner not adversely affecting the life and utility of the component. Marking materials or their placement shall not create hazardous conditions.

3.13.3 Support Equipment

The Contractor shall identify equipment required to meet Operational Readiness IAW the SPS. A list identifying required support equipment for all systems shall be included in the MSP and TM.

3.13.4 Technical Data

The Contractor shall deliver information to operate, maintain and train on the System. ICIDS has requirements for a Department of the Army (DA) Technical Manual (TM). The Contractor shall use as a guide the Manual requirements in Section J Attachment 0012 Technical Manual for development and production of equipment publications. The TM shall be delivered IAW COTS Manuals and Associated Supplemental Data, CDRL A021. The initial TM meeting shall take place at the ESTL to discuss all TM requirements. In Process Reviews (IPR) shall be conducted when TM is 30% and 70% complete.

3.13.5 Training and Training Support

An Executive Training Course for PM FPS personnel shall provide an overview of all training. This training will be at the ESTL. Installation training shall include hands on classroom training using Contractor provided equipment. Training shall include Operator, System Administrator, SCIF Administrator and Maintenance Technician courses. Training courses shall be tailored to each Installation according to the type and quantity of equipment being installed. Contractor shall not use the installed system for training. Contractor shall comply with training requirements stated below and award a training certificate to each attendee upon successful completion.

3.13.5.1 General

The Contractor shall develop a training package and conduct training IAW paragraph 3.13.6.2. The Contractor shall provide the training plan, execution and test IAW Training Program Development and Management Plan, CDRL A022, Training Conduct Support Document, CDRL A023 and Test Package, Training, CDRL A024.

3.13.5.2 Training Requirements

The Contractor shall provide training as described below:

a. Government Executive Training

The Contractor shall provide an eight hour Executive Training Course as required and IAW CLIN X037. First course shall be presented prior to PVT-1 for up to 20 PM FPS personnel. Additional Executive Training and demonstrations shall be provided IAW CLIN X037 upon request of the Government.

b. Installation Training

Combined Installation Training (Operator, System Administrator and Maintainer) shall not exceed 80 hours for Installation personnel. In addition, SCIF training shall not exceed eight hours. Course breakdown shall be:

- Operator Training for 12 students; maximum of 16 hours
- System Administrator Training for four students; maximum of 24 hours
- Maintenance Technician Training for two students; maximum of 40 hours
- SCIF Training for 12 students; maximum of eight hours

Instruction for Operator, System Administrator, SCIF and Maintenance Technician personnel shall be provided at each Installation. The Contractor shall provide each of these training packages as standalone courses. The Contractor shall structure courses for hands on classroom training. Training shall include all equipment operations and functions including Operator Preventive Maintenance Checks and Services (PMCS). Operators must complete only Operator training. System Administrators must complete Operator training prior to the System Administrator training. Maintenance Technician personnel must receive Operator and System Administrator training prior to learning maintenance tasks.

c. Training, Testing Materials and Equipment

Training and testing materials will be approved by the Government prior to Contractor conducting training. The Contractor shall provide training, testing materials and equipment. Contractor shall provide each student a copy of training materials. Equipment shall provide for classroom instruction of all training. The installed ICIDS-VI shall not be used for training except for the maintenance training. The maintenance training shall include reading the design drawing, location of all communications hubs and use of any system aids for trouble shooting.

d. Conduct of Courses

(1) Scope of Training. Maintenance Technician Training shall be in any areas where maintenance is performed. Following completion of each course, students shall be given a test to assess knowledge gained. System Operators shall be tested on their ability to successfully

accomplish all of the operational actions. System Administrators shall be tested on their ability to accomplish operational actions and PMCS functions. SCIF personnel shall be tested on their ability to perform Operator and System Administrator tasks. System Maintenance Technicians shall be tested on their ability to identify, remove, replace and perform prescribed maintenance of major components specified in the TM.

(2) Length of Course. The Combined Operator, System Administrator and Maintenance Technician courses shall not exceed 80 hours. The SCIF course shall not exceed eight hours.

(3) Dates of Installation Classes. Dates for classes are determined by coordination between Contractor and the Government, based on Installation schedule and availability of equipment.

(4) Safety. The Contractor shall include in the training material detailed procedures to ensure safety of all individuals. Safety procedures shall include relevant notices, warnings, cautions and notes extracted from the TMs and from any other source of information pertinent to the safety of personnel.

(5) Facilities. Classroom and practical exercise facilities will be furnished by the Installation POC who will coordinate availability and adequate facilities.

(6) Training Material. Training materials shall be furnished by the Contractor.

(7) Instructor Qualifications. Instructor(s), selected by the Contractor shall be experienced and have complete knowledge of the end item and its components.

(8) Special Instructions.

(a) The Government reserves the right to record any or all training. Training material becomes the sole property of the Government and no additional copyright or individual release shall be required.

(b) All visual aids, materials and test packages developed or specifically produced for use in the conduct of training courses shall become the property of the Government.

3.13.6 Computer Resources Support

The Contractor shall provide all available hardware and software upgrades IAW with CM requirements.

3.13.7 Facilities

Facilities used by the Contractor during installation, testing and training will be identified during SS by the Installation POC. Facilities where the ICIDS-VI is installed shall be identified in the IEP.

3.13.8 Packaging, Handling, Storage and Transportation (PHS&T)

The Contractor shall identify resources and processes required for the PHS&T to maximize availability and usability of the materiel. The Contractor shall perform PHS&T processes during DO execution.

3.13.9 Design Influence/Interface

The Contractor shall incorporate logistics in the systems engineering process IAW Integrated Logistics Support, AR 700-127, Table 3-1 to maximize the availability, effectiveness and capability of the System.

3.13.10 Integrated Logistics Support Plan (ILSP)

The Contractor shall provide a tailored ILSP. The document will be IAW ILSP, CDRL A042.

3.14 Security

The Contractor shall comply with the security regulations and procedures set forth in the National Industrial Security Program Operating Manual (NISPOM) and DD Form 254, Contract Security Classification Guide. Contractor shall provide personnel with appropriate clearance levels to fulfill requirements in each DO. The contract will be Controlled Unclassified Information (CUI). Contractor personnel shall be required to access, view, possess, process and/or use information designated as CUI. Contractor personnel must possess and maintain a SECRET security clearance and/or be eligible for immediate adjudication by the appropriate cognizant security authority upon award of the contract.

Before performing and upon completion of any on site work, Contractor shall report to Installation Security Officer or designated representative. Contractor personnel shall possess and transmit appropriate clearances prior to arrival at the Installation. The current status of all personnel shall be reported in the SMR by duty position, CDRL A001.

3.15 Quality Assurance Requirements

3.15.1 Responsibility for Inspection

Quality Control is an overall system of activities, including inspection whose purpose is to provide a quality of product or service that meets contract requirements.

Unless otherwise specified in the contract, the Contractor is responsible for the performance of inspection requirements. The Contractor shall provide and maintain an inspection system that shall assure that all supplies and services submitted to the Government for acceptance conform to contract requirements, whether manufactured or procured by the Contractor, or procured from subcontractors or vendors. The Contractor shall perform or have performed the inspections and tests required to substantiate product conformance to drawings, specifications, and contract requirements, and shall also perform all inspections and tests otherwise required by the contract.

The Contractor's inspection system shall be documented and shall be available for review by the Government throughout the life of the contract.

The Contractor's plan describes the Contractor's approach and processes to control quality and ensure that the services, equipment, material and installation processes are completed in the same matter for each installation whether in the ESTL or the installation sites. The Contractor shall develop typical drawings for all install activities that shall be maintained as part of the Contractor's system. The typical drawings shall be one basis for inspection of installation efforts showing placement of wiring and components of the system in containers, racks, and enclosures.

3.16 Test and Evaluation

3.16.1 General

The Contractor shall develop and execute a test process that supports verification of the system. The test program shall include planning, executing and assessing system performance against the requirements. Testing objectives include determination and execution of corrective actions and subsequent demonstrations necessary for the system to meet requirements, performance of tests to support additional capabilities, support of maintenance testing and validation of system level training. The Contractor's testing methodologies shall address how future system changes will be tested and validated. The Contractor shall perform the tests described in the following paragraphs. The Contractor shall provide personnel, equipment and supplies necessary to perform or support testing activities. The Contractor shall notify the Government of all testing and evaluations. The Government will witness all testing and evaluation as required.

Contractor shall attend test meetings, prepare minutes, provide required documentation and assist in the resolution of issues or concerns. Discrepancies in the documentation, design or training shall be corrected prior to the conduct of all test events and may involve re-testing and re-training of personnel at Contractor's expense.

Government may terminate testing at any time when the system fails to perform. Upon termination of testing, the Contractor shall commence an assessment period. The Contractor shall deliver a report that identifies the failure and the cause. The Contractor's report shall include corrective actions. All these actions are reported IAW Failure Summary and Analysis Report, PVT-1, PVT-2 and SPV, CDRL A025.

After delivering a written report, Contractor shall convene a test review meeting at the Installation to present results and recommendations to the Government. Based on Contractor's report and test review meeting, Government will approve the recommended restart date, which may include a component re-test or a complete system re-test. The cost of any re-starts or re-tests shall be borne by the Contractor.

The Contractor shall consider the following in developing/executing the test process:

a. The Government will conduct a Test Readiness Review (TRR) at the Installation prior to any test.

b. The Contractor shall attend meetings and provide the required documentation and assistance in the resolution of any issues or concerns.

c. Discrepancies in the documentation, design or training shall be corrected prior to the conduct of the PVT and the ET by the Contract Site Manager and may involve re-test of zones and re-training of personnel at Contractor's expense.

d. The Contractor shall not be held responsible for failures in system performance resulting from any of the following:

(1) An outage of main power supply in excess of the capability of backup power source, provided the automatic initiation of backup sources and automatic shutdown and restart were accomplished.

(2) Failure of a Government-furnished communications link, provided the failure was not due to Contractor-furnished equipment, installation or software.

(3) Failure of existing Government-owned equipment, provided the failure was not due to Contractor-furnished equipment, installation or software.

(4) Failures due to environmental extremes exceeding the SPS.

The Contractor shall perform test events as described in the following paragraphs.

3.16.2 PVT-1

a. General. The Contractor shall conduct PVT in two parts as described below. PVT-1 shall be conducted IAW Government-approved Test Plan, PVT-1, CDRL A026 and Test Procedure, PVT-1, CDRL A027 to verify functional requirements of ICIDS. PVT-1 shall be conducted at the ESTL within 90 days of contract award. The Contractor shall submit Test/Inspection Report, PVT-1 IAW CDRL A028 after completion of PVT-1.

b. PVT-1. The PVT-1 shall be conducted on a fully integrated system consisting of at least one component of each hardware/software component except exterior sensors. PVT-1 shall be performed on equipment provided by the Contractor for PVT-1 test at the ESTL. The Contractor shall conduct tests to verify system performance complies with contract requirements. Tested equipment models shall be identical to those delivered for installations. Contractor shall prepare drawings to reflect the design of the system tested for PVT-1 at the ESTL IAW CDRL A008. Drawings shall be maintained for life of the contract and shall be updated when changes are made to the ESTL. A TRR shall be conducted at the ESTL prior to conducting PVT-1.

3.16.3 PVT-2

a. General. PVT-2 shall not begin until PVT-1 and Safety Assessment Report, CDRL A029, have been completed and approved by the Government. PVT-2 and an ET shall be conducted on the first site installed. After completion of PVT-2, the Government will operate and manage ICIDS-VI for a 30 day ET IAW paragraph 3.16.6. PVT-2 site design and test shall include all components that comprise a total ICIDS-VI system using Government-approved test plan and procedures. The ICIDS-VI installation effort shall use new components. At least one component of each installed hardware/software item shall be tested. The Contractor shall deliver

PVT-2 and ET Plans, IAW Test Plan, PV-2, CDRL A030, Test Plan, Endurance PVT-2, CDRL A031, Test Procedure, PVT-2, CDRL A032 and Test Procedure, Endurance PVT-2, CDRL A033. After testing, the Contractor shall submit Test/Inspection Report, PVT-2 IAW CDRL A034 and Test/Inspection Report, Endurance PVT-2 IAW CDRL A035.

b. PVT-2. PVT-2 shall verify successful system integration and proper installation of the system IAW SPS. Physical and functional requirements of ICIDS-VI shall be verified and documented IAW test plan.

c. Upon successful completion of testing event PVT-2, the Contractor shall deliver a test report IAW CDRL A034 prior to commencing the ET.

3.16.4 PVT-2 and System Performance Verification (SPV) Tests

During the course of PVT-2 and subsequent System Performance Verification (SPV) tests, all installed equipment is active and reports to the command & control console. The SPV shall test 100% of connected devices. SPV is developed as a result of PVT-2 to support future installations.

3.16.5 System Acceptance Test (SAT)

The SAT consists of SPV and ET. The Contractor shall conduct a SAT for follow on installations after PVT-2. SPV and ET shall be conducted on all installed sites. After completion of SPV, the Government will operate and manage the ICIDS-VI for a 30 day ET IAW paragraph 3.16.6. The Contractor shall deliver SPV and ET Plans, IAW Acceptance Test Plan, SPV, CDRL A036, Acceptance Test Plan, Endurance SPV, CDRL A037, Test Procedure, SPV, CDRLs A038 and Test Procedure, Endurance SPV, CDRL A039. After testing, the Contractor shall submit Test/Inspection Report, SPV IAW CDRL A040 and Test/Inspection Report, Endurance SPV IAW CDRL A041.

3.16.6 Endurance Test (ET)

The ET shall be conducted after Government approval of PVT-2, SPV Tests and completion of training and correction of failures. Contractor shall provide personnel to support testing 24 hours per day, including weekends and holidays, during a 30 day ET. Contractor shall not make repairs during ET unless authorized by the Government. The Government will operate the system during this test. The test shall demonstrate the system operates IAW SPS, training and technical documentation.

4. OTHER REQUIREMENTS

4.1 DoD Common Access Cards (CAC)

Contractor personnel requiring recurring access to DoD Installations may, at the discretion of the Government, be issued DoD CACs. The Contractor shall furnish all requested information required to facilitate the use and possession of the badges. The Contractor's Program Manager shall be responsible for ensuring that all identification badges issued to Contractor employees are

returned immediately following the completion of the Contract, relocation or termination of an employee and/or upon request of the KO or the COR.

4.2 Access to SECRET Data

There is not Secret data on this contract.

4.3 Travel outside Continental United States (OCONUS)

The Contractor shall comply with the requirements for OCONUS travel if required by the DO. The Contractor shall coordinate for OCONUS travel as directed by the DO and discussions with the COR.

4.4 Anti-Terrorism (AT) Level I 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 10 calendar days after contract award 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 KO, if a COR is not assigned, within 30 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: https://atlevel1.dtic.mil/at. This information will be reported via the SMR, CDRL A001.

4.5 Access and General Protection/Security Policy and Procedures

Contractor and all associated subcontractor employees shall comply with applicable Installation, facility and Area Commander Installation/facility access and local security policies and procedures (provided by Government representative). The Contractor 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 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.

4.6 AT Awareness Training for Contractor Personnel Traveling Overseas

All US based Contractor employees and associated subcontractor employees shall be made available to receive Government provided Area of Responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit Anti-Terrorism Officer (ATO) being the local point of contact.

4.7 iWATCH Training

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 90 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR via the SMR.

4.8 Contractor Employees Who Require Access to Government Information Systems (IS)

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 and must successfully complete the DoD Information Assurance Awareness prior to access to the IS and then annually thereafter. This information will be reported via the SMR.

4.9 For Contracts that Require an OPSEC Standing Operating Procedure/Plan

The Contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan will include the Government's critical information, why it needs to be protected, where it is located, who is responsible for it and how to protect it. In addition, the Contractor shall identify an individual who will be an OPSEC Coordinator. The Contractor will ensure this individual becomes OPSEC Level II certified per AR 530-1. This is mission dependent requirement and is considered a contingency item if required.

4.10 For Contracts that Require OPSEC Training

Per AR 530-1, Operations Security, new Contractor employees must complete Level I OPSEC training within 30 calendar days of their reporting for duty. All Contractor employees must complete annual OPSEC awareness training. This is mission dependent requirement and is considered a contingency item if required.

4.11 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 IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of employment.

4.12 For Information Assurance (IA)/Information Technology (IT) Certification

Per DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the Contractor employees supporting IAM/IAT Level functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

4.13 For Contractors Authorized to Accompany the Force and Performance or Delivery in a Foreign Country

If there is a requirement for Contractors to accompany the U.S. Armed Forces or deliver systems to a foreign country, the KO will provide theater business clearance clauses in the DO IAW DFARS Clauses 252.225-7040 and 252.225-7043.

4.14 For Contracts That Require Handling or Access to Classified Information

Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires Contractors to comply with the Security Agreement (DD Form 441), including the NISPOM, DoD 5220.22-M and any revisions to DoD 5220.22-M, notice of which has been furnished to the Contractor.

5. CONTRACT SUPPORT INFORMATION

5.1 Government Furnished Property (GFP)

The Contractor shall accept all GFP and shall be responsible for fielding and maintaining all Government-designated GFP. The Contractor shall closely coordinate their supply and delivery schedules with the Government to ensure all hardware and software is available to meet schedule requirements. Contractor shall maintain ICIDS-ESTL equipment needed to support legacy systems for the life of the contract. The Contractor shall be responsible for providing GFP Inventory IAW Report of Receipts, Inventory, Adjustments and Shipments of Government Property, CDRL A043.

5.2 Government COTS Products

Government sources for proposed COTS products shall be given priority. The Contractor shall coordinate procurement of items they have identified as available from Government sources. The Army's preferred source is the Computer Hardware Enterprise Software and Solutions (CHESS) and shall be given priority over non-DoD sources. A letter will be provided at time of award authorizing the winning offeror the ability to order from the CHESS website. Procurement of equipment on behalf of the Government shall be in compliance with all applicable regulations and policies.

For items that are required to be Federal Information Processing Standards (FIPS) 201 compliant, the Contractor shall provide products that are on the General Services Administration's FIPS 201 Evaluation Program Approved Products List. All FIPS 201 compliant items shall be identified by product number, category, name and part number.

5.3 Health and Safety

The Contractor shall update and maintain the programmatic environmental compliance, health and safety program compliance and 29 Code of Federal Regulations (CFR) 1926 Occupational Safety and Health Administration (OSHA) compliance. The Contractor shall develop and provide a Safety Assessment Report IAW CDRL A029.

6. SYSTEM ENHANCEMENTS

Since ICIDS has been demonstrated through or is active at various Military Installations, the Government may support inter Service development or detailed component design activities under the ICIDS-VI Contract. The Government may initiate system enhancement research and development within the scope of this contract.

7. TRAVEL

Contractor personnel shall be required to travel to ICIDS-VI installation sites, participate with Government personnel at meetings, conferences and other activities. Costs for transportation required to perform the work may be based upon mileage rates, actual costs incurred or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel. The Joint Travel Regulations (JTR), while not wholly applicable to Contractors, shall provide the basis for the determination as to what is reasonable and allowable. Travel costs are reimbursable for direct costs only. The Government will not pay General and Administrative, profit or fees on travel costs. Exceptions to these guidelines will be approved in advance by the KO.

8. OTHER DIRECT COSTS

Over the PoP of the Contract, the Contractor may need to procure items or make other expenditures not covered under the work and deliverables specified in other paragraphs. The Contractor shall specifically identify the requirement prior to making the expenditure and obtain approval from the KO for one-time or recurring purchases greater than $10K.