

**Statement of Work**

for

N00039-14-R-0221

**Global—Theater Security Cooperation Management Information System (G-  
TSCMIS) Release 3 (R3) Software Development**

Version 1.0

30 October 2014

**DISTRIBUTION STATEMENT C.** Distribution authorized to U.S. Government agencies and their contractors (Administrative or Operational Use)(3 NOVEMBER 2014); other requests must be referred to the Command and Control Program Office (PMW 150), Navy Program Executive Office C4I.

# Statement of Work (SOW) for Global—Theater Security Cooperation Management Information System (G-TSCMIS) Release 3 (R3) Software Development

---

## **1.0 Scope**

This section provides an introduction of the Global – Theater Security Cooperation Management Information System (G-TSCMIS), background on the G-TSCMIS program, and outlines the scope of the contract.

### **1.1 Introduction**

G-TSCMIS is a joint command and control (JC2) architecture-compliant, web-based, enterprise-hosted solution that standardizes theater security cooperation (TSC) data and provides consistent planning and assessment capabilities across all Combatant Commands (COCOMs), Services, and Agency users. G-TSCMIS provides for data aggregation and assessment to help decision-makers and analysts evaluate the outcome of activities (events or tasks), planning more effective security cooperation (SC) events and engagements, and finding gaps and opportunities for developing capable Nation partners. It is also the partnership-building investment analysis tool for identifying redundant investments and supporting monitoring, assessment, and allocation of SC funding. It provides users the ability to create customized information dashboards and provide a comprehensive set of reporting capabilities. Users access G-TSCMIS through their existing web browsers on Secret Internet Protocol Router (SIPR)/Unclassified, but Sensitive Internet Protocol Router (NIPR) workstations. G-TSCMIS provides capabilities that meet the spectrum of different needs of users from the Office of the Secretary of the Defense and the Joint Chiefs of Staff to COCOM country desk officers.

### **1.2 Background**

G-TSCMIS provides first the Department of Defense (DoD) and eventually the entire U.S. Government with the ability to organize and use SC data more effectively. Department of Defense Directive (DoDD) 5132.03 defines SC as:

*Activities undertaken by the Department of Defense to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DoD*

*interactions with foreign defense and security establishments, including all DoD-administered security assistance programs, that: build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities; develop allied and friendly military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations.*

The Secretary of Defense identifies security cooperation objectives, assesses the effectiveness of SC activities, and revises goals when required to ensure continued support for U.S. interests abroad. These overarching goals derive from the directives and guidance in the National Military Strategy, Guidance for the Employment of the Force (GEF), COCOM direction, intermediate military objectives, and service and agency policy. Although they can shift over time, examples of typical SC objectives, include creating favorable military regional balances of power, advancing mutual defense or security arrangements, building allied and friendly military capabilities for self-defense and multinational operations, and preventing conflict and crisis.

As the GEF moved security cooperation guidance from a smaller community to mainstream planning and execution, the importance of security cooperation rose. The 2008 DoDD 5132.03, "DoD Policy and Responsibilities Relating to Security Cooperation," directs that security cooperation activities shall be planned, programmed, budgeted, and executed with the same high degree of attention and efficiency as other integral DoD activities. Security cooperation requires careful analysis to determine which programs and activities encourage and enable international partners to work with the United States to achieve strategic objectives.

### **1.3 Scope**

The scope of the effort described in this statement of work includes:

- Engineering
  - software development,
  - design,
  - integration,
  - technical and engineering support,
  - configuration management (CM),
  - testing,
  - data management,
- Program Management and contract administration, and
- Logistics.

Pursuant to FAR Subpart 7.5, the contractor shall not perform inherently governmental functions.

## 2.0 Applicable Documents

The documents in Table 1 form a part of this SOW to the extent specified herein and are current at the time of award. As these are updated, the government will notify the contractor. In the event of a conflict between the directive documents listed here and the contents of this SOW, the contents of this SOW are the superseding requirement. The contractor shall adhere to the following documents in the performance of work specified in this SOW.

**Table 1: Applicable Documents**

Document Type	No. / Version / Revision	Title	Date
Instruction	8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT)	Mar 2014
Joint Standard	Version 3.0	Joint C2 Reference Architecture	April 2014
Developer Guide	Version 2.0.0	C4 Widget Cookbook	Feb 2013
Developer Guide	N/A	Ozone Widget Framework Developer Guide	URL, maintained current
Software Tool	Version 2.0.1.0	Joint C2 CUI Single Sign-On Toolkit	May 2012
Standard	1.2	Common Map Widget API	Feb 2014
Instruction	Version 2.1	PMW 150 Configuration Management Plan	Jan 2014
Instruction	8500.01	Cybersecurity	Mar 2014
Policy	No. 11	Committee on National Security Systems (CNSS)	Jun 2013
Directive	N/A	IA Vulnerability Management (IAVM) Program ( <a href="http://www.prim.osd.mil/cap/iavm_req.html?p=1.1.1.3">http://www.prim.osd.mil/cap/iavm_req.html?p=1.1.1.3</a> )	N/A
Guidance	N/A	Security Technical Implementation Guides (STIGs) ( <a href="http://iase.disa.mil/stigs/index.html">http://iase.disa.mil/stigs/index.html</a> )	N/A
Guidance	DJSM 0452-11	G-TSCMIS CONOPS	Jul 2011
Template	N/A	Software Quality Assurance Plan (SQAP) Template	Sep 2011
Template	N/A	Design Review Briefing Template	Aug 2011
Instruction	4160.3B	SPAWAR Instruction for Technical Manual Management Operations	Aug 2007
Instruction	130004	G-TSCMIS Technical Manual Contract Requirements (TMCR)	Feb 2013
Guidance	1.1	G-TSCMIS ABAC Design Document	Apr 2014
Directive	N/A	G-TSCMIS Capability Package (CP) 3 including MOE/MOP	May 2014
Guidance	N/A	G-TSCMIS Systems Engineering Plan (SEP)	Draft
Guidance	2.0	Software Quality Assurance Metrics Specification	Feb 2014

Guidance	1.0	DISA Cross-Domain Solutions (IA32) Cross Domain Solutions (CDS) Cross Domain Gateway (CDG) 1.0 Concept of Operations (CONOPS)	Sep 2012
Guidance	1.0.1	Security Guidance for the use of XML Schema 1.0/1.1 and RELAX NG	May 2011
Guidance	N/A	Using Schematron for Cross Domain Security Policy Enforcement	June2012

### 3.0 Requirements

The contractor shall implement proven engineering and management methods, processes, and approaches to provide G-TSCMIS with deliveries that meet all the release requirements described in this SOW and performance criteria in the G-TSCMIS SRS/RTM.

This section contains the following subsections that describe sets of requirements:

- Engineering
- Program Management
- Logistics

#### 3.1 Engineering (CLIN 0001, CLIN 0004, RDT&E)

The contractor shall deliver a software-only product as specified in the G-TSCMIS SRS/RTM (Attachment 3) and CDRL A006, Computer Software Product.

The G-TSCMIS solution shall be interoperable with existing government-used software systems as specified in the G-TSCMIS SRS/RTM. The G-TSCMIS solution shall incorporate, as part of the deliverable, all data and requirements completed from prior G-TSCMIS releases, to sustain current operations, preserve historical data, and promote a quick and seamless transition to the software deliverable. This does not necessitate reuse of existing code.

The contractor is encouraged to use an Agile software development methodology for the design, development, test, and delivery of G-TSCMIS. The contractor is also encouraged to re-use existing software but may develop all R1 – R3 functionality if they can do so within the contract's required delivery date. Regardless of the development methodology, the contractor shall provide multiple, incremental software deliveries; three iterations in total. Each incremental delivery shall provide new capabilities as described in the G-TSCMIS SRS/RTM.

##### 3.1.1 Software Development Process and Approach

The contractor shall define a software development approach appropriate for the computer software effort to be performed under this solicitation. This approach shall be documented in a Software

Development Plan (SDP) (CDRL A001). The contractor shall follow this SDP for all computer software to be developed or maintained under this effort.

The SDP shall define the contractor's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is as defined in IEEE/EIA Std. 12207.0. The SDP shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work content of this solicitation. In accordance with the framework defined in IEEE/EIA Std. 12207.0, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. Because IEEE/EIA Std. 12207 does not prescribe how to accomplish the task, the contractor must provide this detailed information so the Government can assess whether the contractor's approach is viable.

The SDP shall contain the information defined by IEEE/EIA Std. 12207.1, section 5.2.1 (generic content) and the Plans or Procedures in Table 1 of IEEE/EIA Std. 12207.1. In all cases, the level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must include, at a minimum, specific standard, methods, tools, actions, strategies, and responsibilities associated with development and qualification. The government will review SDPs at PDR and CDR events and process for government acceptance.

The contractor shall precede development of each iteration with a critical design review (CDR) event (CDRL A007).

The contractor shall work with the Government to develop business processes and algorithms. The contractor and the PMW 150 engineering staff shall maintain a close, open, and transparent working relationship to ensure that all developmental requirements are understood and being appropriately addressed. Further, both sides will leverage this relationship to shorten the time required to identify and provide any emergent GFI requirements to the development team.

### ***3.1.1.1 Systems Engineering***

The contractor shall use a development approach that enables effective design, development, integration, and testing activities to meet contract requirements by leveraging timely contractor and government systems engineer interaction, review, and feedback. Human Systems Integration (HSI) shall be an integral part of the Systems Engineering Process to determine human performance, design factors, and trade-offs at all levels of the development and testing efforts. The contractor shall ensure the development approach complies with the precepts defined in the SDP (CDRL A001), this SOW, and the engineering principles outlined within the Systems Engineering Management Plan (SEMP, CDRL A002), which will define the G-TSCMIS systems engineering strategy. The contractor shall invite the government to any development planning, status, and review meetings, as an advisory member of the development team.

### **3.1.1.1.1 Requirements Management**

The contractor shall analyze each functional and architectural requirement in the RTM to resolve conflicts within the RTM and with other requirements and ensure the requirement is complete, consistent, and documented accurately in the SRS. If an agile approach is used, the contractor shall transform the requirements into user stories and use them to drive software development. The contractor shall also use an application life cycle management tool to organize and report metrics to the government that would indicate progress in the development of the software as specified in the Agile Software Metrics Report (ASMR, CDRL A018). The contractor shall assess each requirement in the G-TSCMIS SRS/RTM for risk and G-TSCMIS program constraints and objectives, assign a verification and validation method to the requirement, allocate each requirement to one or several components of the system or subsystem, and document the preceding activities in a file that can be used for input to PMW 150's requirements management tool, IBM Rational Dynamic Object Oriented Requirements System (DOORS®).

The G-TSCMIS SRS/RTM provides the set of functional requirements at the Release level. As part of the contractor's software development process, the contractor shall propose which requirements will be fulfilled in each software iteration. The contractor shall include this proposal in the contractor's first Software Development Plan (SDP) version submitted for government approval after contract award. The RTM, though the primary source for G-TSCMIS requirements, is not representative of a full accounting of all requirements for the contracted development. The contractor shall comply with all requirements defined in the contract regardless of origin.

### **3.1.1.1.2 Phased Implementation of Requirements**

The contractor shall deliver software documentation including a Software Version Description (SVD), Software Design Description (SDD), and the Interface Design Description (IDD) with each fielded capability delivery in accordance with CDRL items A008, A009, and A010. The software architecture must be modular and comply with Modular Open Systems Approach (MOSA) principles. The software for Release 3 must meet all previous Release requirements in the first fielded capability release. The requirements for all G-TSCMIS Releases are in the SRS/RTM. This effort covers development of the Release 3 requirements and maintenance of Release 1 and 2 requirements.

## ***3.1.1.2 Configuration and Change Management***

### **3.1.1.2.1 Configuration Management Process**

The contractor shall implement a CM process that complies with the PMW-150 Configuration Management Plan (v2.1), and PEO C4I Naming and Numbering Standard (v1.0), using tools that support the traceability and flow-down of high-level requirements through system hierarchies into detailed requirements. The contractor's process shall optimize the use and reuse of the contractor's CM standards and best practices and MIL-HDBK 61A. The contractor shall ensure that comprehensive CM plans, policies, procedures, and processes are in place for the G-TSCMIS program. The contractor's CM

documentation shall describe the process, methods, and activities that the contractor will develop, implement, and fully adhere to throughout the contract for all software and documentation. The contractor also shall establish document management (DM) standards for identification, version control, change management, approval, archival, and submission of deliverables and documentation.

The contractor shall document CM practices in an approved CMP (CDRL A019), consistent with the functions and principles as listed in Section 5 of the ANSI/EIA-649B standard. It must compliment and interface with the PMW 150 CMP. The government Configuration Manager (CMGR) will review the contractor's CMP to ensure the CMP captures the intent of Section 5 of the ANSI/EIA-649B and the contents will complement the PMW 150 CMP for compliance. The contractor's CM personnel and the government's CM personnel shall coordinate and interface on all CM business related to G-TSCMIS. Attendance by the contractor's CM personnel and the government's CMGR at specified meetings and Configuration Control Boards (CCB) are required. The government CMGR will ensure the contractor's CM performance and deliverables meet all government CM requirements and thresholds as defined in the PMW 150 CMP.

The contractor shall submit a monthly Configuration Status Accounting Report (CSAR) (CDRL A021). The Contractor shall establish and maintain a Configuration Status Accounting (CSA) database, which represents the configuration of the G-TSCMIS. The contractor shall document all baselines and changes in the CSA database. The contractor shall permit acceptance of commercial product information in the CSA database; however, if requirements to report data outside of the CSA database or format exist, the contractor shall deliver the information as a supplement to prevent disruption to their existing system. The contractor shall reconcile any differences between supplier information and contractor practices in the CSA database to provide the government with clear accountability of product information.

If the government accepts any feedback for implementation that constitutes a change in scope, an Engineering Change Proposal (ECP) (CDRL A028) must be submitted to the COR. The ECP process is defined in the PMW 150 CMP.

#### **3.1.1.2.2 Change Recommendation**

The contractor shall propose recommendations for changes to data sources and system interfaces to facilitate the development during the IPT and design review processes. Changes to existing baselines shall conform to the governing CM processes provided on this contract.

#### **3.1.1.3 Development Approach**

##### **3.1.1.3.1 Software Tailorability and Extension**

The contractor shall use a design process that maximizes user tailorability and extension of capabilities without changing the cybersecurity profile and minimizing the need to modify adjoining software modules by:

1. Externalizing the users' individual cybersecurity profiles from G-TSCMIS source code. The solution shall decouple the code and cybersecurity profiles to support extension of capabilities without changing the cybersecurity profiles. The decoupling shall increase the user tailorability by enabling operators to add or remove a user without any impact on the code.
2. Leveraging Ozone Widget Framework (OWF), where appropriate. The government encourages usage of the OWF in developing specific capabilities. Properly leveraged, OWF solutions allow users to customize and tailor authorized UIs and services for use without changing the cybersecurity profile or redeveloping G-TSCMIS software. When implementing these tailorability and extension capabilities, the contractor shall use the Joint C2 CUI Widget Developer Guide listed in Table 1 as appropriate.
3. Designing a normalized interface and data model that minimizes the use of hard-coded values in the source code, particularly with respect to UI controls.

#### **3.1.1.3.2 Human Systems Integration (HSI) Activities**

The contractor shall develop and execute a HSI engineering effort that ensures the effective incorporation of Human Factors Engineering (HFE) principles, requirements, and activities into the layout, design, development, testing, and fielding of the system for all user roles by using MIL-STD-46855A. The contractor shall conduct user assessments during scheduled CSITs to determine system suitability and usability. The contractor shall provide a Human Engineering Program Plan (HEPP, CDRL A023) to the government on HSI efforts including but not limited to the process to obtain and manage user feedback, documents related to the collection of user feedback and actions taken in accordance with the obtained feedback.

#### **3.1.1.3.3 Common Data Model**

The contractor shall collaborate with the government to obtain stakeholder data from external systems. From the data, the contractor shall produce JC2-compliant common data models, including metadata, and document it in the IDD. The government will publish it to appropriate JC2 GIG data registries (e.g. Metadata Registry, Enterprise Catalog) to facilitate data exchange between G-TSCMIS and other systems.

#### **3.1.1.3.4 Use of New, Reused, and COTS Software**

The contractor shall maximize the use of COTS/GOTS software and Defense Information Systems Agency's (DISA) enterprise services for the G-TSCMIS. The contractor shall ensure the COTS Enterprise Software Agreements are valid for no less than the life of the contract. During the development process, the contractor shall document—in the Software Product Specification (SPS, CDRL A011), Software Requirements Specification (SRS, CDRL A012), and Software Design Description (SDD, CDRL A009)—all software reuse, including size in Source Lines of Code (SLOC), and all COTS software use with an explanation of the portability across infrastructure products.

For open source software or unsupported software, the contractor shall provide software support for the life of the contract. The contractor shall use commercial software support or implement the following:

- Verification of compliance with the Open Source User License Agreement in accordance with cybersecurity regulations prior to implementing the OSS software
- Compliance with all DoD and Navy directives regarding waivers and approval to include OSS waiver(s) drafts provided to the Government cybersecurity representative for approval
- Maintenance of code including CM
- Ensuring that cybersecurity support of the software is documented within the C&A Plan as well as how it is supported by the developer.

#### **3.1.1.3.5 Consolidated Enterprise-Hosted Joint C2 Compliant Solution**

Using the Joint C2 Standards Profile listed in Table 1, the contractor shall provide a consolidated enterprise-hosted joint C2-compliant G-TSCMIS materiel solution.

### **3.1.2 Technical Reviews**

The contractor shall conduct a Preliminary Design Review (PDR) for the enter R3 effort, and a Critical Design Review (CDR) for each iteration. In addition to the remainder of this section, required documentation for each review is in the CDRL item A007. The contractor shall conduct the PDR and CDR in accordance with the SEP and this SOW.

At each technical review, the contractor, in addition to providing process, methodology, and recommendation detail, shall provide the analyses and methodologies used to arrive at specific recommendations and conclusions for a design approach. The contractor shall make available all captured technical review data following event completion to include engineering data, specifications, design and test documentation. This data shall include design documentation, screen mock-ups, object-oriented design analyses, schedules, working papers, and results of studies and analyses available for reference in the contractor collaboration tool to support the proposed way forward in each review. The contractor shall deliver relevant G-TSCMIS product information in the contractor collaboration tool via the Data Accession List (DAL) deliverable (CDRL A017). The contractor shall present an updated risk matrix (RM) and the current software testing strategy during all design reviews and IPRs and delivered in accordance with CDRL A007.

#### **3.1.2.1 Preliminary Design Review (PDR)**

The contractor shall conduct a PDR for the entire Release 3 effort no later than 45 working days after contract award. The PDR will be hosted at the contractor's facility and also conducted via Defense Connect Online (DCO) to facilitate remote participants. The contractor shall prepare the PDR briefing package in accordance with the Design Review Briefing Template listed in Table 1. The contractor shall deliver the agenda and briefing materials in accordance with CDRL A007. The contractor shall deliver

meeting minutes and action items in accordance with CDRL A029. The PDR will not be considered complete until all actions are adjudicated by the Government and contractor.

### **3.1.2.2 Critical Design Reviews (CDRs)**

The contractor shall conduct a CDR for each iteration. The initial (Iteration 1) CDR shall be held within 90 working days after contract award. CDRs will be hosted at the contractor's facility and also conducted via Defense Connect Online (DCO) to facilitate remote participants. The contractor shall conduct CDRs to demonstrate that the final software design satisfies the functional and architectural requirements in the G-TSCMIS SRS/RTM. The contractor shall prepare the CDR briefing package in accordance with the Design Review Briefing Template listed in Table 1. The contractor shall deliver the agenda and briefing materials in accordance with CDRL A007. The contractor shall deliver meeting minutes and action items in accordance with CDRL A029. A draft system and subsystem SDD (CDRL A009) and IDD (CDRL A010) shall be presented by the contractor during CDRs. The CDR will not be considered complete until all actions are adjudicated by the Government and contractor.

### **3.1.3 Testing and User Feedback**

#### **3.1.3.1 Software Acceptance Tests (SATs)**

The contractor shall perform unit testing and record test results in a series of test reports. The contractor shall make test reports and test results available in the DAL (CDRL A017).

The contractor shall complete the SAT for each iteration before delivery to the government. The contractor shall fully verify the system baseline software requirements and ensure that each Computer Software Configuration Item (CSCI) is tested against all G-TSCMIS software requirements, including all applicable items in the Software Test Plan (STP) (CDRL A004). The contractor shall capture issues arising from contractor testing and assign a Software Trouble Report (STR) Priority (i.e., Priority 1, 2, 3, 4, or 5) to each issue in the Government's issue tracking system. Priority definitions are in Section E of the contract. The contractor shall submit in their STR the priority assigned for review and solicit approval by the government. The contractor shall accomplish the testing in accordance with the applicable STR and record testing results in a formal Software Test Report (STR, CDRL A005). The contractor shall provide support to the Government during installation and/or test of G-TSCMIS software following delivery of each iteration milestone.

#### **3.1.3.2 Contractor System Integration Tests (CSIT)**

The contractor shall conduct CSITs following development of each iteration but prior to SATs. The contractor shall conduct both structured (test) and unstructured (user free play) events. The contractor shall conduct each CSIT at a Government facility (e.g., NEDC) and shall include user involvement and feedback in-person or via collaboration tools and use external system data sources and services. The government will coordinate each CSIT Community of Interest (COI) activity with the contractor.

The contractor shall accompany each CSIT event with a Software Test Description (STD, CDRL A003) and a Software Test Plan (STP, CDRL A004). The STP will provide a CSIT schedule to include preparation, conduct, and feedback processes for the CSIT. The contractor shall produce and deliver a Software Test Report (STR, CDRL A005) at the conclusion of each CSIT.

The contractor shall present training sessions, using PowerPoint presentations and trainee guides, in preparation for each CSIT (CDRL A024). The contractor shall update training materials with each release to reflect additional capabilities of that release and shall organize them to minimize training time for users familiar with previous iterations of the system.

#### **3.1.3.2.1 User Feedback**

The contractor shall provide user comment sessions for all developed user interfaces (UI). The contractor should time these sessions to precede any development on the subject UI and contain mock-ups of the targeted UI end-state. Each fielded capability shall also include a CSIT event that uses end users as testers, cybersecurity certification tests, and a government acceptance test (GAT). Prior to each CSIT, the contractor shall coordinate with the COR to conduct CSIT planning. Each of these events may result in feedback from PMW 150 and/or the end user community. The contractor shall gather, log, adjudicate, and record all feedback from receipt through adjudication or implementation.

The contractor will receive primary feedback during CSIT events and UI mock-up reviews. The contractor shall log all feedback, with adjudication comments, and track for inclusion in the product backlog, as appropriate. The contractor shall provide the government with access to view and download user stories and product backlog.

#### **3.1.4 Cybersecurity Risk Management Framework (RMF)**

The contractor shall produce software-release deliverables that meet applicable RMF requirements as defined in the SDP, SEP, G-TSCMIS SRS/RTM, Department of Defense Instructions (DoDI) 8500.01 and 8510.01, Security Technical Implementation Guides (STIGs), and National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11. The contractor shall engineer and develop secure system releases that meet all applicable Cybersecurity and system security requirements. The contractor shall build in and test for security requirement compliance during system development to ensure the release and iterations can obtain accreditations.

##### ***3.1.4.1 RMF Implementation***

The contractor shall work closely with government Cybersecurity representatives to progress G-TSCMIS through RMF implementation. This includes developing a plan to determine Cybersecurity and system security requirements, implementing those requirements into G-TSCMIS, verifying and validating that the solution satisfied those requirements, and document the implementation status using the RMF.

The contractor shall develop and deliver a security plan (CDRL A013) that contains the following:

- The security controls in accordance with the STIGs, and Information Assurance Vulnerability Management (IAVM) requirements
- An annotation of software differences between the classified and unclassified systems
- The implementation plan to guide the implementation of the system's security controls
- The validation plan to guide the verification and validation of security controls
- Artifacts that document security control implementation.

The contractor shall submit a combined Plan of Action and Milestones (POA&M) for the classified and unclassified systems using the results of the security control analysis in accordance with CDRL A013. The contractor shall conduct security testing concurrent with each iteration and software release delivery. The contractor shall conduct security testing frequently during development to determine effective implementation of security controls. The contractor shall conduct final release security testing on the final version of the release to verify and validate release compliance with Cybersecurity regulations and requirements. The contractor shall document these results and include them in the STR (CDRL A005). The contractor shall compile all security testing results and document them in Automated IA Test Tool Reports (AIATTR, CDRL A014) and the STR.

#### **3.1.4.2 System Authorization**

The contractor shall support the government's system authorization process per the DoDI 8510.01 and Department of the Navy (DON) policies. The contractor shall support the government in creating authorization artifacts as required.

The contractor shall support the government's authorization efforts with the goal of achieving and maintaining an Authority to Operate (ATO) in accordance with DoDI 8510.01 shortly after delivery and acceptance of final contract deliverables. For new development and for modification of re-used capability, the contractor shall correct CAT I and CAT II findings or institute an Operational Designated Approval Authority (ODAA)-approved mitigation if a fix does not exist so that the finding can/will be reported as a CAT III. This will exclude third party software. Mitigations may include operational policies and procedures.

#### **3.1.4.3 Information Assurance Vulnerability Management (IAVM)**

The contractor shall establish and execute a program to implement security updates to the system releases. The contractor shall develop and implement an IAVM Program to ensure each software release remains current with security updates including Information Assurance Vulnerability Alert (IAVA) and Information Assurance Vulnerability Bulletin (IAVB).

### **3.1.5 Engineering Services (CLIN 0002, CLIN 0004, CLIN 1001, CLIN 1003, RDT&E)**

The contractor shall provide engineering services including software changes to Revisions 2 and 3 to ensure compliance with the requirements specified in Attachment 3, SRS-RTM. Changes may be required pre-acceptance or post-acceptance to support requirements identified during the fielding

process. These changes may include patches and fixes to address cybersecurity-driven changes. The contractor shall receive, review, and provide actionable response and in-depth analysis for support requests directed to the contractor. If it is determined that a problem can be solved, contractor shall develop responses for associated course(s) of action, evaluating each report in a test case environment, and implementing the best solution to the problem. Once the solution is verified, it is delivered to the customer and made available for future troubleshooting and analysis. If it is determined that a problem cannot be solved, the contractor will notify the COR and create courses of action for government consideration. Specific requirements will be clarified in the form of Technical Instructions issued against funding provided under CLINs 0002 and 1001.

## **3.2 Integrated Program Management and Reporting (CLIN 0001, CLIN 0004, RDT&E)**

### **3.2.1 Program Management**

The contractor shall perform administrative, technical, schedule, financial, and other program management efforts during the performance of the G–TSCMIS R3 Software Development contract to ensure all work is planned and executed in an integrated manner to achieve cost, schedule, and technical performance objectives.

### **3.2.2 Integrated Program Management**

The contractor shall use its existing internal management processes, procedures, tools, resources, and systems in a manner that is both cost effective and sufficient for integrating and reporting cost, schedule and technical performance of the G–TSCMIS R3 Software Development contract work scope.

### **3.2.3 Integrated Program Management System**

#### ***3.2.3.1 Electronic Transmission of Data***

The contractor shall utilize the existing Government Integrated Digital Environment (IDE) for soft copy distribution of data items, as specified in the Contract Data Requirements List (CDRL) (DD Form 1423), via upload to the Government CMPRO tool. If there is a conflict with use of this IDE, an alternate Government-owned collaboration site shall be identified.

#### ***3.2.3.2 Integrated Master Schedule (IMS)***

The contractor shall develop and deliver a logically networked Integrated Master Schedule (IMS) using the DoD IMP and IMS Preparation and Use Guide and Section L instructions as guidance. The Contractor shall submit an initial IMS as part of its technical proposal response.

The IMS shall serve as the baseline that reflects the contractor’s best plan to complete G-TSCMIS Release 3 SOW scope and as the benchmark against which the contractor’s progress and contract performance will be measured. The IMS shall contain the planned events and milestones, all activities from contract award to contract completion, activity entrance and exit criteria, and risks/risk mitigation

activities. IMS updates shall be maintained and reported in conjunction with CDRL A026, Contractor's Progress, Status and Management Report (CPSMR).

### **3.2.3.3 *Software Metrics Report***

The contractor shall use software development tools to plan and provide status and progress information on software development activities. If an Agile methodology is used, the contractor shall report monthly cost, schedule, and performance information in accordance with instructions provided in CDRL A018, Agile Software Metrics Report. If an Agile methodology is not used, the contractor shall report cost, schedule, and performance information in accordance with instructions provided in CDRL A026.

### **3.2.3.4 *Contract Funds Status Report (CFSR)***

The contractor shall submit a monthly Contract Funds Monthly Status Report CFSR in accordance with instructions provided in CDRL A027. The CFSR will be used by the contractor and the Government to update and forecast contract funds requirements; to plan and communicate funding changes; to develop funding requirements for approved efforts; to determine funds in excess of contract needs and available for de-obligation; and to obtain rough estimates of termination liability and open commitment costs. The CFSR reporting level will provide funding requirements and time phased detail at the CLIN, ACRN, and total contract levels

### **3.2.3.5 *Contractor's Progress, Status, and Management Report (CPSMR)***

The Contractor shall report the status of their effort towards achieving the G-TSCMIS R3 Software Development contract objectives, including technical activities and efforts, cost and schedule progress, problems and deficiencies, impacts, and recommended solutions, in accordance with instructions provided in CDRL A026.

## **3.2.4 Program Reviews**

### **3.2.4.1 *Post Award Conference***

The contractor shall hold a post award conference (PAC) at the Government's facility in accordance with FAR Subpart 42.5, Post-Award Orientation, with the COR, PCO, and government program management team no later than 15 calendar days after contract award to achieve a clear and mutual understanding of all contract requirements and identify and resolve potential problems. The government, with the contractor, shall establish the specific date.

The contractor shall deliver the PAC briefing package five working days before the PAC in accordance with CDRL A007. The contractor shall deliver meeting minutes and actions from the PAC in accordance with CDRL A029. The contractor shall discuss the following topics at the conference:

1. Identify and introduce the contractor management, engineering, and other personnel to the government representatives. Each individual shall define his or her area of responsibility and accountability
2. Explain the contractor's organization, plans, procedures, and schedules to execute this SOW
3. Present the contractor's business and technical management procedures (e.g., technical POC assignments, status reporting procedures, and designated lines of authority) that shall be implemented to accomplish the requirements of the contract
4. Present the contractor's current staffing plan
5. Allocate time for the government to present its organization, plans, procedures, schedules, and concerns
6. Discuss topics described in FAR Subpart 42.5
7. Allocate time for an open forum to discuss contract-related issues.

#### **3.2.4.2 Program Management Reviews**

The contractor shall prepare and conduct the first Program Management Reviews (PMR) within 90 calendar days of contract award and quarterly thereafter. The contractor shall include the following information or items, as appropriate in each PMR:

1. An updated IMS
2. An updated CWBS, if required
3. Cost and performance metrics
4. An updated Risk Matrix
5. Status of code development and documentation progress, including bug resolution, and code growth or deltas from plan / previous baseline.
6. Certification and accreditation (C&A) status
7. T&E status
8. Present quality metrics, as outlined by the Software Quality Assurance Plan SQAP (CDRL A015).
9. Other issues that may negatively affect technical performance, schedule, or cost.

The contractor shall submit all briefing materials (A007) five business days before the review, and shall submit meeting minutes and action items (A029) within five business days after the PMR meeting date.

#### **3.2.4.3 In-Process Reviews (IPRs)**

The contractor shall prepare and conduct IPRs biweekly or as deemed necessary by either the contractor or the government. The contractor shall include, at a minimum, the following in each IPR:

1. Technical progress since the last review
2. Status of overall capability development
3. Technical and development risks and issues

4. Any issues identified by the government or the contractor
5. Any expected deviations in terms of cost, schedule, and/or performance.

The contractor shall document any decisions and actions resulting from IPRs in its Progress, Status and Management Report (CDRL A026).

### **3.2.5 Quality Assurance Approach**

The contractor shall define and implement a Quality Assurance (QA) approach for work performed that implements industry best practices and the contractor's CMMI standards and procedures for ensuring quality of software and documentation. The contractor shall document its QA approach in the SQAP, CDRL A015. The SQAP shall address those areas that affect project quality and customer satisfaction and is designed to ensure that quality is built into the G-TSCMIS capabilities.

The contractor shall identify practices, conventions, statistical techniques to meet quality requirements. In accordance with the Software Quality Assurance Metrics Specification listed in Table 1, the contractor shall identify metrics to apply to G-TSCMIS products and Software QA metrics in the contractor's SQAP.

The contractor shall generate problem and change reports for baselined and developmental products as required. The Quality Assurance Manager (QAM) or test engineers shall generate software problem reports (e.g., ECPs, problem reports (PRs), engineering requests (ERs), change requests (CRs), or issues) on baselined products, in accordance with the procedures prescribed in the program CMP. The contractor shall create, track, and control these items as specified in the CMP.

The contractor shall present all quality metrics at each design review and make them available to the government to support other reviews.

The contractor shall ensure G-TSCMIS meets the performance metrics identified in the G-TSCMIS Measurements of Effectiveness (MoEs) and Measurements of Performance (MoPs) as found in the G-TSCMIS Capability Package 3. Where the contractor cannot meet any of these MoE/MoP parameters because of external constraints, the contractor shall notify the COR.

The contractor shall provide an index of the contractor internal (non-deliverable) data generated while performing the work described in this SOW upon government request, but no more frequently than quarterly in the form of a DAL (CDRL A017). The contractor shall retain all items until the final G-TSCMIS delivery to the customer and in accordance with the FAR Subpart 4.7.

## **3.3 Logistics Support (CLIN 0001, CLIN 0004, RDT&E)**

### **3.3.1 Leveraging COTS Data and NDI**

The contractor shall leverage COTS technical data and manuals for all COTS included in the G-TSCMIS software. The contractor should leverage existing documents developed for G-TSCMIS to minimize total ownership life cycle cost.

### **3.3.2 Training**

The contractor shall make available qualified technical Subject Matter Experts (SMEs) to assist in the training curriculum development process. The contractor shall review the training curriculum, facilitate courseware updates by providing remote access to a test environment, and participate in training system plan reviews or updates. The contractor shall provide experienced professional instructional system designers, as needed, who are able to support the SPAWAR Training and Development Support Center (TDSC) in any phase of training development.

The contractor shall provide training support to PMW 150 for training document reviews and updates. The G-TSCMIS Technical Manual Contract Requirements (TMCR) captures training requirements for G-TSCMIS.

### **3.3.3 User Manuals**

The contractor shall deliver a G-TSCMIS Software User Manual (SUM, CDRL A022) in accordance with the requirements to develop technical manuals authorized in SPAWARINST 4160.3B. Per the CDRL, SUMs are due with every delivery of the computer software product. The contractor shall leverage the content in the SUMs to serve as the basis for the embedded help system. The contractor shall create system documentation in Extensible Markup Language (XML) format using the specified system level document data (SLDD) and component product document data (CPDD) document type definition (DTDs). The contractor shall import the approved XML technical manual into the relevant Content Management Capability (CMC), to convert from XML to a portable document format (PDF) presentation.

The SUMs shall detail systematic instructions in two volumes: Volume 1 shall be the User Guide and Volume 2 shall address the Systems Administrator's Manual and include software installation and configuration procedures.

SUMs shall have the G-TSCMIS logo, provided by the Government, on the cover page.

### **3.3.4 Help Desk Support**

In support of remote help desk functions, the contractor shall provide Level 2/3 technical support to personnel who staff the SPAWAR System Center (SSC) Atlantic Tier 1 help desk. When the SSC Atlantic Tier 1 help desk contacts the contractor by email or telephone during normal business hours (8 a.m. – 5 p.m. Eastern Time), the contractor shall respond within one business day.

### **3.3.5 Installation Plan**

The contractor shall submit an Installation Plan (CDRL A025) with each delivered software iteration to provide instructions for loading and executing the software.

#### **4.0 Deliverables (CLIN 0004, CLIN 1003, RDT&E)**

The contractor shall deliver the documents listed in Exhibit A, G-TSCMIS CDRL in accordance with the specific direction provided in the SOW, CDRL, and data item descriptions (DIDs) listed in the CDRL.

The contractor shall submit any deliverables containing classified or sensitive information on compact disc (CD) or digital video disc (DVD) to the G-TSCMIS COR using appropriate means. Deliveries shall include all information necessary to enable the government to compile and configure the run-time executables, as described in the SDP.

#### **5.0 Government-Furnished Information and Government Furnished Property (GFP)**

In addition to the contract attachments discussed elsewhere, Government Furnished Information (GFI) includes the Release 2 software, Release 2 documentation, and ADS information when available. The Government NIPR/SIPR test environments will be made available to the contractor. In order to access government test environments, the contractor must submit the appropriate signed SAAR-N and PAA forms and obtain a DoD CAC and SIPR token.

The same NIPR data used by the Government test team will be made available to the contractor to facilitate testing at the contractor's facility.

#### **6.0 Other Direct Costs (ODCs)**

##### **6.1 Licenses (CLIN 0003, CLIN 1002, RDT&E)**

The contractor shall purchase software licenses as required to meet the requirements of this SOW.

Commercial software and software documentation delivered under this contract shall be subject to the terms of the contract and the governing commercial product license, to the extent the latter is consistent with Federal law and FAR Subpart 12.212, Computer Software. Notwithstanding the foregoing, the commercial product license shall apply only if a copy of the license / product key is delivered to the COR and accepted by the COR under the contract.

All software shall be, at a minimum:

- licensed and priced for use on a single computer or for use on any computer at the Government's hosting site
- in the name of the U.S. Government
- perpetual (also referred to as a nonexclusive, paid-up, world-wide license)

The contractor shall provide software and software documentation with license rights no less than rights provided with the software and the software documentation when sold to the public.

The license shall apply to any software changes or new releases.

Actual COTS license purchases shall follow COR approval of quantities, license key number delivery method, and manual quantities and type of media to be delivered.

Any use of reuse software, shareware or similar product requires pre-approval by the COR.

In situations where the purchase of new commercial software is needed to satisfy the requirements of the contract, the contractor shall first review and use available Software Agreements for Navy use. In the event that the software required to satisfy a particular requirement is not available to the contractor through a DoD ESI source, the contractor is authorized to obtain the software through an alternate source. The listing of COTS software available from DoD ESI sources can be viewed on the web at <http://www.esi.mil/>.

Use of government sources of supply is authorized for the purpose of fulfilling the terms of the contract. The contractor shall bill costs associated with ESI COTS software acquired in support of G-TSCMIS at cost (no fee) under the ODC CLIN(s).

## **6.2 Travel (CLIN 0003, CLIN 0004, CLIN 1002, CLIN 1003, RDT&E)**

Before any travel, the contractor shall submit a request to the COR for approval. The request shall include purpose, location, dates of travel and number of personnel. The contractor shall submit Trip Reports (CDRL A016) to the government within 5 working days of each trip.

For planning and cost estimating purposes, the contractor shall assume one trip for one individual to the Software Support Activity (SSA) in Charleston, SC to coincide with each iteration delivery. The contractor can make other trips as necessary to accomplish software development activities described elsewhere in this SOW.

## **7.0 Security**

### **7.1 Personnel Security Requirements**

The contractor's personnel shall possess security clearances up to the Secret level in accordance with the provisions stated in the DD-254. The contractor shall designate the level of personnel filling automatic identification system (AIS) IT-I, IT-II, and IT-III level positions and shall ensure those personnel

have completed appropriate access request forms. The Government will sponsor SIPR access for up to 2 contractor staff.

## **7.2 Facility Security Requirements**

The contractor shall have document storage capability up to and including Secret, in accordance with the provisions stated in the DD-254.