

Joint Tactical Radio System Network Enterprise Domain

Statement Of Work for JTRS EPLRS Crypto Mod Upgrade



19 Oct 2009

Prepared for

Joint Program Executive Office (JPEO) Joint Tactical Radio System (JTRS)

DISTRIBUTION STATEMENT D: Distribution to Department of Defense (DoD) and U.S. DoD Contractors for administrative/operational use only: (June 2007). All other requests for this document will be referred to the JTRS NED-W.

HANDLING and DESTRUCTION NOTICE: Comply with distribution statement and destroy by any method that will prevent disclosure of contents or reconstruction of the document.

1 Scope

1.1 Purpose

The purpose of this Statement of Work (SOW) is to support the Joint Program Executive Office (JPEO) Joint Tactical Radio System (JTRS) Network Enterprise Domain (NED) by upgrading the JTRS EPLRS v3.1 waveform software with the Crypto Mod upgrade included in the “Legacy” EPLRS waveform baseline.

1.2 Background

Compliance with the National Security Agency (NSA) Crypto Mod impacts all legacy and Joint Tactical Radio System (JTRS) DoD radio and waveform designs that employ COMSEC and/or TRANSEC cover. This SOW identifies the technical requirements for the JTRS EPLRS v3.1 software waveform in achieving Crypto Mod compliance.

1.3 Period of Performance

The Contractor shall propose an overall schedule to complete the analysis, coding, integration, formal test and certifications for the JTRS EPLRS v3.1 software changes required by Crypto Mod.

1.4 Place of Performance

The primary place of performance shall be the Contractor’s site. The Contractor also shall perform work at Government sites when necessary and/or directed by the Government. Contractor work at Government sites may include, but shall not be limited to short-term overnight trips as well as temporary or extended performance of work necessary.

1.5 Security

All work shall be performed in accordance with DoD and Navy Operations Security (OPSEC) requirements in accordance with the DD254.

All personnel working this requirement shall possess at least a SECRET security clearance at the time of delivery order award. The Contractor’s facilities shall be secure to the SECRET level due to the classified nature of the work to be performed.

The nature of this delivery order requires access up to SECRET information. The work performed by the Contractor will include access up to SECRET data, information, and spaces. The Contractor will be required to attend meetings classified up to the SECRET level.

Note: If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC PAC foreign travel team, OTC2, Room 1656 for action. A request for foreign travel form shall be submitted for each traveler, in advance of the travel to initiate the release of a clearance message at least 35 days in advance of departure. Each traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure, and a country-specific briefing within 90 days of departure.

2 Applicable Documents

Title	Reference
Software Communications Architecture Specification	Version 2.2, 17 November 2001
Software Communications Architecture Specification	Version 2.2.2, 15 May 2006
Software Communications Architecture Extensions	Version 2.2.2, 22 December 2006

Title	Reference
JPEO JTRS Standards Standardization Plan	Version 1.91, 03 Jun 2009
JTRS Test and Evaluation Laboratory SCA Test and Evaluation Plan	Version 1.1, 6 January 2009
JTRS Test and Evaluation Laboratory Standard API Verification Plan	Version 1.0, 04 April 2008
JPEO JTRS Software Standards	Version 1.2.2, 01 October 2007
IEEE/EIA 12207.0, Standard for Information Technology – Software life cycle processes	March 1998
IEEE/EIA 12207.2, Standard for Information Technology – Software life cycle processes – Implementation considerations	April 1998
JTRS Unified INFOSEC Criteria	Revision 2, 02 December 2005 (SECRET//NOFORN)
Network Enterprise Domain Software In-Service Support (SwISS) Plan	Version 1.1, 06 August 2008
JTRS NED T&E Waveform Portability Guidelines	Version 1.1, 26 June 2008
JPEO JTRS Enterprise Information Support Plan (E-ISP)	Version 1.1, 30 September 2008 (UNCLASSIFIED//FOR OFFICIAL USE ONLY)
Joint Tactical Radio System (JTRS) Information Repository (IR) User Registration Guide	Version 1.6, 07 May 2007

3 Requirements

3.1 General

3.1.1 Overview

The Contractor shall enhance the JTRS EPLRS v3.1 software waveform as required by the NSA Cryptographic Modernization initiative. The Contractor shall execute structured software engineering and program management processes that facilitate effective and high-quality software development. The Contractor shall ensure that all changes to the JTRS EPLRS v3.1 software waveform adhere to the JTRS Application Programming Interfaces (APIs) standards, JTRS Unified INFOSEC Criteria (UIC), JTRS NED Waveform Portability Guidelines, JTRS Software Standards, JTRS Software Communications Architecture (SCA) requirements, and interoperability certification requirements.

3.1.2 Acceptance Criteria

The Contractor shall conduct successful unit/module testing of the modified JTRS EPLRS software waveform, shall conduct successful Functional Qualification Test (FQT) and shall support the JTRS Test and Evaluation Laboratory (JTEL) API testing and SCA 2.2.2 certification. The Contractor shall integrate the modified JTRS EPLRS software waveform onto the GMR EDM hardware set for regression testing and for NSA delta IA assessment. Areas of activity shall include the following.

3.1.2.1 Functional Qualification Test (FQT)

The Contractor shall conduct successful regression testing of the modified JTRS EPLRS waveform in the GMR EDM environment. The Contractor shall make applicable updates and changes to test procedures, simulators and other test support software and hardware. The Contractor shall address any FQT deficiencies by making code corrections as agreed to by the Government. The Contractor shall develop and deliver applicable request(s) for deviations and/or waivers.

3.1.2.2 SCA and API Testing

The Contractor shall provide support to the JTRS NED program office and to JTRS Test and Evaluation Laboratory (JTEL) for successful JTEL API and SCA testing. Support shall include, but may not be limited to development of input for the JTEL API checklist, on-site manual code walk-thru(s), development of applicable request(s) for deviations and/or waivers and associated follow-up technical support. The Contractor shall address any deficiencies by making code corrections as agreed to by the Government.

3.1.2.3 NSA Review

The Contractor shall coordinate with the NSA for review of the modified JTRS EPLRS software waveform. The intent of this review is to prepare for the NSA delta IA assessment. The Contractor shall integrate the JTRS EPLRS waveform into the GMR EDM environment allowing complete testing/regression testing of the modified software in a known JTRS hardware suite and operating environment. The Contractor shall support the NSA delta IA assessment of the JTRS EPLRS software waveform as integrated into the GMR EDM environment. The Contractor shall support associated IA TIM(s), and coordinate with NSA regarding any deficiencies identified in the IA assessment, resolving any issues. The Contractor shall resolve all IA deficiencies by making code corrections as agreed to by the Government.

3.2 Specific

3.2.1 Software Enhancements

The full set of Crypto Mod requirements are captured in the following documents:

- 1) CJCSI 6510.02 COMSEC Modernization Planning,
- 2) CJCSN 6510 Information Assurance Cryptographic Equipment Modernization Requirements,
- 3) CJCSI 6510.06 COMSEC Releases to Foreign Nations, and
- 4) NSA/CSS Policy No 3-9 Cryptographic Modernization Initiative Requirements for Type 1 Cryptographic Products.

The Contractor shall integrate the updated "Legacy" EPLRS baseline waveform (including Crypto Mod) with the JTRS EPLRS v3.1 baseline waveform (including SCA wrapper) to produce an updated JTRS EPLRS baseline (including SCA wrapper and Crypto Mod).

As an optional maintenance update, the Contractor shall implement "Legacy" EPLRS waveform IA deficiency fixes, if not already accomplished at time of delivery order award. The Contractor shall identify and deliver a report of any "Legacy" EPLRS IA deficiencies that should not be corrected because of high risk to interoperability with the Army's "Legacy" EPLRS baseline. The contractor shall implement the "Legacy" EPLRS waveform IA deficiency fixes in a manner which best optimizes schedule. The Contractor shall provide/update all of the CDRL deliveries referenced in this SOW and listed in the Contract Data Requirements List (CDRL), DD Form 1423, Exhibit B.

3.2.2 Software Delivery (CDRL B008, B009, B010, B011, B012, B018, B022, B023, B024)

The Contractor shall deliver all software application releases and associated documentation to the NED Program Office in accordance with (IAW) the attached CDRL, DD Form 1423, Exhibit B.

3.2.3 Model Delivery (CDRL B027)

The Contractor shall deliver all waveform models created as a part of waveform enhancement activities covered by section 3.2.1 of this SOW to the NED Program Office IAW CDRL, DD Form 1423, Exhibit B.

3.2.4 Test Bench/Vector Delivery (CDRL B027)

The Contractor shall deliver all waveform test benches or test vector software created as a part of waveform enhancement activities covered by section 3.2.1 of this SOW to the NED Program Office IAW CDRL, DD Form 1423, Exhibit B.

3.2.5 Program Management

3.2.5.1 Contract Funds Status Report (CFSR) (CDRL A001)

In accordance with paragraph 3.2.8.1 of the basic contract SOW the Contractor shall submit one CFSR (DD Form 1586) under the basic contract that covers all delivery orders. Information from this delivery order will be included in the CFSR submitted under the basic contract. The CFSR report will include funding requirements and time-phased detail at the CLIN level, broken out for each delivery order. The Contractor shall also submit an MS Excel file for delivery to the Joint Tactical Radio System (JTRS) Network Enterprise Domain (NED) as defined in CDRL A001.

3.2.5.2 Contract Status Report (CSR) (CDRL A003)

The Contractor shall provide monthly CSRs. The CSR shall include at a minimum:

- Progress/status reporting for this delivery order and any deliverables identified in this SOW
- A running history of progress in meeting schedules, including a brief description of activities and accomplishments during each reporting period
- A Risk Matrix, maintained by the Contractor that identifies design, schedule, technical, resources, and other program element risks. The Risk Matrix shall be updated with each CSR.
- The following software metrics: (1) Software size e.g. Software Lines of Code (SLOC), (2) Cost/Schedule Percent Complete and (3) Software Defects to include separately FQT findings and IA Assessment findings.
- Program staffing (plan vs. actual)

The Contractor shall use the CSR to propose updates and changes, and document slippages to the deliverables schedule. Government acceptance of the CSR does not indicate concurrence with the CSR content or proposed changes to schedule(s).

3.2.5.3 Configuration Management

- The Contractor shall implement configuration management (CM) processes and maintain an internal CM Plan in accordance with the basic contract SOW.

3.2.5.4 Software Development Plan (SDP) (CDRL B014)

The contractor shall provide a Software Develop Plan (SDP) to the NED Program Office IAW the attached CDRL, DD Form 1423, Exhibit B.

3.2.5.5 Technical Library

As an optional maintenance task, the contractor shall provide shall obtain and integrate with the requirements management system, the specifications and technical documents for the v11.4 Crypto Mod baseline. The contractor shall establish in a baseline, and provide to the government the

specifications for the v11.4 Crypto Mod baseline. The contractor shall maintain for the government the documentation as a technical library.

4 Government Furnished Equipment

The Government shall provide any inherently governmental equipment, information, or property (GFE/GFI/GFP) necessary for completion of the effort(s) under this delivery order. Inherently governmental is defined as those items not available in the commercial marketplace, specifically those items only available for procurement by Government sources such as COMSEC, classified, or other sensitive/restricted equipment/information/property. The final roster of GFE/GFI/GFP shall be incorporated into the delivery order and provided to the Contractor after delivery order award. The Contractor shall accept delivery of the inherently governmental equipment, information, or property (GFE/GFI/GFP) from the Government at a location and time that will be determined after delivery order award.

5 Travel and Other Direct Costs

The Contractor shall propose travel and other direct costs (ODCs) required for completion of this delivery order.

6 Data Deliverables

- a. All data delivered and data made available during this delivery order shall be furnished electronically IAW DD Form 1423.
- b. Classified data shall be handled and delivered IAW the Department of Defense (DoD) 5220.22-M "National Industrial Security Program – Operating Manual, dated February 2006.
- c. All data ordered IAW DD Form 1423 shall be submitted with a Letter of Transmittal (LT) or provide Government notification via an E-mail to the Government Contracting Officer. The LT shall indicate the delivery order number, Contract Line Item, Sub-Line Item Number, Data Item Number, Title and Subtitle (when applicable) of the data, SOW paragraph number reference which required the data to be prepared, and the date of transmittal.
- d. DD Form 250s Material Receipt and Acceptance shall be submitted with final data deliveries only as specified on the individual data item (see Appendix A for the Contract Data Requirements List (CDRL) and applicable Data Item Descriptions (DID)).
- e. The Contractor shall provide a matrix, which states the delivery method for each CDRL deliverable (i.e. CD-ROM, Webpage)

7 Media and File Format

The Microsoft (MS) Office 2003 suite of applications (MS Word, MS Excel, MS PowerPoint, and MS Project) is the preferred format for documents, reports, and information furnished under this delivery order. If the Contractor's file format is not compatible with the formats specified, then the Contractor shall provide a compatible format that will allow the Government to read and write to the files when necessary. Should MS issue a new MS Office suite that the Government adopts as a new standard; the Government will notify the Contractor in writing of the change. Other formats for the transmittal of delivery order documentation and methods for electronically signing DD Form 250s Material Receipt and Acceptance shall be as set forth in the delivery order and as agreed to by the Government and Contractor.