

GXR Engineering Support - FINAL

TECHNICAL INSTRUCTION (TI)

Issue Date of TI	30 March 2009
TI No.	TI-4523-05 (R02 – No Cost Extension (NCE) of POP and Data Deliverable POC) Joint Exp Dog Star
Contract No.	N00178-05-D-4523
Task Order No.	FC01
Revision Date of TI	NA
Government Agency	NSWC Crane
Vendor	Referentia Systems, Inc.
Vendor POC	Kevin Jordan, (505)345-1641, kevin.b.jordan1.ctr@pacom.mil or at kjordan@referentia.com
Human Capital Checklist Approval Number	N/A
Task Description	<p>This TI establishes the tasks to be accomplished in support of an OSD sponsored demonstration of USPACOM Virtual Secure Enclave (VSE) capabilities within the Cyber War portion of USPACOM/JTF 519 Exercise Terminal Fury 09 as part of a larger C2/C2 Protect demonstration called Dog Star</p> <p>Background VSE is a USPACOM sponsored initiative to develop and validate defense-in-depth capabilities for improving computer network security in the Pacific Theater. The VSE concept for defense-in-depth is based on the USPACOM Chief Information Officer (CIO) Agile Coalition Environment (ACE) architecture. Several computer network experiments have been conducted over the past year by USPACOM, PACFLT and JTF-519 to validate the technologies and tactics techniques and procedures (TTP's) for employing an enclave strategy for defense-in-depth. Terminal Fury 09 Cyber War presents an ideal opportunity to assess adjustments made to the VSE architecture and associated TTP's based on lessons learned from earlier IO Range experiments. Cyber war will be conducted on the JFCOM Information Operations Range from 20 April to 8 May 2009.</p> <p>Objective Provide a "blue target network" environment for Terminal Fury Cyber War based on USPACOM approved VSE architecture. Demonstrate the ability to protect</p>

GXR Engineering Support - FINAL

	<p>crucial command and control with a defense-in-depth strategy that employs enclave barriers. Demonstrate the ability to discretely share selected information across enclave boundaries using an appropriate cross boundary solution. Demonstrate the ability to integrate sensors into the enclave architecture to improve defense-in-depth</p> <p>Requirements</p> <p>1 General</p> <p>The Contractor shall furnish all labor and materials necessary to accomplish the tasks described in this SOW except for the GFE and labor. The Contractor will arrange for access to the JFCOM IO Range through the SPAWAR, Pearl City, HI facility. The following specific tasks will be accomplished by the Contractor:</p> <p>1.1 Provide a Blue target network engineering diagram based on requirements to be identified by USPACOM J6/CIO/J81 and JTF519 J6;</p> <p>1.2 Coordinate JFCOM IO Range authorization with USPACOM, USJFCOM, and SPAWAR</p> <p>Procure equipment assets as required beyond GFE to install the target network on the IO Range;</p> <p>1.3 Procure equipment assets as required beyond GFE to install the target network on the IO Range;</p> <p>1.4 Integrate an appropriate cross boundary and sensor solution into the target network architecture for demonstrating the ability to share information selectively across enclave boundaries and detect anomalous network activity</p> <p>1.5 Assist the Government with integration of Government-Furnished Equipment (GFE) specified in Section 4 into the target network architecture;</p> <p>1.6 Demonstrate a working instantiation (lab demonstration) of the target network minus classified GFE at the Contractor's facility by 6 April 2009;</p> <p>1.7 Set up the target network at the SPAWAR, Pearl City, HI demonstration room during the week of 13 April 2009;</p> <p>1.8 Provide engineering support to manage the target network through the Cyber War demonstration from 20 April to 8 May 2009; and</p> <p>1.9 Assist USPACOM J81 is preparing a report of experimentation following Cyber War.</p>
Applicable Documentation	JFCOM IO Range documents
GFI, GFE, GFM	The Government will provide, on an as needed basis, access

GXR Engineering Support - FINAL

	<p>to all government information necessary to complete the requirements of this TI. The Government will provide GFE identified below and personnel to install and operate it during the Cyber War demonstration.</p> <ul style="list-style-type: none"> - Two (2) Global Command and Control System-J (GCCS-J) servers - Two (2) Same Time Chat servers - Two (2) Theater Battle Management System (TBMCS) servers - C2PC client software - Two (2) STE secure telephones
Duty Location	Contractor Facility, Honolulu, HI and SPAWAR demonstration facility in Pearl City, HI
Temporary Duty/Travel Requirements	Honolulu, HI to San Diego, CA, SPAWAR, 1 trip, 5days, 2 persons. Honolulu, HI to Washington DC, 1 trip, 7days, 1 person
SLIN Number(s)	100005 (Year 1)
Period of Performance	31 March 2010 (R02 - NCE)
Data Deliverable (s)	<p>All data deliverables shall be submitted electronically to: amy.haworth.ctr@navy.mil (R02)</p> <p>The contractor shall provide the following deliverables for this TI:</p> <ol style="list-style-type: none"> 1. Program Management Plan 45 days after Contract Award 2. Monthly Status report 30 days after contract award and then every 30 days after that A002 3. Trip Reports Three days after trip completion A010 4. Blue target engineering diagrams 2 weeks after contract award 5. Funds and Man-hour Expenditure Report B001 - Monthly 5. Plan of Action and Milestones (POAM) F001 6. Technical Report /Final Report and demonstration F002
Security Classification	IAW Paragraph 6.3 of basic Task Order. SECRET
Hazard and Safety Information	IAW Paragraph 6.9 of basic Task Order.
Requiring Technical Activity (RTA)	Mr. James R. Williams, PACFLT N6T, james.r.williams@navy.mil , Phone: 808.474.5717
Task Order Manager (TOM)	Brant Ackerman, (808) 477-9552, brant.t.ackerman@navy.mil D.Y. Anderson, 812-854-5176, denise.anderson@navy.mil (R01)

Contingent Upon Task Order Modification Issuance to Increase Funding
 Funding is currently available on the Task Order