Strike Group, LLC SeaPort-e Subcontractor

Subcontractor Company Information	
Company Name and Address:	Conscious Security, Inc., 1000 Corporate Drive, Suite 119, Stafford, VA 22554-4885
Point of Contact Name, Phone Number and Email:	Jeff O'Dell, 540.850.2059, jeff.odell@consciousssecurity.com
Proposed Functional Area(s):	– 3.2 Engineering Support – 3.5 System Design Documentation and Technical Data Support – 3.6 Software Engineering, Development, Programming, and Network Support – 3.12 Information System (IS) Development, Information Assurance (IA), and Information Technology (IT) Support – 3.18 Training Support3.20 Program Support
Registered in SeaPort Website: https://auction.seaport.navy.mil/registration	Yes, Seaport-e contract number: N00178-10-D-5967, CAGE Code: 4DY30, DUNS: 165427373
Subcontractor Agreement in Place with Strike Group, LLC:	TBD

Reference #1	
Client Name and Address:	MCSC GCSS-MC, PM-LIS, Albany GA
Point of Contact Name, Phone Number and Email:	Jeffrey Sanders, 229.639.7339, Jeffrey.sanders@usmc.mil
Contract Number:	N00178-10-D-5967-MU61 (Conscious Security, Inc. PRIME)
Period of Performance:	9/28/2012-9/27/2013
Contract Description:	**GCSS-MC PM LIS Programmatic Support**
Similarity to Proposed Functional Area:	**Conscious Security, Inc.** currently provides programmatic and cyber security support to the PM GCSS-MC LIS, MCSC, Albany, GA. This support includes IA programmatic support services that span system Certification and Accreditation (C&A), Information System Security Engineering, development of Interoperability and Supportability Certification documentation, and management of records in official IT repositories. We register, monitor, update, and maintain LIS system records in tracking tools, databases, and systems, to include the Department of the Navy Application and Database Management System (DADMS), DoD Information Technology Portfolio Repository-DoN (DITPR-DoN) and the MAGTF Collaborative Architecture Environment (MCAE). Our program management support includes the development, maintenance, and updates of Enterprise Architecture drawings and all documentation to satisfy Joint Interoperability and Supportability Certification requirements. Smartronix assists in the development of Information Security Architectures supporting Post Deployment Software Support (PDSS) activities conducted by the GCSS-MC LIS Program Office. We provide IA support that encompasses the complete accreditation process. Our personnel also evaluate GCSS-MC LIS Automated Information Systems (AISs) to include unique system requirements, determine the appropriate level of documentation, conduct audits, prepare required documentation, and collaborate with all necessary Government Representatives to ensure all required security certifications are obtained. Conscious Security is responsible for achieving and maintaining DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation for more than 50 logistics systems. The drafting of all documentation is completed using the Marine Corps Certification and Accreditation Support Tool (MCCAST), currently XACTA, and the System

	Engineering, Interoperability, Architecture, and Technology (SIAT) gated process. This includes all documentation and requirements to achieve Joint Interoperability Certification (JITC) for each system or family of systems. Our IA professionals develop and review System Identification Profiles (SIPs), DIACAP Implementation Plans (DIPs), System Information Briefs, Certification and Accreditation Tasks and Milestones, Ports Protocols and Services, Backup and Restoration plans, Incident Response Plans, Threat Models, Account Management Plans, Configuration Management Plans, Contingency Plans, Detailed Test Plans, Validation Plans and Procedures, and Plans of Action and Milestones (POA&M) for each USMC logistics application. We also draft and conduct Internal Validation and Verification exercises and coordinate risk mitigation procedures in support of DIACAP. Our IA professionals developed multiple secure baseline images upon which to build the new LIS systems. Additionally, Conscious Security Team members collaborate with the LIS IAM, IAO's, and Project Officers to develop numerous internal processes to ensure assigned IA Controls are met. These include generic and system specific versions of processes to control configuration management; access management, document review and management, Contingency Plan test execution, Annual Security Review execution and internal IA control validation among others. **Specific Tasks & Accomplishments:** Conscious Security's key accomplishments on this contract include: • Achieved and maintained nearly 100% Certification & Accreditation of all GCSS-MC LIS supported systems. – Only one (1) remains, awaiting DAA signature. • Met nearly 100% interoperability requirements of all GCSS-MC LIS supported systems. • – Only one (1) remains, awaiting DoD CIO signature. • Developed an integrated C&A project management process to ensure configuration management of all C&A documentation. • Developed numerous internal LIS operational processes and policies to support compliance with DoDI 8500.2 IA Controls to include: Backup and Restoration plans, Incident Response Plans, Account Management Plans, Configuration Management Plans, Contingency Plans. Maintained a stable staff with minimal turnover that exceeded contract requirements for staff certifications.
Reference #2	
Client Name and Address:	**PG10, Marine Corps Systems Command, GDIT Prime Conteractor**
Point of Contact Name, Phone Number and Email:	Greg Sharpe, 703.630.5731, greg.sharpe@gdit.com
Contract Number:	M67854-09-D-4726 DO# 08ESM354354
Period of Performance:	08/2010 – 07/2011
Contract Description:	**USMC Tactical Collaborative Work Suite (TCWS) Software Support**
Similarity to Proposed Functional Area:	**Conscious Security** provided IA, DIACAP, and information systems security engineering (ISSE) support for the TCWS hardware components under another task order. We provided IA Type Accreditation in support of engineering, procurement, integration, testing, fielding, and training for TCWS 2.0 hardware platform. Our delivery of security engineering services, subject matter expertise, and IA oversight ensured the delivered solution was successfully subjected to the DIACAP process, met all required security controls, and achieved an Authority to Operate (ATO). This contract was separate but related effort encompassing implementation of the software components for the TCWS Hardware procurement. As a result of our standing relationship with the TCWS software prime vendor, GDIT, and positive feedback from the government client regarding success on previous work

	including TCWS hardware where we provided the same services for iGov, GDIT subcontracted our team on their task order contract to perform the Information Assurance, DIACAP, and information systems security engineering (ISSE) support for the TCWS software effort. The size, scope, and complexity of the TCWS contract is similar to the PM GCSS-MC LIS PDSS support as we will be supporting several applications in various states of maturity which are being hosted on a number of different software/hardware configurations. Just as with TCWS, Conscious Security will provide direct input, coordination, and oversight support for IA, C&A, Cybersecurity, and maintenance throughout the DIACAP process, ensuring all required security controls, and maintaining Authority to Operate (ATO) for all systems identified in PWS Appendix 1. **Specific Tasks & Accomplishments:** On the TCWS Software contract Conscious Security provided: • a complete DIACAP Package; • data flow diagrams that included Internet Protocol (IP) to IP communications and types of data being transmitted and documentation describing the data flow between each device; • system ports and protocol document that included device source and destination locations, protocols, service types, ports in use, and encryption/tunneling devices; • network/architectural diagrams; • hardware/software/firmware list, to include manufacturer, descriptions, versions, functions, and categories (i.e., Commercial Off-The-Shelf [COTS] and Government-Furnished Equipment [GFE]); • external interfaces and connections. • Version Description Document (VDD), Software Design Document (SDD), Software Version Description (SVD), and/or Approved Baseline List (ABL); • information on how the system complies with DoDI 8500.2 IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL); • backup and disaster recovery/restoration procedures, as required by the Federal Information Security Management Act (FISMA); and • storage and replication procedures. Additionally, Conscious Security documented and implemented the agreed-upon security lockdown procedures prior to the Government's T&E. We conducted/participated in meetings and IPRs as needed to accomplish required Government testing. We supported the Government development of accreditation and IA requirements by providing assistance in analyzing the adequacy of the required protective features, assessed residual risk, and assisted in determining the readiness of the system for accreditation. For detected vulnerabilities that could preclude accreditation, we recommended human procedures, software configuration parameters, system changes, or combinations thereof to mitigate the risk associated with the vulnerability. We ensured all COTS IA devices and IA-enabled devices were procured as described in DoDI 8500.2 and National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11. COTS products were evaluated and validated in accordance with the International Common Criteria for Information Technology Security Evaluation or the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2, as appropriate. We also maintained the DIACAP status for TCWS software components in the USMC workflow tool (currently XACTA IA Manager).
Reference #3	
Client Name and Address:	MCNOSC, Quantico, VA
Point of Contact Name, Phone Number and Email:	Lisa Adkins, 703.784.5060, lisa.adkins@usmc.mil

Contract Number:	89927DBS45
Period of Performance:	03/28/08-03/27/14
Contract Description:	**MCNOSC PKI**
Similarity to Proposed Functional Area:	Conscious Security provides Public Key Infrastructure engineering, information assurance, policy, and project management support. This includes work with supporting technologies such as certificate validation, middleware, public key enabling, and alternate tokens. To support the Marine Corps' implementation of the DoD PKI, the Team leveraged current operations using existing technologies and architectures with Marine Corps and industry best practices to satisfy future PKI requirements as part of HQMC C4's overall Information Assurance (IA) and network defense-in-depth plan. Team members on this effort had been involved in supporting the Marine Corps implementation of DoD PKI since August 2000. The mission requirements and organizational structure unique to the Marine Corps required a tailored and vetted approach to implementation across the enterprise. The ultimate goal was to maintain a reliable infrastructure capable of providing required PKI security and supporting services (e.g., directory services, certificate validation, alternate token) for all garrison and deployed Marine Corps networks and applications. A significant component of this work is the security and accreditation lifecycle management of the supporting infrastructure daily operation, maintenance and upgrade activities. **Specific Tasks & Accomplishments:** • Providing Program Management for a composite team delivering IA support to 6 worldwide locations including Japan, Hawaii, California, North Carolina, Virginia, and Germany, in support of the MCNOSC mission. The MCNOSC maintains a secure, heterogeneous, multi-tiered network in support of classified and unclassified information exchange requirements for the Marine Corps. • Providing support for implementation of the DoD PKI in the Marine Corps with an operational focus on the implementation, management and sustainment of Marine Corps Enterprise PKI. This support includes PKI registration services for authorized personnel and systems at Marine Corps installations world-wide. • Providing a fully functional capability to issue Alternate PKI Tokens to Marine Corps system users. This capability further reduces the risk associated with username/password when use of the CAC is not feasible. • Providing a fully functional capability to issue SIPRNET PKI Tokens to Marine Corps system users. • Providing fully integrated PKI services to elements of the MCEN in conjunction with the Marine Corps upgrade for Active Directory. This extends the Marine Corps capability to take cryptographic logon from in-garrison to deployed locations. • Providing inventory tracking of MCNOSC PKI-controlled hardware, software, and licenses using MCNOSC-designed databases and inventory control procedures. Preparing POM submissions, a Fiscal Year PMC Procurement Plan and an O&M Budget Plan. • Providing technical expertise for applications ensuring confidentiality, authentication of network transactions; data integrity; and non-repudiation of transactions across the Marine Corps network infrastructure. • Provided expertise and systems Information Assurance Manager maintaining the infrastructure security through appropriate patching, IAVA tracking and compliance, and best practices. This effort protected the security posture of the system with a rigorous security lifecycle management program that maintained the system accreditation and ensured no system downtime due to security-related incidents; PKI was the model program for the client organization in this regard. • Participating in planning and policy related working groups that impact Marine Corps Information Assurance programs and operations. Meetings held at the DoD and Service level deal with subjects including

	Certificate Policy Management, program development for DoD PKI Increment 2, cross service technical interchange, Identity Protection and Management, test and evaluation, NMCI integration, and PKI interoperability with partners external to DoD. • This work demonstrates Conscious Security's capability to provide in-depth Security-related Program support and FISMA program support and capability to performance significant technical analysis. • This work demonstrates successful transition planning for work not previously supported by Conscious Security with no impact on government operations • This work demonstrates the use of multiple IA tools to manage risk and vulnerabilities across large network architecture. • This work demonstrates use of personnel and resources in multiple worldwide locations. This work demonstrates a broad technical use of multiple Information Assurance capabilities including certification and Accreditation, CND, IA Assessment Teams, PKI, PKE, IA training, and IA Policy development and implementation.

Additional Company Information:

Founded in 2003 and based out of Stafford, Virginia, Conscious Security draws from expertise in the Department of Defense (DoD) and commercial industry to deliver a best-practices approach for today's challenging security services and initiatives. Conscious Security has been a long-term business partner of the Department of Defense (DoD) and the US Marine Corps (USMC) Information Assurance and Security community in the fields of Public Key Infrastructure (PKI), Identity and Access Management (IdAM), Certification and Accreditation, Vulnerability Assessments, and Desktop Standardization and Compliance. Conscious Security leadership has been supporting these efforts for over twelve years, providing SME support that has helped the DoD move forward with significant IA initiatives that are securing DoD networks on a daily basis. It was from our early efforts, successes, and relationships that Conscious Security was born. That success continues and so do our diligent efforts to partner with government and fellow industry to secure our Nation's networks and systems.

Conscious Security understands the unique challenges of the DoD Cyber Security environment. Each day, our team is supporting mission critical infrastructures that are threatened daily. We understand the important security concerns and requirements that are many times overlooked by application owners and/or systems administrators, and offer our expertise to ensure the integrity of Navy and Marine Corps Enterprise systems and networks are strengthened. We have supported many highly visible enterprise system implementation projects up to and including ACAT Level I programs. Our team's blend of high quality expertise, experience, and strong desire to support the Nation's Cyber Defense mission will enable us to provide Certification and Accreditation support that meets or exceeds the requirements of our clients.

Since Conscious Security is a niche cybersecurity firm, approximately 80% of our technical staff is certified at IAT Level III with CISSP certifications, and many are also Certified USMC Validators. In fact, Conscious Security is an accredited USMC validator, and the only HQMC C4 approved validation-training resource for USMC Information Systems under the cognizance of the USMC Designated Approving Authority (DAA). As such, we have been approved to teach our internally developed Marine Corps Validator Course curriculum, and conduct approximately 12 classes annually to military, civilian, and contractor personnel at our facilities and other government or industry facilities.

Conscious Security, as a Veteran-Owned Small Business (VOSB) meeting the small business size standard for NAICS 541330 with 22 employees, has established itself as a leader in providing Information Assurance services to both government and private industry customers. While we understand we are still small, we have found that with knowledge and experienced subject matter experts who understand the security requirements within DoD, we can accomplish a more complete and accurate validation or security assessment; typically in a shorter time period compared to many of our competitors.

SeaPort-e Functional Areas

Immediately below is a listing of the 22 SeaPort-e Functional Areas.

1) Research and Development Support
2) Engineering, System Engineering and Process Engineering Support
3) Modeling, Simulation, Stimulation, and Analysis Support
4) Prototyping, Pre-Production, Model-Making, and Fabrication Support

5) System Design Documentation and Technical Data Support
6) Software Engineering, Development, Programming, and Network Support
7) Reliability, Maintainability, and Availability (RM&A) Support
8) Human Factors, Performance, and Usability Engineering Support
9) System Safety Engineering Support
10) Configuration Management (CM) Support
11) Quality Assurance (QA) Support
12) Information System (IS) Development, Information Assurance (IA), and Information Technology (IT) Support
13) Inactivation and Disposal Support
14) Interoperability, Test and Evaluation, Trials Support
15) Measurement Facilities, Range, and Instrumentation Support
16) Logistics Support
17) Supply and Provisioning Support
18) Training Support
19) In-Service Engineering, Fleet Introduction, Installation and Checkout Support
20) Program Support
21) Functional and Administrative Support
22) Public Affairs and Multimedia Support

Upon request, a complete description of the above functional areas will be provided.