CONSCIOUS SECURITY, INC.

…Think about IT

A Veteran - Owned Small Business

Conscious Security provides Information Technology Operations and Security services to commercial and government organizations. Our core competencies include system and security infrastructure, information technology, identity and access management, public key and supporting technologies and training.

A small veteran - owned business founded in 2003 and based out of Northern Virginia, Conscious Security has Department of Defense and private industry expertise that we use to deliver a best- practices approach for today's cyber security challenges.

Core Competencies

- Cyber Security
- Certification & Accreditation (C&A)
- Identity and Access Management
- Public Key Infrastructure
- Information Technology
- Risk Management

Delivering a best-practice approach for today's challenging security services and initiatives

Mission Statement:

Provide expertise to customers in overcoming challenges through solutions that provide a significant return on investment and have a profound impact on the effectiveness of client organization's information security program.

CYBER SECURITY

System &Infrastructure Security/Information Assurance. Protecting information and information systems by preventing, detecting, and responding to attacks. Effective policy is the first step to ensuring a solid security framework from which to base system development, operations and life cycle management. We can help establish a well-developed network security and management plan that aligns with the customer's business processes and strategic objectives. We can help enforce policy with proven methodologies in penetration testing, vulnerability assessments and remediation, and security awareness programs that will help bring operations compliance with internal policy and external regulations. This is accomplished, in part, by proper cataloging of assets and identified vulnerability data showing a total threat picture that includes trend analysis and classifications to provide decision makers the ability to accurately evaluate the present threat condition and apply appropriate mitigations for system protection.

C&A

All information systems operating on DoD networks must be certified for compliance with DoD security requirements and accredited for operation. Our staff of experienced subject matter experts, information systems security engineers, security analysts, and validators can assist with IA policy and control evaluations, Information Assurance (IA) and network assessments, preparation of supporting DIACAP package and artifacts, implementation of security postures, and Subject Matter Expertise (SME) in IA life cycle management, coordination, implementation, deployment, and sustainment.

IDENTITY AND ACCESS MANAGEMENT

Access rights, Provisioning, Authentication and Directory Services. Provide a basis from which all systems access springs; corporate users, customers, partners, and suppliers all managed within a single authoritative system. Realize the potential of effectively and securely linking people, applications, and content.

PUBLIC KEY INFRASTRUCTURE

Policy, Implementation and Technology Integration. PKI is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions both internally and externally. By employing this technology for clients, we help them get a firm handle on their users, applications, and hardware infrastructure within the organization. Through policy and technology implementation, PKI will secure logical network access, infrastructure communications, and application transactions with proven technologies. Realize the benefits of authenticating identity, verifying integrity, ensuring privacy, access authorizations, transaction authorizations, and support for non-repudiation.

INFORMATION TECHNOLOGY

Systems Analysis and Network Engineering services based on a complete understanding of customer requirements while keeping security in the forefront of the development process.

RISK MANAGEMENT

The identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Our staff of SME's can assist your organization in managing the risk associated with your enterprise systems, calling on years of experience in operational environments and applying their risk management expertise to create value by institutionalizing RM processes and activities to reduce costs and minimizing the negative effects of risks.

KEY INFORMATION

www.conscioussecurity.com
CAGE Code: 4DY30
DUNS: 165427373

1000 Corporate Drive,
Suite 119 Stafford,
Virginia 22554
540.318.0909

NAICS: 42330, 423490,443120, 454111, 541330, 541511, 541512, 541513, 541519, 541611, 541690, 541712, 611420, 611430, 811212

SeaPort-e N00178-10-D5967

Conscious Security, Inc.

…think about IT

TRAINING

Certification and Accreditation:

All information systems operating on a United States Marine Corps network must be certified for compliance with DoD security requirements and accredited for operation. In April 2010 the CIO of the Marine Corps published MCBUL 5239, MARINE CORPS CERTIFICATION AND ACCREDITATION PROCESS (MCCAP) VALIDATOR REQUIREMENTS establishing the USMC program to authorize “Validators” to perform IA testing on Marine Corps systems. Validators act as the USMC DAA’s trusted agents for completing technical and non-technical information assurance assessments of Marine Corps Information Systems based on the IA Controls in DOD Instruction 8500.2. Conscious Security is the first company authorized as an approved Validator training service provider.

COURSES OFFERED

Marine Corps Enterprise Network Validator Course

This course will walk students through a refresher of DIACAP, the Validator process and specifically how C&A validation is implemented within the United States Marine Corps and the Department of Defense.

Hands-On Training:

Students are immersed in the use of currently utilized Department of Defense assessment tools, USMC specific tools, and emerging tools that are currently being introduced into the IA space. Emphasis is placed on the use of MCCAST (the USMC C&A tool), risk analysis and reporting, C&A package processing and determining an accurate residual risk posture.

Qualification:

Successful course completion requires all students to take and pass a written and practical exam. Each exam requires a passing score of 70%. Passing both exams demonstrates mastery of the course.

Course Completion Certificate:

Students will receive a certificate of completion from the Designated Accrediting Authority verifying mastery of the course.

Marine Corps C&A for the Program Manager

This course is focused on Marine Corps Program Managers and Information Assurance Managers. Training is focused on the use of MCCAST and the creation of the Certification and Accreditation Package.

Hands-On Training:

This course is focused on program management responsibilities in the Certification & Accreditation process and the details of Pre-Validation methodologies in relation to the Marine Corps validation process. Students are trained in the use of MCCAST and the creation of the C&A Package. Emphasis is placed on the use of MCCAST to track lifecycle sustainment of a system’s IA compliancy.