



# Information Assurance

*A Division of VSE Corporation*



## INFORMATION ASSURANCE CAPABILITIES

**High performers are committed to consistent improvement, not drastic change** – Testing and evaluating a network’s security requires specialized knowledge and tools, both of which come at a high cost if acquired for in-house use. Contracting outside security specialists to perform an assessment not only saves long-term expenses but also provides the objectivity needed for evaluating the network security.

VSE can go far beyond simple external assessments. We offer you security solutions. VSE Corporation’s Information Assurance team addresses a wide scope of security concerns including policy, premise, network, business and government regulation issues. Based on your need, the assessment applies multiple discovery tools to detect internal and external threats. Our assessment provides you a clear, step-by-step analysis of the audit with comprehensive recommendations and budgetary cost estimates for mediating vulnerabilities discovered. No agency wants to be vulnerable. An attack on your network infrastructure can compromise your resources, putting employees and even citizens at risk.

### **Maximizing Your Investment in Information Technology Security & Risk Management**

**Six Sigma Approach** – The Six Sigma proven concepts are a natural complement to IT security and Information Assurance. The common thread is to identify and eliminate sources of waste and activities that do not add value, in order to create flow with maximum productivity, capacity, and throughput. Lean methodology incorporates tools within a structured roadmap, with data and calculations behind every decision made in designing the optimum process flow.

Six Sigma is heavily driven by quantitative analysis and the assumption that all processes must, to be efficient, be repeatable. But how do you gain this consistency and create control with

your security? The answer is through the integration of sophisticated, well-tailored solutions into key processes.

By applying Six Sigma methodologies to best security practices we maximize the efficiencies often lacking in security. Standards and methodologies provide repeatable and predictable means of delivering quality security services.

Our certified specialist’s help you combat potential threats and safeguard agency assets, so your staff can focus on its core competencies and responsibilities. Civilian and defense agencies already depend on our expertise to protect their electronic intelligence. You can overcome your security challenges through our portfolio of offerings:

- **Design and execution of Certification and Accreditation (C&A) documentation using DITSCAP, NIACAP, NIST, OMB, and agency requirements**
- **System Security Plans**
- **Penetration Testing**
- **Disaster Recovery Planning**
- **Firewall technology**
- **Public Key Infrastructure (PKI)**
- **Intrusion Detection System (IDS) implementation**
- **Risk and vulnerability assessments**
- **System security plan development**
- **Design of secure networks and applications**
- **Design and performance of security test and evaluations**

Our staff is thoroughly knowledgeable in the federal statutory requirements of automated information security, as well as guidance issued by the National Institute of Standards and Technology (NIST), and the General Accounting Office's recommended best practices. We have active government security clearances and hold industry-recognized credentials, such as: Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM), National Security Agency Information Assurance Methodology (NSA-IAM), Microsoft® Certified System Engineer (MCSE), and the Cisco Certified Design Architect (CCDA) and others.

- **Minimize exposure to fraud, misuse and disruption**
- **Identify and eliminate infrastructure weak points and redundant systems**
- **Bolster your IT team with certified specialists who can design and deliver a turnkey solution**
- **Leverage new technologies to strengthen security measures across your agency**
- **Safeguard the integrity of all your data**
- **Re-engineer your processes to reduce vulnerabilities**
- **Fortify network infrastructure from sophisticated attackers with intrusion detection system**

**Risk Analysis (RA):** VSE analyzes your system vulnerabilities and determines the potential impact of a loss of information or capabilities to your system. Our risk analysis cites identified and potential vulnerabilities, and documents detailed recommendations for minimizing risks within the operating environment. It also includes a cost-benefit analysis and implementation plan. The results of this analysis are provided in report form and can be used in conjunction with the C&A process.

**Certification and Accreditation (C&A):** VSE conducts a comprehensive evaluation of the technical and non-technical security features of your systems and other safeguards, made in support of the accreditation process. We determine the nature and level of compliance your organization has relative to federal guidelines, such as NIST, 800-26, OMB A-130, FISMA, DITSCAP, NIACAP or your industry best practices. We work to assist your agency to gain formal system approval to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. To meet certification and accreditation guidelines, we provide the following services: *Security Planning, Risk Assessment, Security Test and Evaluation, Security Training, and Disaster Recovery*. This includes on-site information assurance and security consulting, physical security management for data centers, information technology policy development, managed security monitoring, vulnerability/penetration testing, and compliance with federal regulations.

**Security Test and Evaluation (ST&E):** VSE conducts systems testing to obtain technical information to support accreditation and certification of your systems. We establish a team of technical experts to create the test based on your organization's specific needs, and identify existing and non-existing controls, threats, and vulnerabilities to be tested. Our team then prepares a security test and evaluation plan for your agency approval, and afterwards conducts the security test and evaluation and documents the results. These results can be used to support the C&A process.

**System Security Plans (SSP):** VSE creates and/or updates security plans for your organization based on your documented policies and procedures. Our security planning provides an overview of your systems security requirements and describes the controls in place, or planned, for meeting those requirements. Our security plan also delineates responsibilities and expected behaviors of all individuals accessing

## INFORMATION ASSURANCE CAPABILITIES

your systems, and documents the structured process of planning adequate, cost-effective security protection for your systems. Our security plan reflects input from those managers with responsibilities concerning your systems, including information owners, the system operator, and the system security manager. The structure/format of the basic plan is organized according to your needs, and additional information is included. These results can be used in conjunction with the C&A process.

**Penetration Testing:** VSE determines if existing control measures are adequate to protect systems; identifies network and system vulnerabilities with remote probing techniques and internal testing; and demonstrates vulnerabilities by acting and employing techniques used by hackers. We review hardware, software, and telecommunications environments, and physically test the current hardware, software, and telecommunications systems via penetration techniques to identify technical vulnerabilities.

**Vulnerability Test Laboratory:** VSE evaluates vulnerabilities in network equipment, mainframe computers, personal computers, firewalls, anti-virus software, and intrusion detection software. We develop vulnerability tools that expose network, host, and application level vulnerabilities (these tools vary from modified public domain utilities to advanced packet generators, enabling us to perform the most sophisticated attacks using proprietary scanning tools). We develop an application vulnerability database, including published and unpublished vulnerabilities, exploit scripts, and possess intuitive knowledge of future standards and technologies to ensure our clients are provided with a broad range of best-in-industry policies, standards and practices upon which to benchmark their capabilities.

**Disaster Recovery and Business Continuity Planning:** VSE develops a Business Continuity Plan that emphasizes continuity of critical functions with minimum interruptions. The plan

documents procedures for rapid recovery of critical systems in the event of a disaster that renders your primary processing site inoperable. The plan includes preventive measures for mitigating high-risk occurrences, business resumption procedures, and contingency plans for recovering critical processing environments. The plan also documents testing procedures.

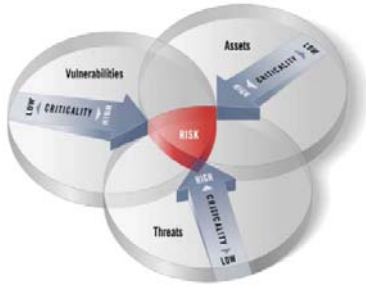
**Security Awareness Training:** VSE develops and delivers a comprehensive security awareness course and training manual detailing security policies and procedures for sustaining information assurance of your systems and personnel. All classes are taught by experienced trainers with CISSP certifications and at least 10 years of industry experience to relate for increased employee comprehension and retention. VSE develops custom training programs based on your requirements, environments and applications.

The value of data in today's information age has forced organizations to increase efforts to mitigate information security risks and maintain their market standing. But providing an effective level of security requires a combination of state-of-the-art technology, experienced personnel, proven processes, and continuous threat intelligence that few organizations possess. Those organizations that choose to tackle these critical issues in-house invariably find themselves struggling to identify security events, provide security event alerts, respond to threats, and manage the security risks that threaten their competitive advantage. VSE's IA professionals can assist with the design and development of secure computing infrastructures and provide a level of technology and expertise that ensures a rapid response to real threats. VSE's IA professionals have extensive experience in the management, design, development, implementation, integration and operation of secure systems, are well published, and are frequent presenters at national and international conferences such as the Federal Information Assurance Conference (FIAC).

### Site Physical Security:

Your information security controls rely on physical security controls that may or may not be within your organization's management

purview. The safety of employees, facilities, and assets is critical to the success of your organization. For maximum protection, you need a thorough understanding of your site's vulnerabilities and all risk related issues you face related to physical security.



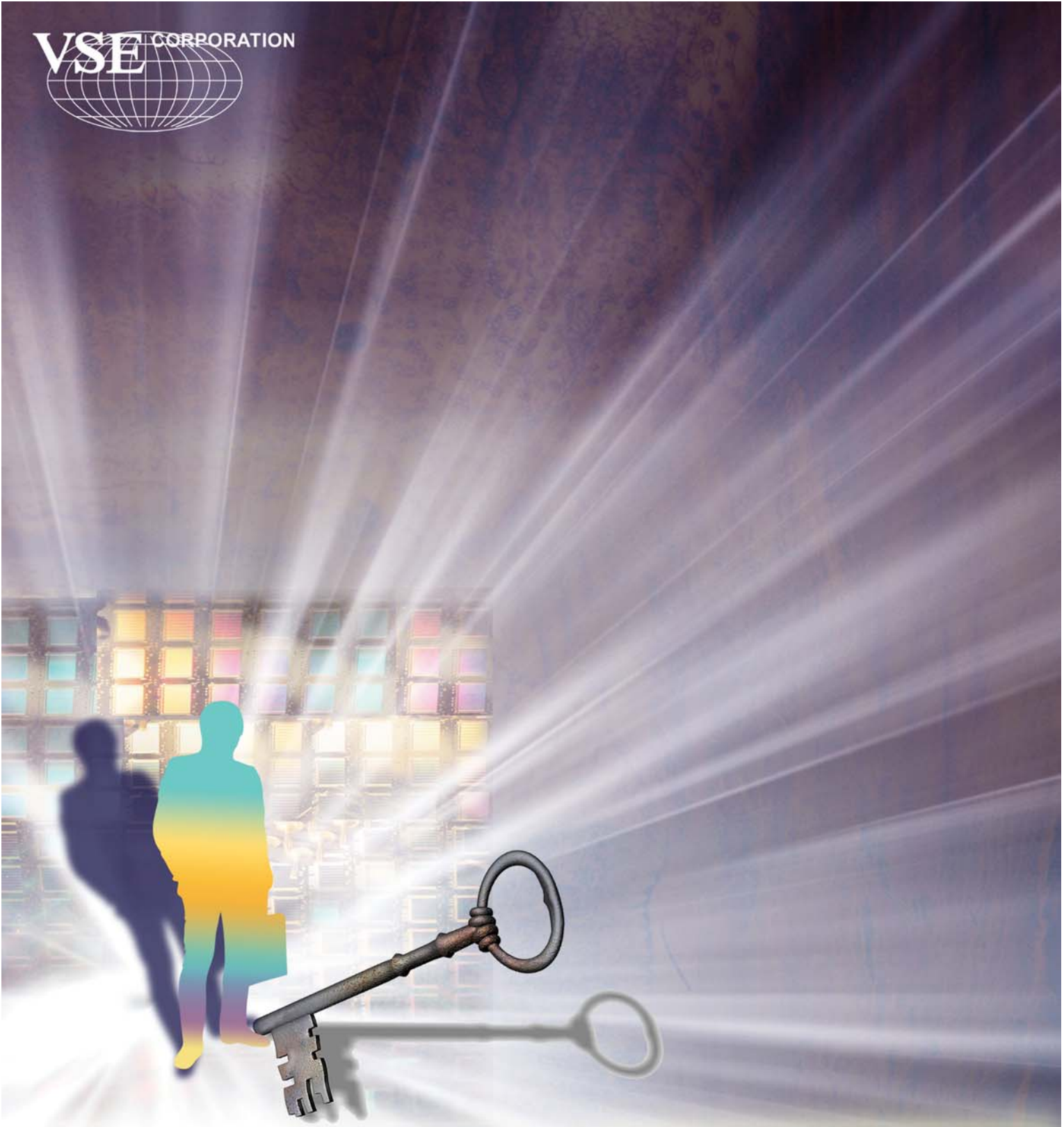
VSE Information Assurance Division Physical Security Assessment services provide an in-depth review of site security controls and processes used at your site or throughout your enterprise. We conduct this review against your corporation's security standards, established VSE Information Assurance Division procedures and guidelines, and a standards-based, best practices industry baseline. We can also include social engineering and infiltration testing. The goal is to help you achieve a secure working environment for employees and other persons working at or visiting your facilities and to help you establish processes that ensure the protection of intellectual assets and all site facilities.

### AVAILABLE CONTRACT VEHICLES:

**CECOM Rapid Response (R2)** – The R2 contract is an ID/IQ contract that supports the U.S. Army, Department of Defense and U.S. Federal Agencies. The R2 contract features a competitive, streamlined acquisition process (in as little as 19 days); full contracting support with low administrative support cost; and a broad SOW and selection of labor categories. For more information, see <http://r2.vsecorp.com>.

**GSA MOBIS Schedule** – MOBIS is a flexible task-order schedule to provide management, organizational and business improvement services so that Federal agencies can improve their mission performance, increase customer satisfaction and transform their operations. For more information, see <http://www.vsecorp.com>

**GSA IT Schedule** - The Information Technology (IT) Multiple Award Schedule (MAS) is an ID/IQ contract providing the full range of IT services. For more information, see <http://www.vsecorp.com>



*VSE Corporation  
2550 Huntington Avenue  
Alexandria, Virginia 22303-1499  
www.vsecorp.com email: info@vsecorp.com  
(703) 960-4600 1-800-455-4873*