**C5i Corporation** in Sterling, VA is a private company categorized under **Management Information Systems Consultant**. Our records show it was established in 2001 and incorporated in Virginia. Current estimates show this company has an **annual revenue** of **6,200,000** and employs a staff of approximately 100. Companies like C5i Corporation usually offer: Managment Consulting, Management Strategy Consulting, Organizational Management Consulting, Top Management Consulting and Performance Management Consulting. <http://bit.ly/kXp9qB>

**Shaun S. Amini** is the President & CEO of **C5i Corporation** and **C5i Federal, Inc.,** an **Information Technology Service Provider** to the ***Federal Civilian, Defense, Intelligence, and Commercial*** sectors.

Prior to C5i, Mr. Amini was the founding CEO of both **EYECAST Corporation** and **PublicNet** communications. EYECAST Corporation was a Video Content and Infrastructure service provider specializing in large-scale digital video acquisition and distribution. ***During his tenure at EYECAST, Mr. Amini raised over $36M from both angel and institutional investors and helped develop strategic and reseller relationship while leading several congressional lobbying efforts.*** PublicNet was a corporate Internet Service Provider and was successfully sold to **DigiNet Communications,** Inc. Mr. Amini has over 21 years experience and has worked for companies such as **MCI, Freddie Mac, Litton, CNA, Legent Corporation, Computer Associates, Axent Technologies (Symantec).** Mr. Amini has a bachelor of science in computer science and ***holds several patents in the area of security***. [**http://bit.ly/mPdYk9**](http://bit.ly/mPdYk9)

**March 3, 2011**: Assessment and Review **Conducted by C5i** **U.S. SECURITIES AND EXCHANGE COMMISSION**

**2010 Annual FISMA Executive Summary Report**

**(OIT): Thomas Bayer, Chief Information Officer, OffICe of Information Technology (OIT)**

[**http://www.sec-oig.gov/Reports/AuditsInspections/2011/489.pdf**](http://www.sec-oig.gov/Reports/AuditsInspections/2011/489.pdf)

**Background. FISMA, 44 U.S.C. § 3541, et seq., is a United States federal law enacted in 2002 as the Title III of the E-Government Act of 2002. The statute recognizes the importance of information security to the economic and national security interests of the United States. Further, the statute requires federal agencies to develop, document, and implement an agency-wide program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by other agencies, contractors, or other sources.**

**FISMA provides the framework for securing the Federal Government’s information technology. All agencies must implement the requirements of FISMA and report annually to OMB and Congress on the effectiveness of their information security and privacy programs. OMB uses this information to: (1) Help evaluate agency-specific and government-wide information security and privacy program performance; (2) Develop its annual security report to Congress; (3) Assist in improving and maintaining adequate agency performance; and (4) Assist in the development of the E-Government Scorecard under the President’s Management Agenda.**

**As part of its FISMA review, C5i also conducted reviews to examine the SEC’s continuous monitoring program and covering the SEC’s oversight of contractor held personally identifiable information. The results of these audits will be issued later, in separate OIG reports.**

**Objectives. The overall objective for the FISMA assessment was to independently evaluate and report on how the Commission has implemented its mandated information security requirements. Secondarily, the objective was to provide clarity regarding the OIG’s input and responses to the OMB.**

**Summary of Recommendations. We developed eight recommendations to address vulnerabilities identified in the current assessment. cont.**

**cont.**

**Specifically, we**

**(1) OIT should identify all exceptions to the Federal Desktop Core Configuration standards and submit them to National Institute of Standards and Technology within 90 days of the issuance date of this report.**

**(2) OIT should ensure justifications for deviations from Federal Desktop Core Configurations requirements are fully documented.**

**(3) OIT should:**

**3a. *Perform a thorough review and identify the universe of all Commission user accounts;***

**3b. *Once the universe has been identified, OIT should then identify all “active” and “inactive” user accounts and determine whether or not the account should be disabled; and***

**3c*. Take immediate action to disable the accounts of employees and contractors who no longer work at the Commission*.**

**(4) *OIT should review their policies and procedures for disabling accounts to ensure they are well-documented and thorough, and provide training to appropriate staff regarding account termination procedures*.**

**(5) OIT should complete the logical access integration of the HSPD-12 card program no later than December 2011, as it reported to OMB on December 31, 2010.**

**(6) OIT should conduct a full review and identify the universe of all users with elevated privileges.**

**(7) Based on the review results of recommendation 6, OIT should enforce or develop procedures to ensure:**

**7a. Only users whose job function require permanent elevated access have the needed privileges;**

**7b. Business justifications are fully documented; and**

**7c. *Elevated privileges are only issued for the finite amount of time needed to complete assigned task.***

**(8) *OIT should establish and maintain an accurate and current list of all users that have elevated privileges.***

**2010 Annual FISMA Executive Report March 3, 2011**

**Report No. 489**

**Page vii**

**Accessing SEC systems remotely can be performed in the following ways: Please see (\*\*APPENDIX V PAGE 40 \*\*)**

**Section 10: Status Agency Program to Oversee Contractor Systems**

**Background. Outside contractors play an integral role in the federal government operations, as well as in commercial enterprises. Contractors can provide a wide range of services from staff augmentation to technology system development, operation and maintenance. Contractors are subject to the same rules of conduct as employees of the organization they are brought in to support, and therefore must adhere to all policies and procedures. Contractor systems deployed in the federal government are subject to a full C&A prior to implementation and are also governed by policies and procedures of the agency for compliance with NIST, FISMA, and OMB guidance.**

**U.S. Securities and Exchange Commission Office of Inspector General Attn: Assistant Inspector General, Audits (Audit Request/Idea)**

**100 F Street, N.E. Washington D.C. 20549-2736**

**Tel. #: 202-551-6061 Fax #: 202-772-9265 Email:** [**oig@sec.gov**](mailto:oig@sec.gov)[**http://bit.ly/iEqLCw**](http://bit.ly/iEqLCw)

Intelligence

C5i’s Intelligence, Surveillance, and Reconnaissance (ISR) products and services are specifically focused on the Cyber Space. C5i’s breadth, depth and ability provides first responders, intelligence gatherers, decision-makers and **military personnel** on the front lines the tools necessary to act with speed and confidence. The combination of C5i’s knowledge and experience in the **Cyber Space sets our ISR capabilities** apart from the rest.

**C5i's Government Solutions** enable you to:

Safeguard the privacy of the public data entrusted to your agency

**Protect your mission-critical IT systems**

**Maintain continuity of operations**

Achieve compliance with IT security laws and regulations <http://www.c5i.com/>

Strike Force Interoperability Officer (SFIO) teams, consist of Navy officers and senior civil service project engineers with a strong technical pedigree in fleet operations using integrated and interoperable command, control, communications, computers, combat systems and intelligence **(C5I) systems aboard U.S. Navy ships**. <http://bit.ly/m8IJAy>