Cybersec INVESTMENTS

Capability Statement

Fernando Machado **800-960-8802**

Cybersec Investments LLC is a SDVOSB cybersecurity firm. We provide specialized services in the areas of compliance, vulnerability assessment management, computer network defense, and cybersecurity strategies.

SERVICES

- Security Assessments
- Vulnerability Management
- Risk Management Framework Implementation
- Security Audit & Information Assurance
- Certification & Accreditation
- Assessment & Authorization

DIFFERENTIATORS

- ✓ Candidate CMMC Third-Party Assessment Organization (C3PAO)
- ✓ CMMC Provisional Assessor
- ✓ Member – CMMC Standards Management Committee, Industry Working Group
- ✓ Working knowledge of NIST SP 800-37, NIST SP 800-53, and NIST SP 800-171
- ✓ Successful implementation, assessment, and monitoring of Risk Management Framework (RMF) controls

CORE COMPETENCIES

- Cybersecurity and information assurance services and solutions
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37: Risk Management Framework (RMF) implementation
- Preparation for Defense Security Service (DSS) Security Vulnerability Assessments (SVA)
- Continuous Monitoring (ConMon) solutions.

NAICS Codes

541512	Computer Systems Design Services
541519	Other Computer Related Services
541614	Process & Physical Distribution & Logistics
541618	Other Management Consulting Services

CERTIFICATIONS

- ISC2 Certified Information Systems Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified Information Systems Auditor (CISA)
- CompTIA Advanced Security Practitioner CE (CASP)
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Computer Hacking Forensic Investigator (CHFI)
- CompTIA Security+ CE
- Certified Scrum Master (CSM)

Service Disabled Veteran Owned Small Business SDVOSB cVE

ACTIVE CLEARANCE

Top Secret / Sensitive Compartmented Information (SCI)

CAGE Code: 8BL95 **DUNS:** 117056191

PAST PERFORMANCE

STG, Inc. (now SOSI) U.S. Army, Network Enterprise Command (NETCOM) under the Cyber Security Directorate (CSD) Contracts

- Routine audits, ensuring systems operated securely and information systems security management policies and procedures were implemented as defined in System Security Plans (SSP's).
- Completed RMF Assessment and Authorization (A&A) packages and worked directly with the Security Controls Assessor (SCA)-Army and provided final risk assessment to the SCA-Army.
- Conducted review of packages using the Enterprise Mission Assurance Support Service (eMASS) to automate the DIACAP and RMF process.
- Identified and remediated security-related risks of information systems.
- Reviewed Information Assurance Vulnerability Alerts (IAVA) and Information Assurance Vulnerability Management (IAVM) and Plan of Action and Milestones (POAM).
- Provided supervision on all aspects of work, including on the spot correction actions and training to peer.
- Conducted information system audits using E-Retina and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG's) / Security Readiness Reviews (SRR's).

Raytheon Missile Systems, U.S. Navy Contracts

- Analyzed and coordinated information assurance requirements for networked and standalone systems within environments of varying complexity levels.
- Created and maintained Certification and Accreditation (C&A) documentation. Ensured system security measures complied with multiple regulatory requirements, including National Industrial Security Program Operating Manual (NISPOM) and DoD RMF, accurately assessing the impact of modifications, changes, and vulnerabilities for each system, when applicable.
- Created and maintained all information assurance documentation, including SSP's, Security Profiles, and approvals for assigned areas.
- Performed Security Content Automation Protocol (SCAP) scans to discover known vulnerabilities and safely secure information systems.

L3Harris, U.S. Department of Defense Classified Contracts

- Performing assessment and authorization planning, testing, and validating activities in coordination with government customers.
- Conduct internal information technology system audits and risk assessments and report findings and recommendations for corrective actions to management.
- Execute first level responses and address reported or detected incidents.
- Safeguard information against unauthorized use, infiltration, exfiltration, modification, destruction, or disclosure of national security information.
- Support secure systems operations and maintenance.

Fernando Machado, President
fernando.machado@cybersecinvestments.com
1900 S Harbor City Blvd. Suite 328
Melbourne, FL 32901
https://www.cybersecinvestments.com

1-800-960-8802