CYBERSECURITY – INFORMATION SYSTEM SECURITY OFFICER

Requisition Number: 20-14

Job Title: Information System Security Officer (ISSO)

Career Level: Mid-Level

Location: Littleton, Colorado (On-site Position, Not Remote)

Relocation: Negotiable

Education Required: Bachelor's Degree in Computer Science, Information Systems Management, Information Technology, Cybersecurity, or other related degree. Equivalent experience and/or earned college credit will be taken into consideration.

Years of Experience: 5-8 years

Travel: Minimal

Job Description:

Our customers trust Oakman Aerospace, Inc. (OAI) to provide best-in-class security of all information technologies and systems. We do not take this responsibility lightly. At OAI, we know the reliability of our cybersecurity infrastructure is paramount in providing information and mission assurance to every customer, ultimately ensuring our continued growth and success.

We are hiring an experienced Information System Security Officer (ISSO) who regards Cybersecurity and Information Assurance (CS/IA) as seriously as we do. The ideal candidate will uphold a high degree of responsibility in ensuring both OAI and our customers are effectively protected.

U.S. Citizenship is required. *Equivalent work experience and/or relevant earned college credit (to be validated with transcripts) will be considered in lieu of a formal degree. This is not a remote position- ISSO will complete work on-site at OAI's Littleton, Colorado facilities.*

Responsibilities include, but are not limited to:

- The ISSO manages the Risk Management Framework program and ensures compliance to governing documents and security policies and assist in regulatory periodic assessments.
- Analyze and coordinate IA requirements for networked and standalone systems within environments of varying complexity levels.
- Create and maintain all IA documentation (e.g. System Security Plan, Security Controls Traceability Matrix, approvals, etc.) and submit required reporting.
- The ISSO will design, develop, and recommend security solutions for platforms with various operating systems.
- The ISSO conducts audits; and, oversees vulnerability scanning and system backups per the organization's Continuous Monitoring Plan and System Security Plan.
- Ensure system security measures comply with multiple regulatory requirements (e.g. DoD RMF), and accurately assess the impact of modifications, changes, and vulnerabilities for each system where needed.
- Coordinate their duties with selected Security, Information Technology, and Project Managers on a regular basis.
- The ISSO will conduct reviews and technical inspections to identify and mitigate potential security weaknesses, and ensure that all security features applied to a system are implemented and functional.
- Participate in interdepartmental projects and provide leadership as necessary.
- Interface with internal and external Security personnel, customers, management, and U.S. Government representatives where required.
- Perform other IA-related duties as assigned by management on an "as required" basis.
- Provide security training to all system users in accordance with the organization's training program.
- Conduct risk assessments and provide recommendations for secure implementation and compliance in accordance with government regulations and CS/IA guidelines.

- Assess and mitigate system security threats/risks throughout the program life cycle.
- Assist with the implementation of security procedures.
- Perform information system certification and accreditation planning, testing, assessing and liaison activities.
- Apply CS/IA standards, directives, guidance and policies to an architectural/risk based framework. Provide architectural/risk based analysis of CS/IA features and relate existing system to future needs and trends and requirements.
- Minimal business travel as needed.

Required Skills & Knowledge:

- Degree in Computer Science, Information Systems Management, Information Technology, Cybersecurity, or other related degree
- Information Technology certification and/or 8 years equivalent related experience (4 years Cybersecurity experience) will be considered in lieu of degree
- Experience with the following: self-inspections, security control assessments, training, log management systems, auditing, configuration management, and patching.
- Experience with the following: DoD 8500 series, NIST Special Publications (800-53, 800-37, etc.), Nessus, SCAP, Log360
- Knowledge in Windows and Linux operating systems
- U.S. Citizenship is required
- Currently have a DoD 8570.01-M IAM level I certified credentials (Security +, etc.) (or ability to obtain within 6 months of employment)

Desired Experience & Skills:

- Experience with the identification, development, and reporting of IA program performance metrics and oversight of appropriate IA policy, processes and procedures
- Experience in the execution and management of Information Systems (IS) incident response and administrative inquiries/investigations in collaboration with the Investigations department
- Experience working with customers, both internal and external in the development of Basis of Estimates (BOE's)
- Public speaking experience
- Experience in the oversight and execution of the Assessment & Authorization processes (Certification & Accreditation), as defined in RMF
- Experience in executing leadership and managerial duties (i.e. performance development, career coaching, mentoring, training, resource management, budget management, etc.)
- Experience interfacing with internal and external customers (i.e. AOs, DAOs, SCAs, Program Managers, etc.)

About OAI:

OAI is on a mission to advance the future of space through innovative and groundbreaking technologies that Enable Your Journey Through Space. Our employees are the foundation of OAI and our products and services reflect their vision of the future. Our team members come from a variety of backgrounds and experiences, and have an unwavering commitment to always do the right thing for OAI's customers, teammates, and stakeholders. They leverage their own skills and that of their peers to unlock the next solution that will revolutionize space. Our company culture is driven by this passion for disruption in the space industry, fosters employee growth and development, and promotes collaboration within our community.