JOB DESCRIPTION

JOB TITLE: INFORMATION SYSTEM SECURITY MANAGER (ISSM)

JOB CODE: **EXEMPT/NON-EXEMPT: EXEMPT**

REPORTS TO: Facility Security Officer **DEPT.: Security**

DEPT. APPROVAL: FSO **DATE: 06/04/2021**

MANAGER LEVEL: **EEO CODE:**

BRIEF POSITION SUMMARY:

Oversee the development, implementation and evaluation of the information system program for STS management, information system personnel, users and others as appropriate

DUTIES and RESPONSIBILITIES:

- Ensure systems are operated, maintained and disposed of in accordance with internal security policies and the system security plan
- Ensure that all users have the requisite security clearances, authorization need-to-know, and are aware of their security responsibilities before being granted access to IS
- Report all security-related incidents
- Initiate protective or corrective measures when security incident or vulnerability is discovered
- Develop and maintain a system security plan (SSP) and Certify to the CSA in writing that the STS systems security plan (SSP) is implemented for each authorized information systems, specified in the SSP; the specified security controls are in place and properly tested; and the information system continues to function as described in the SSP
- Conduct periodic reviews to ensure compliance with SSP
- Ensure configuration management for security-relevant IS software, hardware and firmware is maintained and documented
- Ensure system recovery processes are monitored to ensure security features and procedures are properly restored
- Ensure all IS security-related documentation is current and accessible to properly authorized individuals
- Formally notify the appropriate individuals when changes occur that might affect accreditation
- Ensure that system security requirements are addressed during all phases of the system life cycle
- Follow procedures for authorizing software, hardware and firmware use before implementation on the system
- Create/provide security education and awareness training to cleared employees

- Coordinate with the STS ITSPO so that Insider Threat Awareness is addressed in STS' information system security program
- Develop, document and monitor compliance of STS' information system security program in accordance with the CSA-provided guidelines for management, operational land technical controls
- Verify self-inspections are conducted at least every 12 months on STS's information systems that processes classified information, and that corrective actions are taking for all identified findings
- Brief users on their responsibilities with regard to information system security and verify that STS personnel are trained on the security restrictions and safeguards of the information system prior to access to an authorized information system
- Develop and maintain security documentation of the security authorization request to the CSA. Documentation may include:
    - SSPs
    - Security Assessment reports
    - Plans of Actions and Milestones
    - Risk assessments
    - Authorization decision letters
    - Contingency plans
    - Configuration management plans
    - System interconnection agreements

The ISSM may assign an Information Systems Security Officer (ISSO). If assigned, the ISSO will:

- Verify the implementation of STS' information system security program as delegated by the ISSM
- Ensure continuous monitoring strategies and verify corrective actions to the ISSM
- Conduct self-inspections and verify corrective actions to the ISSM

*The Company reserves the right to add or change duties at any time

EDUCATION, EXPERIENCE & QUALIFICATIONS:

- Must be a U.S. citizen
- Ability to obtain and maintain a U.S. Security Clearance/access approval at the appropriate IS level (requires U.S. Citizenship) (*Active Clearance Preferred*)
- Bachelor's degree and 6 or more years related secure information system experience, or any equivalent combination of education, training and experience in lieu of degree
- Working knowledge of system functions, security policies, technical security safeguards, and operational security measures
- Administrative knowledge of Microsoft operating systems
- Strong documentation skills
- Experience with LINUX variants such as CentOS is preferred
- Strong customer service skills
- Security+ certification is required, CISSP is preferred
- Working experience with RMF, ICD 503, CNSSI 1253, NIST SP 800-53/53A, NISPOM Chapter 8, DAAPM Manual
- Experience with DCSA tools such as eMASS, STIGs and SCAP
- Holds and able to maintain a valid U.S. Driver's license
- Must pass pre-placement drug screen and background investigation

PHYSICAL REQUIREMENTS:

- Must be able to sit/stand for extended periods – 9 hours minimum
- Physically able to handle items weighing up to 40lbs (unassisted)
- May be exposed to high level noise, dust, and vibration and chemical fumes (within OSHA limits)