Job Description
Information System Security Manager
Cyber Innovation Center

This position is for an **Information System Security Manager (ISSM) at Cyber Innovation Center (CIC) in Bossier City, LA and is responsible** for the Information Assurance (IA) program as stipulated by various US Government requirements including (but not limited to): National Industrial Security Operating Manual (NISPOM) and related documentation such as the Office of the Designated Approving Authority (ODAA) Process Manuals, Baseline Technical Security Configuration Standards as well as customer/contract specific Information Assurance (IA) regulations. Components of the IA program include Certification and Accreditation (C&A) activities (documentation preparation, system configuration/validation, certification testing, etc.), security sustainment activities (hardware change management, software change management, account management, media protection, user interface, file transfers, etc.), conducting self-inspections, audit trail review, and delivering information systems security education and awareness. This position manages the IA incident response program as well as interfaces with other IA team members, other security disciplines (industrial security, physical security, special programs security, etc.), program personnel and government security representatives.

Required Skills:

- Five or more years of systems and network security experience with a clear understanding of the challenges of information security.
- Applicant must possess and maintain Information Security professional certification commensurate with DoD 8570.1 IAM Level III requirements (CISM, CISSP or other).
- Existing & current SCI-DCID 6/4 Top Secret Clearance- US Citizenship required
- Experience with national security information system related security requirements (e.g. JAFAN, DCID, JSIG, ICD 503, RMF, DIACAP, NISPOM or DAAPM) to include technical computer/network system certification and auditing.
- Analytical and problem-solving abilities to identify and fix security risks.
- Excellent communication and presentation skills.
- Excellent team working skills to develop security solutions in collaboration with other information technology professionals.
- Ability to handle difficult people and/or situations in high pressure environments and make tough decisions.
- Self-motivated with strong communication skills (written and oral).
- Excellent time management skills.
- Must be flexible and work with limited supervision.

- Customer focused, adaptable and willing to work varying assignments.
- Working experience with operating systems such as Windows, UNIX, LINUX, etc.

Desired Skills:

- Experience developing Risk Management Framework (RMF) body of evidence artifacts.
- Experience managing Firewalls (Cisco, Barracuda, Juniper) and Vulnerability scanners (Nessus, OpenVAS, Retina).
- Experience with development and delivery of IA related briefings and training material.

Required Education:

Bachelor's Degree in either Computer Science, Information Systems Management, Information Technology, or other relevant degree. Eight years of relevant experience may substitute for Bachelor's degree requirement.

Work Requirements:

Hours: 8 a.m. to 5 p.m., Mon-Fri (typical).
Due to the nature of the business and depending on specific event schedules, the employee will be required to vary typical work hours. Occasional weekend work could be required.

Compensation:

Salary: Commensurate with ability and experience. Excellent employee benefits package.