

**Job Announcement**  
**Facility Security Officer/Insider Threat Program Senior Official**  
**Cyber Innovation Center**

This position is for a **Facility Security Officer (FSO)/Insider Threat Program Senior Official (ITPSO) at the Cyber Innovation Center (CIC) in Bossier City, LA** and is responsible to the CIC Senior Management Official for managing all aspects of the National Industrial Security Program (NISP) and its operating manual (NISPOM), and routine aspects of Department of Defense (DoD) personnel, physical, and industrial security programs to ensure compliance with government and company security policies and procedures.

**Job Description**

The FSO follows the NISPOM, all applicable Intelligence Community Directives, and other DoD regulations, to apply and manage an in-depth information security program that includes the protection of multiple levels of classification up to sensitive compartmented information (SCI). Primary responsibilities are to:

- Administer the CIC personnel security program by initiation and completion of SF86/Agency nomination packages and Continuous Vetting updates in National Background Investigation Services (NBIS), use of fingerprinting system/software and Secure Web Fingerprint Transmission (SWFT), preparation of visit authorization letters, use of the Defense Information Security System (DISS), and coordination with customer security representatives to process security clearance requirements.
- Manage the Insider Threat Program for cleared and uncleared staff including, but not limited to, the Insider Threat Working Group, initial insider threat awareness training, annual refreshers, and Insider Threat Awareness Month education
- Maintain applicable security documentation and files in accordance with the Defense Counterintelligence and Security Agency (DCSA) and the Office of the Director of National Intelligence.
- Update and maintain Facility Clearance records within the National Industrial Security System (NISS).
- Create, provide, and document all new employee security briefings, exit interviews, annual refresher training, and debriefing
- Investigate and report security violations and incidents to the appropriate Cognizant Security Office.
- Develop and maintain an effective “Inventory Management System” for management of classified systems, media and documents and prepare classified transmittals in accordance with NISPOM guidelines and requirements.
- Advise personnel of their reporting requirements, both personal/administrative and compliance/incident-related reports.
- Interpret government policies for the development and implementation of security plans and procedures and recommend corrective actions for violations.

- Maintain a working relationship with DCSA and other Federal agencies and each contract's security office for processing and maintaining employee clearances or suitability determinations.
- Create and update security plans, procedures, and instructions.
- Participate in the development and execution of security education programs.
- Manage daily security activities and enforce government and company security policies.
- Perform access control responsibilities including creating and managing badges and access cards as required.
- Maintain security oversight for DCSA Open Storage Areas and DoD sensitive compartmented information facilities.
- Conduct required self-inspections.
- Collaborate with Information Systems Security Manager and team regarding physical, personnel, and industrial security and insider threat as they relate to classified information systems and CMMC.
- Interface with program management to address security items specific to each program.
- Provide mentorship/training to Alternate Facility Security Officer
- Provide support and assistance to other CIC and subcontractor personnel at multiple locations.

**Required Skills:**

- Current SCI-DCID 6/4 Top Secret Clearance. US Citizenship required.
- Five years of experience in security field.
- Facility Security Officer training for Possessing Facilities in Center for Development of Security Excellence (CDSE) (must be completed within six months if selected).
- Practical knowledge of and experience with NBIS, DISS, e-APP, NISS, and SWFT.
- Previous industrial security experience and an in-depth knowledge of the NISPOM.
- Experience with personnel security, document, and visitor control.
- Experience in the contractor community in security management.
- Experience with insider threat/counterintelligence.
- Communicate effectively (written and oral) with all levels of staff and outside personnel.
- Self-starter able to take initiative within a fast paced, agile environment.
- Proficient with Microsoft applications: Excel, Word, PowerPoint.
- Well organized and confident to work independently but be a strong team player.
- Ability to effectively manage ambiguity and multi-task on a variety of initiatives.

**Desired Skills:**

- Three years of experience as Alternate FSO or FSO.
- Security certifications such as NCMS ISP or CDSE SPeD
- Completed Insider Threat Program Management Personnel Curriculum through CDSE
- COMSEC training.

**Required Education:**

Associate degree minimum; bachelor degree preferred.

**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. Occasional travel may be required.

**Compensation:**

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