SECURIFENSE

POSITION: Security Specialist
LOCATION: Pentagon
SECURITY CLEARANCE: Top Secret / SCI

Position Description:
Security Specialist will provide oversight of a DoD organization's security functions in their Pentagon secure facility. Responsibilities include, but are not limited to, administer, coordinate, and evaluate security programs that support the strategy, policies, and standards established for the physical safety of all visitors, employees, or customers to the organization's facilities and the security of property and assets.

Duties and Responsibilities

- Perform a wide range of administrative security activities associated with operating in a very sensitive and classified environment to include sensitive compartmented information (SCI) and Special Access Programs (SAP).
- Have a strong knowledge around DoD Instruction 5200.48 and National Industrial Security Program Operating Manual (NISPOM) Rule 32 CFR 117 and DoD security rules and regulations
- Assist in the functions of personnel security (PERSEC), physical security (PHYSEC), communication security (COMSEC), continuity of operations (COOP), information security/operations security (INFOSEC/OPSEC), industrial security (INDSEC), and general security administration (customer support) in accordance with:
    - DoD 5200.02
    - Intelligence Community Directive 704
    - DoDD 5200.08
    - DoDD 5200.01 DoD 5105.02
    - Intelligence Community Directive 705
    - DoDI 8523.01 and NSA Manual 3-16
    - DoD 5200.01 (DoD Information Security Program
    - DoD 5205.02 (DoD Operations Security Program) and DoDI 5220.22 and the National Industrial Security Program Operating Manual (NISPOM)
    - DoDM 5208.07 Volumes 1-4
- Provide general security functions and customer support, including, but not limited to:
    - Processing CAC & building access applications and visit authorization requests
    - Access control requests
    - Country and threat briefs
    - In/out processing of personnel (civilian, military, and contractor) indoctrinations/debriefings
    - Security record management
    - Courier card application processing
    - Computer/network account access requests
- Run queries of the DISS Information for Security database for clearance information, pass clearances, provide SCI indoctrination assistance, and update DISS records as necessary; provide guidance to R&E personnel as required concerning clearance information; process and accredit Sensitive Compartmented Information Facilities; certification of Temporary Secure Working Areas, Top Secret Closed Storage areas, Open Storage Secret areas and Closed Storage Secret areas.

- Provide guidance to R&E personnel on Classification and Declassification as necessary; compile annual reports (e.g., ISOO Standard Form 311 Report); and conduct Original Classification Authority/Derivative Classification training
- Conduct security assessments and audits to identify vulnerabilities and areas for improvement.
- Ensures that contract-specific SAP security requirements such as TEMPEST and Operations Security (OPSEC) are accomplished.
- Oversees an information management system for the SAP to facilitate the control of requisite information within the SAP.
- When designated by the SAPCO as GSSO/CPSO, may perform Special Access Program Personnel Security Official (SPO) functions.
- Manage access control systems, surveillance equipment and other security technologies to ensure proper functioning and effectiveness.
- Collaborate with internal departments, such as human resources and IT, to ensure compliance with security protocols and standards.
- Investigate incidents and violations, document findings and implement corrective actions.
- Maintain strong relationships with external partners, such as law enforcement agencies and security vendors, to enhance security capabilities.

Minimum Requirements

- TS Clearance w/ ability to obtain SCI access
- BS/BA degree in security management, criminal justice or a related field.
- In-depth knowledge of DISS and Scattered Castles
- 5+ years of current experience conducting security inspections/reviews, providing security management of facilities and equipment used in processing classified, SCI, and/or SAP material, accomplishing periodic reports, and overseeing security matters to include COMSEC, annual training, accreditation standards, and physical security requirements.
- Be required to complete the below list of security training classes in order to perform duties. If completed within the past five (5) years, may provide certificates of completion.
    - Personnel Security Management Course
    - Risk Management for DoD Security Programs Course
    - Intro to DOD Personnel Security Adjudications Course
    - NISP Self-Inspection Course
    - Derivative Classification
    - Identifying and Safeguarding Personally Identifiable Information (PII)
    - Cybersecurity Awareness Course
- In-depth knowledge of security technologies, incident management software and other security-related equipment, such as access control systems and CCTV surveillance.
- Demonstrated ability to develop and implement security policies, procedures and programs.
- Proficiency in security assessments, audits and investigations.
- Excellent leadership and management skills; able to lead and motivate a diverse security team.
- Attention to detail and a keen eye for identifying and mitigating security risks.
- Excellent communication and interpersonal skills to interact with individuals at all levels of an organization.
- Ability to handle sensitive and confidential information with discretion and integrity.
- Strong organizational, customer service and oral and written communication skills