

JOB ID: 09-057
LOCATION: DAHLGREN, VIRGINIA



INFORMATION ASSURANCE ANALYST

POSITION SUMMARY:

The successful candidate will act as a lead consultant, interfacing between our US Navy NSWC Dahlgren Division Integrated Warfare Systems Laboratory (IWSL) and SQQ-89 Anti-Surface Warfare Combat System (ASWCS) projects and our information assurance team throughout the DIACAP and Navy Afloat Platform Information Technology (PIT) certification and accreditation life cycle. The analyst will be actively engaged in analyzing and preparing security accreditation reporting packages for both the Navy's ODAA and RDAA. The analyst will join a growing team working on Certification & Accreditation packages for both the US Navy and US Marine Corps.

POSITION RESPONSIBILITIES:

- Perform system test and evaluation (ST&E) activities on a variety of hardware and software systems (Windows, UNIX and Cisco IOS) using the latest Navy-approved vulnerability scanning tools (eEye Retina, Nmap, Windows Production Gold Disk and DISA Security Readiness Review (SRR) scripts)
- Interview end users and collect data that will be critical for the development of certification and accreditation (C&A) packages
- Analyze collected data
- Write C&A documents per DIACAP and Navy Afloat PIT standards, including System Security Plans, Risk Assessment Plans, Plans of Actions and Milestones, Security Test and Evaluation Plans, and/or Contingency Plans
- Ability to perform basic system administration functions for both Windows and UNIX servers
- Ability to execute data collection software for capturing system configuration details
- Ability to perform basic database queries (Oracle et al.)

ESSENTIAL SKILLS AND EXPERIENCE:

- Bachelor's degree or equivalent combination of education and experience
- Possess at least a DoDI 8570.1-M IAM Level-II security certification (CISSP, GSLC, CISM, etc.) or have the ability to obtain certification within 90 days
- Four or more years of experience in network, host, data and/or application security in multiple operating system environments
- Experience working with IP networking, networking protocols and understanding of security related technologies including encryption, IPsec, PKI, VPNs, firewalls, proxy services, DNS, and access control lists

- Experience working with relevant operating system security (Windows, Solaris, Linux, etc.)
- Experience working with leading firewall, network scanning and intrusion detection products and authentication technologies
- Experience working with DoD (DITSCAP / DIACAP), NIST Special Publications, or Director of Central Intelligence Directives (DCIDs) C&A process methodology
- Possess or be able to obtain a SECRET security clearance

PREFERRED SKILLS AND EXPERIENCE:

- Bachelor's degree in computer science or related field
- Strong communication skills
- Strong analytical and problem solving skills to troubleshoot and resolve network/operating system security issues
- Experience working with federal regulations related to information security (FISMA, Computer Security Act, etc.) a plus
- Ability to perform and interpret vulnerability assessments
- Ability to balance and prioritize work