L·SQUARED Innovation Starts with Information

POSITION: SYSTEM SECURITY ENGINEER

POSITION DESCRIPTION: Job is in Princeton, NJ at the NOAA facility. Salary is negotiable.

System Security Engineer is responsible for conducting systems security analysis to include but is not limited to: Continuous Monitoring, Authorization and Accreditation (A&A), Security Categorization, Security Test and Evaluations (ST&E), System Security Plans (SSP), Security Assessment Reports (SAR), Contingency Plans (CP), Plan of Action and Milestones (POA&M), Vulnerability Assessment Reports (VAR) and development of complex information systems and architectures that comply with the technical reference model and meet assigned security requirements.

The nature of work involves complex information technology project management, tactical planning, coordination, control and critical decision-making. Requires technical experience related to work being performed. They will be involved in complex technical engineering design and technology architectural tasks. They will routinely interface with multiple internal and client staffs and management. This position has significant responsibility for the quality of all deliverables, prepares and performs final reviews on critical written communications documents and regularly makes presentations on program progress. They are expected to work independently. They must display excellent judgment and provide advanced application of tools and skills.

Additional tasks will include:

- Plan, execute, and document annual Contingency Plan training/test/exercise for the customer
- Develop a procedure for reviewing security logs and generating appropriate security metrics for reporting to System Owner (SO), Authorizing Official (AO), and ISSO (Information System Security Officer); train existing local staff to perform/execute
- Serve as the deputy ISSO
- Manage POA&Ms
- Respond to security calls as required
- Plan for the annual review of security documentation with the SO, AO, and ISSO
- Review security documents at least quarterly to ensure updates are made in a timely manner
- Assist the SO and ISSO in the planning and coordination of the annual certification of the system
- Assist the ISSO in providing control/process guidance and oversight of the Account Management tool
- Represents the company in meetings with key stakeholders and customers
- Aligns project deliverables with stakeholder organizational goals
- Provides their primary customer with the senior corporate point of contact and takes full responsibility to ensure that time, scope, and quality expectations are met

POSITION DUTIES:

1. Primary Duties

- Independently provides analysis, evaluation, and recommendations designed to promote economy, efficiency, and effectiveness in the security program;
- Reviews and evaluates programs and operations to determine adherence to policies and procedures;
- Keeps management fully informed concerning security issues;
- Assists external customers in developing, implementing, and assessing a security program based upon on requirements;
- Acts as primary liaison with management in all security matters;
- Evaluates security policy and provide recommendations to managers;
- Leads independent and objective evaluations and audits of the security policy implementation;
- Identifies risks; evaluates safeguards; ascertains compliance with security policies; evaluates efficiency and cost effectiveness of protective measures;
- Provides project management input to project

2. Secondary Duties

- Participate in security audits, risk analysis, vulnerability testing and security reviews
- Identify security issues and risks, and develop mitigation plans
- Leads the development and interpretation of security policies and procedures;
- Contributes to the development of enterprise-wide security strategy;
- Evaluates and recommends new and emerging security products and technologies;
- Translates security and technical requirements into business requirements;
- Contributes to the technical direction on all areas of the security architecture;
- Works with development teams to identify functional requirements that drive security;
- Develops strategies and architectures which support advanced security topics such as Vulnerability Lifecycle, Management, Identity Management, Intrusion Detection, Authentication, Authorization and Auditing, etc;
- Influences the selection of security related hardware and software product standards and the design of standard configurations; accountable for security centric, architectural road maps and principles.

Documentation/Reports:

- Document all work appropriately in coordination with customer requirements and contractual deliverables.
- Draft weekly status reports.
- Daily timekeeping both electronic and paper timesheets.
- Respond to email and voice messages within 24 hours during normal business hours.

POSITION QUALIFICATIONS/REQUIREMENTS:

Education/Experience:

- Be a United States citizen or legal resident.
- Hold a US Government security clearance/access.
- Bachelor’s Degree and 5+ years of relevant experience

- CISSP certification or equivalent required.
- 1-3 years experience with NIST Special Publications.
- 1-3 years of experience in a scientific computing environment.
- Familiarization with FISM, NIST, DOC and NOAA security policies and procedures.
- Applicant must have general knowledge with heterogeneous computing environments connected to the Internet including working knowledge of ports, protocols, and services.
- Applicant must be able to travel
- Experience/skills in setting priorities and managing multiple tasks simultaneously
- Experience in supporting systems at field sites.
- Excellent written and verbal communication skills.

To apply, please send resume to info@lsquared.com