OVERVIEW

HOURS OF WORK: 4/10’s, 7am-6pm, M-Th

The ideal candidate will have the ability to work collaboratively with other units and departments to optimize effectiveness of the District/SNWA cyber security program; be able to analyze policy, trends, and intelligence to better understand how a cyber security threat actor may think or act, using deductive reasoning and problem-solving skills to develop appropriate countermeasures. Proficiency in the Unix operating system, Windows Powershell, and Penetration Testing is desired. Experience with web services development, DevSecOps, secure coding standards and Agile/Scrum development processes is desired.

Roles and Responsibilities
Under general supervision, performs complex and highly responsible duties in implementing, maintaining, evaluating and enhancing the District/SNWA cyber security protection framework including security architectures, policies, standards and systems to safeguard the integrity and confidentiality of information assets and the availability and reliability of systems operations; participates in activities to ensure compliance with PCI security standards; and performs related duties as assigned.

Education and Qualifications
Knowledge of:
Principles, practices and methods of cyber-security infrastructure and vulnerability management; Cyber Security and Information Protection and Privacy principles and practices; evolving sources of security threats and vulnerabilities; on-line systems security products and methodologies, applicable to both the enterprise infrastructure and its applications and data management systems; preventative security controls in general industry use including firewalls, IDS/IPS, VPN and others; common security management frameworks such as NIST, SANS Twenty Critical Security Controls and other cyber security standards; PCI compliance requirements and standards; principles, practices and techniques of information technology
management; the software development life cycle; operating system architectures, characteristics, components, uses and limitations applicable to the District information technology environment; network architectures and theory and principles of secure network design, integration, configuration and management; principles and methods of enterprise level data management and data storage solutions; troubleshooting principles and practices applicable to areas of responsibility; customer relationship management and internal consulting concepts and practices; systems integration and optimization design concepts and techniques particularly as applicable to areas of assigned responsibility; principles of effective teamwork.

Ability to:
Participate in development, administration and enhancement of a comprehensive cyber security protection framework including policies, standards and guidelines; work collaboratively with other IT units and departments to optimize effectiveness of the District/SNWA cyber security program; assess specific cyber security requirements, define options, recommend appropriate courses of action, develop cost estimates and procurement packages in support of cyber security management, preventive maintenance and mission critical systems and equipment; analyze policy, trends, and intelligence to better understand how a cyber security threat actor may think or act, using deductive reasoning and problem solving skills to develop appropriate countermeasures; apply critical thinking skills to isolate problem causes, perform root cause analysis and formulate solutions and workarounds, analyze cyber security management problems and alternatives, identify potential technical solutions and develop sound conclusions and recommendations; prepare clear, concise and accurate reports and other materials; communicate clearly and effectively to diverse audiences of technical and non-technical personnel, orally and in writing; exercise sound independent judgment within policies, standards and general guidelines; use tact and diplomacy when dealing with sensitive, complex and/or confidential issues; establish and maintain highly effective customer-focused working relationships with all levels of management, employees, consultants, contractors, vendors and others encountered in the course of work.

Training and Experience:
A typical way of obtaining the knowledge, skills and abilities outlined above is graduation from a four-year college or university with major coursework in computer science, information systems or a closely related field; and five years of progressively responsible professional information technology experience involving network/systems infrastructure administration and security; or an equivalent combination of training and experience. Experience in a government or public utility setting is highly desirable.

Licenses; Certificates; Special Requirements:
- A valid Nevada driver's license and ability to maintain insurability under the District's Vehicle Insurance Policy may be required for certain assignments.
- Certification as a Certified Information Systems Security Professional (CISSP), current CompTIA Security+ certification or comparable certifications with at least four years of comparable experience is required.

PHYSICAL AND MENTAL DEMANDS
The physical and mental demands described here are representative of those that must be met by employees to successfully perform the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

**Physical Demands**
While performing the duties of this class, employees are regularly required to sit; talk or hear, in person and by telephone; use hands to finger, handle, feel or operate computers and other standard office equipment; and reach with hands and arms. Employees are frequently required to walk and stand.

Specific vision abilities required by this job include close vision and the ability to adjust focus.

**Mental Demands**
While performing the duties of this class, employees are regularly required to use written and oral communication skills; read and interpret data, information and documents; analyze and solve highly complex and ambiguous problems; observe and interpret people, conditions and situations; learn and apply new information or skills; perform highly detailed work under changing, intensive deadlines on multiple concurrent tasks; and interact with all levels of District/SNWA managers and staff, IT staff, vendors, contractors, representatives of other governmental agencies including Homeland Security and the FBI and others encountered in the course of work.

**How to Apply**
Go to: [https://www.lvvwd.com/jobs/jobs.html](https://www.lvvwd.com/jobs/jobs.html)
Click “Job Openings”
Search for “Information Security & Compliance Analyst.”

For any questions regarding this announcement, please contact Jaclyn Lombardo at Jaclyn.Lombardo@lvwvd.com.