DATE: November 14, 2018

POSTING #: 290908

POSITION: Information Security Supervisor

SALARY RANGE: $102,041 - $165,081

DEPARTMENT: Technical Services

LOCATION: Anadarko / Moore

This position could be located at our Headquarters in Anadarko or at our satellite office in Moore, OK

Applications will be accepted until position is filled – Apply on-line at www.wfec.com

SUMMARY: Under the general supervision of the Manager, Technical Services, the Information Security Supervisor provides leadership, direction, and support for the Information Security staff. In addition, the incumbent plans, schedules, and coordinates group activities related to troubleshooting, installation, and maintenance on equipment and software systems related to electronic access control and monitoring. The Information Security Supervisor ensures the stability and integrity of in-house electronic access control and monitoring systems. In addition, the incumbent performs change management and configuration activities, security controls testing, system baseline activities, vulnerability testing and analysis, and network traffic analysis to ensure system reliability and security. The incumbent participates in in-house, regulatory, and industry teams including working groups, committees, incident response teams, and business continuity teams as required. Also, the incumbent participates in exercises that test policies, procedures, and skills which are required by business and critical operations. The incumbent responds to anomalous events that will require analysis, and will have to synthesize and correlate complex events to ensure operational security. The incumbent also maintains hands-on technical skills to assure a current knowledge of technologies used.

SUPERVISORY RESPONSIBILITIES: Senior Information Security Analysts, Information Security Analysts

ESSENTIAL DUTIES AND RESPONSIBILITIES: Include the following; other duties may be assigned. Provides leadership, direction, and support for the Information Security staff. Plans, schedules, and coordinates group activities related to troubleshooting, installation, and maintenance on equipment and software systems related to electronic access control and monitoring. Ensures the stability and integrity of in-house electronic access control and monitoring systems which may include SEIM devices, IDS sensors, IPS, data diodes, firewalls, switches, routers, application white listing, network anomaly detection devices, log retention systems, log forwarding systems, network monitoring systems, and analytics software used in the monitoring of critical cyber assets associated with the operation of multiple departments. Performs change management and configuration activities, security controls testing, system baseline activities, vulnerability testing and analysis, and network traffic analysis to ensure system reliability and security. Installs, troubleshoots, and maintains hardware and software systems related to electronic access control and monitoring systems. Reviews logs, configurations, rule sets, user accounts, account groups, and network traffic for adherence to policy/procedure. Responds to anomalous events that will require analysis and will have to synthesize and correlate complex events to ensure operational security. Tests and implements IDS/IPS rule sets and signatures. Conducts security controls testing after significant changes to cyber assets to ensure proper security posture to meet regulatory guidelines. Monitors cyber assets and critical infrastructure to ensure system up-time. Engages in change/configuration management activities for cyber assets. Performs network traffic analysis when anomalous traffic needs to be investigated. Assists in conducting incident response and forensic investigations. Conducts vulnerability testing, analysis, and mitigation for cyber assets. Analyzes network infrastructure rule sets manually and uses software tools to ensure proper security posture for compliance. Writes reports and briefings related to specific information security issues. Tickets and tracks operational issues related to the security posture of cyber assets which are in scope for this group. Conducts research on network products, services, protocols, and standards to remain abreast of developments in the information security industry.

The incumbent participates in exercises that test policies, procedures, and skills which are required by business and critical operations. Participates in in-house, regulatory, and industry teams including working groups, committees, incident response teams, and business continuity teams as required. Ensures training and development activities so that staff remains current and knowledgeable on technical changes and updates. Provides information for the annual department budget. Prepares staff performance reviews, training and development plans, and coaching and performance feedback.

COMPETENCIES: To perform the job successfully, an individual should demonstrate the following competencies:

Leadership and Managing People: Includes staff in planning, decision-making, facilitating and process improvement; Takes responsibility for subordinates' activities; Provides regular performance feedback; Develops subordinates' skills and encourages growth; Continually works to improve supervisory skills; Inspires and motivates others to perform well; Accepts feedback from others; Gives appropriate recognition to others; Delegates work assignments; Matches the responsibility to the person; Gives authority to work independently; Sets expectations and monitors delegated activities; Provides recognition for results.

Judgment/Problem Solving: Displays willingness to make decisions; Exhibits sound and accurate judgment; Supports and explains reasoning for decisions; Includes appropriate people in decision-making process; Makes timely decisions; Identifies and resolves problems in a timely manner; Gathers and analyzes information skillfully; Develops alternative solutions; Works well in group problem solving situations; Uses reason even when dealing with emotional topics.

Planning/Organizing: Prioritizes and plans work activities; Uses time efficiently; Plans for future resources; Sets goals and objectives; Effectively organizes or schedules people and their tasks; Develops realistic work plans.

Oral and Written Communication: Speaks clearly and persuasively in positive or negative situations; Listens and gets clarification; Responds well to questions; Participates in meetings; Writes clearly and informatively; Varies writing style to meet needs; Presents numerical data effectively; Able to read and interpret written information.

Interpersonal Skills: Focuses on solving conflict, not blaming; Maintains confidentiality; Listens to others without interrupting; Keeps emotions under control; Remains open to others' ideas and tries new things.

Organizational Support: Follows policies and procedures; Completes administrative tasks correctly and on time; Supports organization's goals and values.

Safety and Security: Observes safety and security procedures; Determines appropriate action beyond guidelines; Reports potentially unsafe conditions.

Diversity: Demonstrates knowledge of EEO policy; Shows respect and sensitivity for cultural differences; Promotes a harassment-free environment; Builds a diverse workforce.

Customer Service: Manages difficult or emotional customer situations; Responds promptly to customer needs; Solicits customer feedback to improve service; Responds to requests for service and assistance; Meets commitments to customers.

Cost Consciousness: Works within approved budget; Develops and implements cost saving measures; Conserves organizational resources.

QUALIFICATIONS: To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the education, experience, knowledge, skills, abilities, and behaviors required of this position.

Education and Experience: A Bachelor's degree in a related field and ten (10) years of directly related experience in information security, digital networking, computing, or telecommunications is required. Extensive knowledge of TCP/IP, Cisco routing and switching, proven experience with Cisco ASA firewall and VPN appliances is required. Industry specific certifications may be substituted for experience at the rate of one (1) year of experience for each certification. Directly related experience may be substituted for education at the rate of two (2) years of experience for one (1) year of education.

Language Skills: Ability to read, analyze, and interpret general business periodicals, professional journals, technical procedures, or governmental regulations. Ability to write reports, business correspondence, and procedure manuals. Ability to effectively present information and respond to questions from groups of employees, managers, clients, customers, and the general public.

Mathematical Skills: Ability to work with mathematical concepts such as probability and statistical inference, and fundamentals of plane and solid geometry, trigonometry, calculus and differential equations. Ability to apply concepts such as fractions, percentages, ratios, and proportions to practical situations.

Reasoning Ability: Ability to solve practical problems and deal with a variety of concrete variables in situations where only limited standardization exists. Ability to interpret a variety of instructions furnished in written, oral, diagram, or schedule form.

Computer Skills: In addition to the qualifications listed above, knowledge and experience using Microsoft Office products is required.

CERTIFICATES, LICENSES, REGISTRATIONS: Requires a current driver's license. Must hold a CISSP in good standing or be able to achieve CISSP certification within 12 months. CCNA, CCNP, Comptia Network +, Comptia Security +, GIAC, CEH, or Engineer level Operating System certifications are desirable.

WORK SCHEDULE REQUIREMENTS: Normally works a weekday schedule, but may be required to work evenings, holidays, or weekends. May be required to travel on short notice. On-call nights and weekends will be required for response to anomalous issues.

PHYSICAL DEMANDS: The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. While performing the duties of this job, the employee is regularly required to sit and talk or hear. The employee is frequently required to use hands to finger, handle, or feel and reach with hands and arms. The employee is occasionally required to stand and walk. The employee must occasionally lift and/or move up to 50 pounds. Specific vision abilities required by this job include close vision, distance vision and color vision.

WORK ENVIRONMENT: The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. While performing the duties of this job, the employee will be subject to moderate outdoor weather conditions. The noise level in the work environment is usually quiet.

MUST MEET ALL PHYSICAL AND ENVIRONMENTAL REQUIREMENTS

WFEC IS AN EQUAL OPPORTUNITY PROVIDER AND EMPLOYER
MINORITIES, FEMALES, DISABILITY, AND
VETS ARE ENCOURAGED TO APPLY
EOE/AA/M/F/DISABILITY/VETS