PUBLIC UTILITY COMMISSION OF TEXAS
JOB DESCRIPTION

Classified Title:	Cybersecurity Analyst I-II	**Class Code:**	0319, 0320
Working Title:	Cybersecurity Analyst	**Salary Group:**	B23, B25
Division:	Agency Operations	**FLSA:**	Exempt
Supervisor:	IT Director	**Date:**	10/03/23

GENERAL DESCRIPTION:

Perform moderately to complex (journey-level) information security and cybersecurity analysis work involving planning, implementing, and monitoring security measures for the protection of information systems and infrastructure. Work includes protecting cybersecurity assets and delivering cybersecurity incident detection, incident response, threat assessment, cyber intelligence, software security, and vulnerability assessment services. Work under general supervision, with moderate to limited latitude for the use of initiative and independent judgement.

ESSENTIAL FUNCTIONS:

- Perform the design, automation, and deployment of security applications and infrastructure program activities.
- Oversee and implement computer system security plans with PUC staff.
- Develop and/or coordinate the development of agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.
- Develop, recommend, and implement plans to safeguard computer configurations and data files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Develop information technology disaster recovery and business continuity planning for the PUC technology infrastructure. Advises management and users regarding security configurations and procedures.
- Perform and review technical risk assessments; reviews of new and existing applications and systems, including data center physical security and environment; and reviews of account permissions, computer data access needs, security violations, and programming changes.
- Modify and monitor computer configuration and data files to incorporate new software and virus protection systems, correct errors, or change individual access status.
- Design and plan deployment of continuous automated security compliance capabilities.
- Monitor and evaluate systems and procedures to protect data systems and databases from unauthorized access.
- Research, evaluate, and recommend systems and procedures for the prevention, detection, containment, and correction of data security breaches.
- Train users and promote security awareness to ensure systems security and to improve application, server, and network efficiency.
- Serve as a primary backup to the agency DCS Customer Representative.
- Assist in resolving performance issues relating to the State Data Center and the PUC network.
- Attend work regularly and observe approved work hours in accordance with agency leave and attendance policies.
- Demonstrate a spirit of teamwork, offering positive and constructive ideas, encouragement, support to other members of the staff and team, and respond professionally to constructive feedback from others, while upholding the PUC's mission and core values.

- Adhere to all agency personnel policies and division procedures and perform other work as assigned.

REQUIRED MINIMUM QUALIFICATIONS:

- Cybersecurity Analyst I: Undergraduate degree from an accredited college or University **and** a minimum of one (1) year experience working in the IT security industry.
- Cybersecurity Analyst II: Undergraduate degree from an accredited college or University **and** a minimum of two (2) years' experience working in the IT security industry.
- Additional relevant experience may be substituted for education on a year-for-year basis.

PREFERRED QUALIFICATIONS:

- Undergraduate degree in information technology, computer information systems, computer science, cybersecurity, or management information systems.
- Knowledge of the regulatory processes and procedures of PUC.
- Experience working with state IT regulatory issues and processes.
- Experience and training in analyzing, recommending, developing, and implementing cogent enterprise-wide policies, standards, and guidelines.
- Have or working towards obtaining a Certified Information Systems Security Professional (CISSP) or similar certification.

KNOWLEDGE, SKILLS AND ABILITIES:

Must possess required knowledge, skills, abilities, and experience and be able to explain and demonstrate, with or without accommodations, that the essential functions of the job can be performed.

- Knowledge of state and federal laws related to the administrative and operational functions of a state agency; of public administration techniques; and of IT security tools, processes, and techniques.
- Strong background in IT support and operations.
- Excellent problem-solving skills and ability to drive IT solutions and foster resolution.
- Exceptional communication and leadership skills.
- Ability to manage third-party vendor engagements, including evaluation and assessment.
- Ability to gather, assemble, correlate, and analyze facts; to devise solutions to problems; to prepare reports; to develop, evaluate, and interpret policies and procedures; and to communicate effectively.
- Ability to maintain effective working relationships within and outside the agency.
- Ability to attend work regularly and adhere to approved work schedule.

TELECOMMUTING ELIGIBILITY:

- This position is eligible for telecommuting up to three (3) days a week but may require team members to come into the office for scheduled meetings, and there may be unscheduled requests with appropriate notice for any PUC business need.
- If approved to telecommute, must have a secure workspace with reliable Internet service to perform duties, ability to maintain a reliable consistent work schedule and be available for weekly meetings and group collaboration via Microsoft Teams and other applications during regular business hours.

PHYSICAL AND COGNITIVE REQUIREMENTS AND WORKING CONDITIONS:

The physical and cognitive 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 will be made if needed to enable individuals with disabilities to perform the essential functions.

This position primarily performs sedentary office work. It requires extensive use of computer, copiers, printers, telephone and requires communication with staff and the public. This position also requires cognitive abilities consistent with the essential functions and with the knowledge, skills and abilities; requiring the ability to learn, recall, and apply practices and policies. It requires the stamina to maintain attention to detail despite interruptions.

Work is performed in a standard office environment or secure telework space and requires:

- Regular and punctual attendance.
- Frequent use of personal computer, copiers, printers and telephones.
- Frequent sitting.
- Frequent work under deadlines, as a team member, and in direct contact with others.
- Frequent moving and lifting objects up to 10 pounds.