**TEXAS DEPARTMENT OF LICENSING & REGULATION**
**920 Colorado, 7th Floor**
**Austin, Texas 78701**
**(512) 463-2476, Fax (512) 475-3377**
**Human.Resources@tdlr.texas.gov**

# JOB POSTING

## Information Technology/ IT Security

**Chief Information Security Officer**
**Cybersecurity Officer**
**$120,000- $130,000 annually**
**$10,000- $10833.34 monthly**

**Posting No: 1205-23** **Opening Date: 12/22/22**

**Group: B30**
Position: 22

**Closing Date at 5PM: UNTIL FILLED**

**Job Description**

The Chief Information Security Officer is selected by and responsible to the Senior Deputy Executive Director and performs highly advanced and supervisory cybersecurity analysis work providing direction and guidance in strategic operations and planning. Primary job responsibilities include performing as the agency's designated Information Security Officer (ISO); overseeing cybersecurity programs and environments; the prevention, detection and remediation of cybersecurity threats and intrusions; and developing cybersecurity policies and monitoring protocols. Work also involves leading the development of a security plan, with an emphasis on technical infrastructure and long-term risk mitigation. Also responsible for staff training and supervision. Work is performed under minimal supervision with extensive latitude for the use of initiative and independent judgment.

**Essential Duties**

- Directs and/or performs the design and deployment of cybersecurity infrastructure and protects critical infrastructure service.
- Oversees the day-to-day activities of the Information Security Division and its staff. Develops performance standards and position descriptions; plans, assigns and supervises the work of section staff; provides guidance, mentoring and coaching of Information Security Team to their highest potential; recommends section personnel actions; and ensures accurate and timely appraisals and meaningful training and developmental opportunities for each employee under direct supervision.
- Oversees cybersecurity management initiatives to assist the Department in meeting its goals and objectives. Supervises, assists and advises staff in security solutions and resolution of security problems.
- Develops and/or coordinates the development of agency policies for encryption of data transmissions and the erection of firewalls to conceal information as it is being transmitted and to eliminate tainted digital transfers.
- Develops, recommends, and implements appropriate safeguards to ensure system resiliency, protecting against accidental or unauthorized modification, destruction, or disclosure.
- Confers with users regarding computer data access needs, security violations, and programming changes.
- Monitors and modifies computer files to incorporate new software and virus protection systems, correct errors, or change individual access status.
- Oversees detection activities and leads the response to internal and external cybersecurity threats and vulnerabilities.
- Oversees the initiation, implementation, and development of incident response plans and recovery programs; the review of intrusion and misuse detection reports; and the delivery of guidance for corrective action.
- Maintains knowledge of and ensures compliance with applicable federal, state, agency and department policies, procedures, rules and regulations, including changes in legislation and accreditation standards that affect cybersecurity.
- Responsible for the development, review and implementation of the agency's cybersecurity plans, policies, guidelines, standards and procedures.

- Acts as liaison to the Software Development Services Section to assist with securing agency assets.
- Directs, and/or conducts security audits, assessments reviews and security risk assessments to identify gaps in compliance with agency and State of Texas policies and procedures and makes recommendations for security improvements in existing applications, network and systems.
- Coordinates responses to cybersecurity audits and other cybersecurity assessments.
- Develops and provides cybersecurity awareness training to all agency employees, contractors and users; and facilitates cyber preparedness exercises. Advises and trains management and users regarding security procedures and security violations. Monitors the effectiveness of the training and reports compliance issues to management or administrators.
- Provides innovation, management, and successful leadership in assisting the agency in achieving its long-term cybersecurity goals.
- Directs and/or conducts research related to cybersecurity trends and technology; and evaluates cybersecurity trends, tools, and techniques for potential application to infrastructure and research areas.
- Monitors, evaluates and maintains internal control systems and processes to ensure appropriate access levels are maintained and to protect agency systems and data from unauthorized access, modification, disclosure and/or destruction.
- Responsible for ensuring all software and related components are evaluated on regular basis ensuring compliance with all applicable and pertinent standards.
- Develops and maintains agency incident response capability. Participates in the agency's disaster recovery and business continuity planning; Coordinates with the Disaster Recovery / Business Continuity Plan (DR/BCP) representative.
- Researches, reviews, and evaluates technical developments in information security software and/or hardware, and makes purchasing recommendations to management, including the evaluation and procurement of forensics tools; assists with the writing of Request for Offer (RFO), Request for Information (RFI), and Request for Production (RFP) for information systems security technical products and services.
- Represents the agency at business meetings, hearings, trials, legislative sessions, conferences, and seminars or on boards, panels, and committees.
- Maintains professional and technical knowledge by attending education workshops, reviewing professional publications, establishing personal networks, and partnerships and recommends implementation of new technologies.
- Complies with Division and/or Agency training requirements.
- Demonstrates a spirit of teamwork, offering positive and constructive ideas, encouragement and support to other members of the staff and team, while upholding the agency's core values.
- Keeps management appropriately informed of ongoing activity and critical matters affecting the operation and well-being of the agency.
- Adheres to all TDLR Personnel Policies and performs other duties as assigned.

**Minimum Requirements**

Six (6) years' full-time experience in cybersecurity analysis work, with emphasis on security operations, incident management, intrusion detection, firewall deployment, and security event analysis OR four (4) years' experience as an information security analyst in a technical or supervisory role required. Three (3) years management, team lead, or supervisory experience in leading a technology team, preferably in information security, required. The experience requirements may run concurrently. Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) or equivalent certification preferred or ability to qualify for and acquire within one year of hire required.

Graduation from an accredited four-year college or university with major coursework in cybersecurity, information technology security, management information systems, or a related field is preferred.

**Preferred Qualifications:**

**Experience in:**

- Implementing National Institute of Standards and Technologies (NIST) Information Cybersecurity Framework (NIS CSF).
- Implementing Texas Administrative Code (TAC) 202.

- Cybersecurity program development, analyzing security controls, and developing solutions in compliance with the NIST Cybersecurity Framework and industry best practices.
- Developing and establishing security controls, auditing/monitoring compliance with established security controls and standards.
- Developing/updating information security documentation such as System Security Plans (SSP), Security Risk Assessment Reports (SAR), test and evaluation reports, security policies, contingency plans, Plan of Action and Milestones (POAM), and Incident Response plans.
- Conducting vulnerability assessments, evaluating exploitation, and performing or conducting remediation of system, network, and web application vulnerabilities.
- Assessing information security requirements, conducting research, and making recommendations for the design and implementation of solutions/tools to meet information security and all applicable compliance requirements.
- Providing direct guidance and cybersecurity best practices for managing the installation and integration of system fixes, updates, and security enhancements.
- Evaluating operational practices, including security awareness, incident response/management, disaster recovery, access management, auditing and logging, policy and procedure development, and network security management.

*Veterans, Reservists or Guardsmen with an MOS or additional duties that fall in the fields of 17C- Cyber Operations Specialist, 0651- Cyber Network Operator, 14NX-IntelligenceTechnology, CT- Cryptologic Technician or other related fields pertaining to the minimum experience requirements may meet the minimum qualifications for this position and are highly encouraged to apply.* **Additional Military Crosswalk information can be accessed at:**
http://www.hr.sao.texas.gov/Compensation/MilitaryCrosswalk/MOSC_InformationTechnology.pdf

**Remarks**

**The successful will have:** Knowledge of the limitations and capabilities of computer systems and technology; of operational support of networks, operating systems, Internet technologies, databases, and security infrastructure; and of information security controls, practices, procedures, and regulations. Knowledge of concepts and techniques for enterprise risk management, audits, and risk assessments; of security requirements and evaluation mechanism for security of cloud-based services; and, of incident response program practices and procedures. Skill in the operation of computers and applicable software and in configuring, deploying, and monitoring security infrastructure. Ability to resolve complex security issues in diverse and decentralized environments, to communicate effectively, and to train others. Ability to implement and act as an advocate for security best practices and security awareness; and, to plan, develop, monitor and maintain information technology security processes and controls.

Applications may be downloaded from TDLR's website https://www.tdlr.texas.gov/employ.htm. E-mail or fax applications to: TDLR, Human Resources Office, P.O. Box 12157, Austin Texas 78711, Fax (512) 475-3377. E-mail Human.Resources@tdlr.texas.gov. **Resumes will not be accepted in lieu of State Applications. Applications not completely filled out may be rejected. Only typed applications will be considered.**

*This job is not covered by the Fair Labor Standards Act (FLSA).*
***TDLR IS AN EQUAL EMPLOYMENT OPPORTUNITY EMPLOYER***
*TDLR provides a total compensation package that enables us to attract, motivate, and retain highly skilled and talented employees, including a merit system, full use of salary ranges, performance awards, retention and recruitment bonuses.*
*TDLR participates in E-Verify and will provide the Social Security Administration (SSA) and, if necessary, the Department of Homeland Security (DHS), with information from each new employee's Form I-9 to confirm work authorization.*
*In compliance with the Americans with Disabilities Act (ADA), TDLR will provide reasonable accommodation during the hiring and selection process for individuals with a disability. If you need assistance completing the application, contact TDLR Human Resources at 512-463-7184. If you are contacted for an interview and need accommodation to participate in the interview process, please notify the person scheduling the interview.*