DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
STATE AGENCY JOB VACANCY NOTICE

Opening Date: Immediately **Number of Openings:** 1 **Classification:** Exempt **Closing Date:** 01/29/2025 **Location:** Austin (Some remote work possible)	**Posting Number:** SML-393 **Duration of Job:** Regular Full Time **Group/Class #:** B27/0321 **Salary*:** B27 $7,016 min - $11,864 max *Commensurate with qualifications and Experience	**Military Specialty Codes:** **Army** – 17C, 25D; **Navy** – 183X; **Coast Guard** – CYB10, CYB11, CYB12; **Marine** – 0605; **Air Force** – 1B4X1, 1D7X1, 3D0X2; **Space Force** – 514A, 5C0X1D, 5C0X1N, 5C0X1S

Benefits Offered: Comprehensive healthcare options, State of Texas retirement plan, paid vacation/holidays, Employee Assistance Program, Training/Employee Development Program, and more.

Additional information on the SAO Military Crosswalk is available here: Military Crosswalk for Occupational Category - Information Technology

JOB TITLE: Cybersecurity Analyst III – (Executive)

JOB DESCRIPTION: Performs highly complex (senior-level) information security and cybersecurity analysis work involving planning, implementing, and monitoring security measures to protect information and information systems against accidental or unauthorized modification, destruction, or disclosure, and to assure their confidentiality, integrity, and availability. Work also includes protecting cybersecurity assets and delivering cybersecurity incident detection, incident response, threat assessment, cyber intelligence, software security, and vulnerability assessment services. May guide others. Works under limited supervision, with considerable latitude for initiative and independent judgment.

EXAMPLES OF WORK PERFORMED:

- Performs technical risk assessments to identify and prioritize potential cybersecurity and privacy risks to information systems.
- Performs cybersecurity incident response activities.
- Monitors and analyzes cybersecurity alerts from cybersecurity tools, network devices, and information systems.
- Monitors and reviews new and existing systems' account permissions, data access needs, security violations, programming changes, and physical and environmental security to protect them from unauthorized access.
- Implements continuous automated security compliance capabilities.
- Develops, recommends, and participates in the implementation of plans to safeguard system configurations and data against accidental or unauthorized modification, destruction, or disclosure.
- Conducts cybersecurity awareness training for users to promote a secure culture.
- Develops and distributes educational materials on cybersecurity best practices and emerging threats.
- Supports the implementation of system security plans with agency personnel and external vendors.
- Collaborates with agency personnel and external partners to remediate identified vulnerabilities and ensure compliance with cybersecurity policies and standards.
- May perform vulnerability scans and penetration testing of networks, systems, and applications.
- May assist in developing, reviewing, and updating cybersecurity policies, procedures, and standards to align with regulatory requirements and best practices.
- May assist in preparing detailed reports on cybersecurity incidents, vulnerabilities, and regulatory compliance status for management and other stakeholders.
- Ability to oversee and/or supervise the work of others.
- Performs related work as assigned.

GENERAL REQUIREMENTS:

- **PREFERRED EDUCATION**: Graduation from an accredited four-year college or university with major coursework in information technology security, computer information systems, computer science, management information systems, or a related field is preferred.
- **EXPERIENCE:** Minimum three years of full-time experience in information security or cybersecurity analysis, or IT security administration and operations work is required. Experience with Microsoft Office is required.
- **PREFERRED EXPERIENCE**: Proficiency in scripting languages (e.g., PowerShell, Python, etc.), experience with security tools and technologies including firewalls, IDS/IPS, SIEM, and endpoint protection solutions, and experience with Microsoft on-prem and cloud environments is preferred.
- **REQUIRED CERTIFICATION OR LICENSURE:** Certifications obtained in two or more of the following are required:
    - Certified Information Systems Security Professional (CISSP)
    - Microsoft Cybersecurity Architect (SC-100)
    - Certified Cloud Security Professional (CCSP)
    - Certified Information Systems Auditor (CISA)
    - Certified Information Systems Manager (CISM)
    - Certified in Risk and Information Systems Control (CRISC)
    - Information Systems Security Management Professional (ISSMP)

KNOWLEDGE, SKILLS, AND ABILITIES:

- Knowledge of local, state, and federal laws and regulations relevant to information security and privacy (e.g., Texas Administrative Code Chapter 202, NIST SP 800-53, etc.)
- Knowledge of cybersecurity and information security controls, practices, procedures, and standards
- Knowledge of the limitations and capabilities of computer systems and technology; technology across all mainstream networks, operating systems, and application platforms; operational support of networks, operating systems, Internet technologies, databases, and security applications and infrastructure
- Knowledge of incident response program practices and procedures
- Knowledge of disaster recovery and business continuity concepts
- Knowledge of change management best practices
- Skill in the use of computers and applicable software and the configuring, deploying, monitoring, and automating of security applications and infrastructure
- Skill in analysis and problem-solving
- Proficient written and verbal communication skills
- Demonstrated organizational skills and the ability to work independently and as part of a team
- Ability to resolve complex security issues in diverse and decentralized environments; to plan, develop, monitor, and maintain cybersecurity and information technology security processes and controls
- Ability to gather, assemble, correlate, and analyze facts to prepare and develop reports and actionable recommendations
- Ability to establish goals and objectives
- Ability to map processes
- Ability to communicate effectively to both technical and non-technical audiences using interpersonal and collaborative skills, and appropriate supporting technology
- Ability to establish and maintain effective and cordial working relationships at all organizational levels, including agency management, direct supervisors, co-workers, and internal and external customers
- Ability to resolve and respond timely to support requests

NOTE:

- The position may require travel up to 5% of the time, additional work hours including evenings, weekends, and/or holidays to meet critical deadlines.
- The job posting in no way states or implies that the duties listed above are all inclusive. Employees are required to perform other duties as assigned.

External final male applicants who are 18-25 years of age will be required to furnish proof of registration or exemption from registration with the Selective Service System as a condition of state employment.

All offers of employment are contingent upon the candidate having legal authorization to work in the United States. Failure to present such authorization within the time specified by the U.S. Department of Labor will result in the offer being rescinded.

All offers of employment are also contingent upon satisfactory credit and background check.

HOW TO APPLY:

Submit a completely filled out state of Texas application using one of the methods below:

- Online at https://www.workintexas.com, or
- Email to humanresources@sml.texas.gov, or
- Mail to 2601 N. Lamar Blvd., Ste. 201, Austin, TX 78705, or
- Fax to 512-475-1505.

Applications are available at https://www.twc.texas.gov/sites/default/files/busops/docs/state-of-texas-applications-e-133-twc.pdf

Resumes and cover letters are optional. Resumes are not accepted in lieu of a completed application.

For directions or to request physical accommodations call Human Resources at 512-475-0614.

E-Verify – This organization participates in E-Verify. This employer 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.

Department of Savings and Mortgage Lending is an equal opportunity employer.