CANCER PREVENTION AND RESEARCH INSTITUTE OF TEXAS

INFORMATION SECURITY OFFICER

Cancer Prevention and Research Institute of Texas (CPRIT) is the second largest funder of cancer research and prevention activities behind only the federal government. Over the past decade, CPRIT has invested more than $2.9 billion in cutting edge research leading to a significant increase in intellectual property and knowledge related to cancer treatments, cures, and prevention best practices. CPRIT offers an unparalleled opportunity to catalyze discovery and progress in the prevention, diagnosis, and treatment of cancer.

Position Summary
Performs senior level information security work providing direction and guidance in strategic information technology operations and planning. Work involves overseeing and/or planning, implementing, and monitoring security measures and resolving information security threats to ensure the protection of agency systems and infrastructure. Directs the agency's response to and resolution of cyber incidents in collaboration with the Texas Department of Information Resources. Depending on the incident, the ISO will be expected to provide direction outside of normal working hours until resolution. Develops information security and business continuity standards and action plans; develops security architecture and policies based on business needs, risk assessments, and regulatory requirements; and conducts information security risk analysis and system audits. Works under minimal supervision, with extensive latitude for the use of initiative and independent judgment. This position works closely with the Information Resources Manager and reports directly to the Chief Compliance Officer.

Salary Range: $101,630 - $171,881/year

Closing Date: May 16, 2022

GENERAL QUALIFICATION REQUIREMENTS

Experience
A minimum of 7 years' work experience in security operations and/or information technology in the public sector or at a private sector company.

Must have at least three years' experience working with:

- Texas Administrative Code § 202 cybersecurity rules, the Texas Cybersecurity Framework or similar public sector cybersecurity standards.
- Cloud platforms (Azure, AWS).
- Implementing and managing information security tools and platforms including but not limited to endpoint management systems, two-factor authentication services, and incident management systems.
- Implementing and enforcing information security policies, procedures, and guidelines.

Education

Graduation from an accredited four-year college or university with major course work in computer science, management information systems or a related field is generally preferred. Experience and education may be substituted for one another on a year for year basis.

Preferred Certifications: Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP) certification, and/or Certified Information Systems Manager (CISM)

Knowledge, Skills and Abilities

Knowledge of local, state, and federal laws and regulations relevant to information security, privacy, and computer crime.

Knowledge of the NIST-Cybersecurity Framework.

Preferred knowledge of NIST 800 series frameworks.

Knowledge and experience with the limitations and capabilities of computer systems; technology across all network layers and computer platforms; and operational support of networks, operating systems, Internet technologies, databases, and security applications.

Knowledge of business and management principles involved in strategic planning and resource allocation.

Ability to think strategically and focus on results.

Ability to analyze complex information and exercise sound judgment in making critical decisions or providing recommendations to agency management that lead to critical decisions.

Ability to identify problems, evaluate alternatives, and implement effective solutions.

Ability to develop, evaluate and write policies and procedures.

Ability to respond to and resolve advanced security issues in a decentralized environment.

Ability to communicate effectively including translating complex technical information into non-technical, clear concepts, both orally and in writing. Written communication will include reports, memos, and other documents.

Knowledge of monitoring agency security infrastructure.

Ability to work in a structured environment with third-party oversight by other state agencies and entities.

Ability to work well under pressure, complete tasks to defined schedules, and effectively plan, organize, and coordinate multiple priorities.

Ability to establish and maintain effective working relationships with agency personnel across the organization and with the agency board.

Ability to comply with all agency policies and applicable laws.

Ability to comply with all applicable health and safety rules, regulations, and standards.

EXAMPLES OF WORK PERFORMED

Develops, revises, and oversees the implementation of state-mandated information security and cybersecurity policies, standards, guidelines, and procedures to ensure agency information security capabilities address current threats.

Develops and manages the agency's information security and risk management awareness training programs.

Leads the agency's information technology governance group with responsibility to organize regular meetings, prepare and distribute policy and procedure revisions to the group, maintain minutes and other documentation, and incorporate decisions into existing agency policies and procedures for implementation.

Designs, updates, and monitors all agency infrastructure information security configurations to adhere to the established information security and cybersecurity policies and procedures.

Periodically reviews security requirements for new and existing applications and systems, including physical security and infrastructure environment security, documenting every review; periodically reviews account permissions and computer data access needs of agency personnel and vendors, documenting every review; reviews, documents the review of, and reports security violations and any necessary follow-up activities.

Coordinates implementation of recurring technical risk assessments, vulnerability scans and penetration tests of agency-managed IT systems; reviews the results; monitors resolution of action items; and documents each review.

At least annually assesses the information resource functions adherence to established policies and procedures, documenting exceptions to and reporting on the effectiveness of the security program to the agency’s information technology governance group and Chief Executive Officer.

Prepares and submits the agency's Information Security Plan to DIR every even-numbered year.

Monitors and assesses the security practices of outsourced information technology service providers.

Develops and maintains the information technology disaster recovery, business continuity and incident response plans. Oversees tests of each plan at least annually and prepares reports on the results of the tests with recommendations for improvements, as necessary, to the Chief Executive Officer and other agency management.

Coordinates with the agency Information Resources Manager to maintain a compliant information technology environment in adherence with established agency and state security and technology policies, guidelines, and practices.

Coordinates with the Information Resources Manager to verify that security requirements are identified, and risk mitigation plans are developed and implemented prior to the deployment of internally developed information systems and/or related applications or services.

Coordinates with the Information Resources Manager on the review of security requirements and specifications for and to verify that security requirements are identified, and risk mitigation plans are developed and contractually agreed and obligated prior to the acquisition of new information systems and/or related services and applications.

Performs related work as assigned.

Military Occupational Codes

You may access the Military Occupational Specialty (MOS) codes applicable to this position at Military Crosswalk for Occupational Category - Information Technology. CPRIT encourages Veterans, Reservists, or Guardsmen with a MOS or additional duties that fall in the fields listed in the above link who meet the minimum qualifications listed above to apply.

Application Instructions

If you meet the qualifications, complete, and submit a State of Texas application online via the WorkInTexas.com portal. You may also mail the application to Cancer Prevention and Research Institute of Texas, Human Resources, P.O. Box 12097, Austin, Texas 78711.

A State of Texas application may be obtained from https://www.twc.texas.gov/jobseekers/state-texas-application-employment#applicationFormForDownload.

All résumés must be accompanied by a fully completed state of Texas application. Incomplete applications may be disqualified at the agency's discretion. Faxed and emailed applications will not be accepted.

CPRIT is a non-smoking office; the agency is in the Capitol Complex of Austin, Texas.

CPRIT currently offers teleworking as an option to employees.

The Cancer Prevention & Research Institute of Texas is an equal opportunity employer.

You may find additional information regarding the Institute's history and operations on the agency's website at https://cprit.texas.gov/.