UNIFIED JUDICIAL SYSTEM
POSITION DESCRIPTION

CHIEF INFORMATION SECURITY OFFICER (CISO)

CLASS CODE: 99-31-51

POSITION PURPOSE

Serves as trusted advisor and strategic security personnel responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. This includes managing security operations, overseeing cybersecurity policies, and ensuring compliance with regulatory requirements to safeguard the organization's data and infrastructure.

DISTINGUISHING FEATURES

The Chief Information Security Officer (CISO) provides leadership, as well as expertise to ensure effective systemwide security analysis; standards and testing; risk assessment; awareness and education; and development of policies, standards, and guidelines. The CISO will partner with BIT technology leadership to maintain and enforce the information security framework and the associated policies and standards to reduce risk to information systems.

MAJOR RESPONSIBILITIES

Note: The duties listed are typical examples of work performed by positions in this job classification. Not all duties are included, nor is the list inclusive.

1. Develops and implements a security strategy that aligns with UJS objectives and regulations providing vision and direction.

2. Identifies, audits, evaluates, assesses, and mitigates cybersecurity risks to the UJS to ensure continued operations.
   a. Assesses the threat landscape and UJS vulnerabilities constantly.
   b. Develops risk managements strategies to mitigate identified risks and prevent potential security incidents that could disrupt operations, cause financial loss, or damage reputation.
   c. Defines and documents how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.

3. Develops and maintains an incident response plan that enables the UJS to quickly respond to and recover from security incidents to ensure reduced downtime, limit the impact of breaches, and ensure business continuity.
   a. Establishes and maintains an incident response plan to address security breaches or incidents effectively.

   b. Leads incident response activities, including investigation, containment, recovery, and post-incident analysis.

4. Monitors and audits security systems and the IT environment for signs of compromise to ensure security risks are identified and minimized.
   a. Evaluates new security technologies and practices to enhance the security posture of the state government.
   b. Ensures the seamless integration of security technologies with existing systems and processes.
   c. Acts as a liaison between the state government office and external entities on matters related to information security.
   d. Provides expert advice on how to secure sensitive information and technology resources.

5. Directs the installation of network hardware and configuration of network access privileges including:
   a. Server creation, deployment, management, maintenance, upgrade and removal
   b. Active directory account management and monitoring
   c. Multi Factor Authentication requirements
   d. Endpoint protection deployment and monitoring

6. Develops and oversees disaster recovery and business continuity plans related to information security to ensure systems can be quickly restored in the event of a disaster or failure.

7. Develops a professional team of cybersecurity experts through mentorship, creating and facilitating professional development opportunities, and quality reviews and feedback of work.

8. Performs other work as assigned.

SUPERVISORY FUNCTIONS

This position supervises the positions in the Security Standards and Support area.

ESSENTIAL FUNCTIONS REQUIRE

In-state travel for project implementation and meetings; and in-state and out-of-state travel for training; evaluating and understanding of computer systems' interaction, hardware, software, and data storage capabilities; working in cramped spaces, lifting heavy equipment, and exposure to electrical hazards during installations; sitting for extended periods of time; working outside normal work hours when needed; operating computer systems' hardware and technology; operating standard office equipment such as copier, telephone, etc.; and attendance in accordance with rules and policies. The incumbent is also required to work effectively with coworkers and the public; understand, evaluate, and analyze statistical data and draw reasonable and accurate conclusions from that data; manage stress appropriately; possess organizational and

leadership skills; meet deadlines; demonstrative initiative and motivation; and communicate (verbally and in writing) complex technical concepts and ideas to non-technical individuals.

PROBLEMS AND CHALLENGES

Challenges include maintaining a continual and updated knowledge of existing cybersecurity threats and possible responses to ensure systems are secure and maintain operations; ensuring that acquired or developed systems and architectures are consistent with organization's cybersecurity architecture guidelines; building an incident threat response plan that is responsive and current; and evaluating and analyzing a multitude of threats and responding to immediate threats as needed.

DECISION-MAKING AUTHORITY

Decisions include developing and implementing the disaster recovery plan, analyzing cybersecurity threats and incidents, recommending security strategy, building relationships with other branches of government and outside vendors/agencies to ensure security, and security and approval of new and existing technologies.

Decisions referred include approval of statewide security strategy; cybersecurity breaches for response that include data breaches, fiscal response, and public scrutiny; and statewide continuity of operations policies and procedures due to cybersecurity events.

CONTACT WITH OTHERS and PURPOSE

Daily contact with BIT personnel to ensure statewide systems are secure and informed of potential cybersecurity issues; and UJS staff to ensure new and existing technologies conform to security strategy and guidelines.

WORKING CONDITIONS

The incumbent works in a typical office environment.

COMPETENCIES/QUALIFICATIONS FOR APPOINTMENT

Knowledge, Skills and Abilities

Knowledge of:

- data security requirements and standards including installation options, access monitoring, and problem solving techniques;
- disaster recovery methods;
- computer networking concepts and protocols, and network security methodologies;
- cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation);

- management and supervisory techniques.

Skill in:

- conflict management;
- time management;
- planning and project management.
- establishing, defining, and documenting standards and policies.

Ability to:

- research new technologies and advocate methods to use them and benefit UJS;
- make decisions in highly stressful and impactful situations;
- understand the overall impact of system security;
- effectively set priorities;
- build effective teams;
- communicate effectively with diverse groups of users;
- see potential issues and forestall their development;
- exercise sound judgment and make timely and well-informed decisions.

Education

Bachelor's degree from an accredited university or college in computer science, computer security, or a related field.

Experience

Three (3) years of experience in cybersecurity, including managing security operations and incident response; one (1) year of supervisory experience leading and managing a team.