Classification: Division Assistant Director (Cybersecurity and Technology Section)

Title Code: V07901

Pay Range: 30

POSITION SUMMARY: This is a highly technical, supervisory and administrative position responsible for developing, directing, and managing the Cybersecurity and Technology section of the Criminal Justice Information Services (CJIS) Division. This section includes units focused on: security operations, security compliance and auditing, product research, cloud infrastructure support and technical support. An employee in this position serves as the Missouri State Highway Patrol (MSHP) Chief Information Security Officer (CISO), the MSHP Chief Privacy Officer (CPO), as well as supervises the CJIS Information Security Officer (ISO). General direction is received from a superior, but the employee is given latitude for using independent judgment and initiative in attaining overall objectives.

DESCRIPTION OF DUTIES PERFORMED (Any one position may not include all of the duties listed nor do the listed examples include all tasks which may be found in positions of this class.):

The CISO is responsible for the implementation, direction, execution, and monitoring of highly sophisticated information security and technology programs for the agency that affect several technical environments within the CJIS Division. In addition, this position is responsible for frequent coordination and interaction with troops, divisions, and other state, local, and federal agencies, as well as vendors and contractors, to include routinely advising and briefing command staff and other high-level employees regarding information security topics and strategies.

The CPO oversees the privacy and compliance impacts of various agency activities, to include leading the Patrol's Privacy Review Team in performing the Patrol's yearly internal privacy audit.

Supervises the CJIS ISO for the State of Missouri who acts as the security point of contact for the Federal Bureau of Investigation's (FBI) CJIS Division, as well as ensures/documents technical compliance with the FBI's CJIS Security Policy and maintains state policies in line with industry standards; enforces technical security policies, system compliance and initiates possible sanctions; as well as plans, coordinates, and executes a security plan and often serves as the CJIS division point of contact for the criminal justice information technology (IT) projects.

Develops and maintains the technical security audit program, acts as the lead on any security incident event, analyzes and designs security for information systems, IT projects, network infrastructure, administrative and oversight control of local-area network (LAN), network, server and virtual private network (VPN) privileges and architecture direction, as well as future network connectivity design.

Provides technical direction, as well as strategic and tactical plans, for the implementation and operation of law enforcement technology and information security enabling the agency to operate efficiently, effectively, and with the highest level of data integrity.

Documents technical compliance with the CJIS Security Policy and other applicable security and technology standards with the goal to assure confidentiality, integrity and availability of CJIS information to the user community, as well as ensures that personnel screening procedures are being followed as stated in the CJIS Security Policy; and ensures compliance of Patrol components, as well as local, state, and federal agencies, in accordance with MSHP security policies.

Authorizes all access privileges to Patrol employees, contractors, and external partners ensuring access is based on the principle of least privilege and that all pre-requisites for access have been met.

Plans, organizes, directs, and coordinates IT security management efforts across multiple hardware and software platforms and technologies.

Directs and coordinates the work of a staff of IT professionals.

Prepares and evaluates grant applications, statements of work, bid specifications and other documentation for funding and acquisition of tools, technology, contractual services, and education relating to computer security.

Regularly participates in user groups and professional organizations focused on IT security and service delivery.

Researches and oversees the selection of all IT and security products.

Advises senior staff and the Chief Security Officer (CSO) in policy-making decisions concerning CJIS requirements and IT security procedures for all the MSHP automated systems.

Provides direction to the MSHP personnel on all security and technology related products and endeavors.

Serves as lead of the privacy governance/audit team and manages overall privacy policy/impact studies for the Patrol.

Performs work-related travel as necessary.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Extensive knowledge of the principles, practices, and techniques of information security/information technology program management including network, server, device, data, application, physical and personnel security.

Extensive knowledge of security and technology operations related issues of server hardware, operating systems and storage technologies.

Comprehensive knowledge of emerging trends and developments in information technology.

Comprehensive knowledge of leadership principles and techniques.

Comprehensive knowledge of the concepts and principles of project management.

Comprehensive knowledge of the principles of cost benefit analysis.

Comprehensive knowledge of or the ability to learn the agency's functions and interrelationships.

Considerable knowledge of modern management principles and techniques, particularly as applied to security of enterprise IT infrastructure.

Considerable knowledge of principles and practices of administration and supervision.

Considerable knowledge and experience in information privacy laws, access, release of information, and release control technologies.

Working knowledge of systems analysis and design techniques.

Thorough knowledge of or ability to learn the CJIS Security Policy.

Through knowledge of or ability to learn the MULES system as it relates to the technical connectivity and CJIS requirements.

Intermediate knowledge of the procurement and bid processes.

Considerable knowledge of the principles and practices of administration and effective supervision.

Considerable knowledge of computer operating systems.

Considerable knowledge of database management systems.

Working knowledge of or ability to learn the agency's automated information systems.

Working knowledge of the principles of disaster recovery.

Working knowledge of various computer platforms.

Working knowledge of the information strategic planning process.

Working knowledge of the systems management process.

Working knowledge of the principals of information system audits and security testing

Possess high-level skill in legal interpretation and policy development.

Possess good public speaking skills and the ability to interact with a variety of business professionals.

Possess good organizational skills.

Possess research and analysis skills.

Ability to plan and implement projects and audits necessary to ensure effective and efficient operation of security measures.

Ability to maintain accurate records, files, and documentation.

Ability to exercise judgment and discretion.

Ability to perform job related travel as needed.

Ability to provide direction/guidance to projects involving multiple organizations and/or groups.

Ability to support, coach, and mentor assigned team members.

Ability to utilize project management tools.

Ability to prepare and maintain standards, policies, procedures, guidelines and technical manuals.

Ability to train and assist less experienced personnel.

Ability to create and present materials for training programs.

Ability to operate basic office equipment as detailed in the description of duties.

Ability to handle restricted and confidential information in a professional manner and maintain the information as such.

Ability to communicate in English clearly and concisely, both orally and in writing.

Ability to establish and maintain harmonious working relations with others.

Ability to work with material that may be of a sexual nature relating to criminal activity (e.g., written material, photographs, and/or verbal language, etc.).

Ability to work hours as assigned.

MINIMUM EXPERIENCE AND EDUCATION REQUIRED (The following represents the minimum qualifications used to accept applicants, provided that equivalent substitution will be permitted in case of deficiencies in either experience or education.):

Possess a Bachelor's degree in Cybersecurity, Information Security, Information Assurance, Computer Science, Computer Information Systems, or Business Administration with an emphasis in Information Security or Information Technology, or a closely related area, with a minimum of 15 hours of IT-related coursework.

AND

Seven years experience in the Information Security or Information Technology field with duties directly related to information security and technology principles, designing, and managing an information security/information technology management program. Two of the seven years must have been in a supervisory position responsible for training, mentoring, and developing less senior employees.

Possession of a Master's degree may be substituted on a year-for-year basis for the required experience.

NECESSARY SPECIAL REQUIREMENTS: Must be a United States Citizen, or a legal resident of a country participating in the Visa Waiver Program (VWP).

Must be able to obtain and maintain MULES certification within six (6) months of appointment.

Must attend and successfully pass Police Instructor School within twelve (12) months of appointment.

Must be able to obtain and maintain a Certified Information Security Manager (CISM) certificate within three (3) years of appointment.

Successful completion of the Patrol's Supervision School and other leadership/management related courses within twelve (12) months of appointment, or as soon as scheduling will allow.

FLSA STATUS: Exempt

WORK SCHEDULE: An employee in this position works an eight-hour shift as directed; however, working hours are subject to change at the discretion of the commanding authority.