Classification: Computer Information Technologist (CIT) III
Security Intelligence Unit (SIU)

Title Code: V08003

Pay Range: 28

POSITION SUMMARY: This advanced position performs technical work and provides expertise, as it relates to cyber security (e.g., security issues, cyber threats, and cyber mitigation/remediation, etc.), to MSHP components, as well as local criminal justice agency staff. The position works closely with other Security Intelligence Unit (SIU) personnel in assessing cyber threats to the Missouri State Highway Patrol. Work is performed under general supervision; however, the employee is expected to use technical knowledge and exercise initiative and independence in the performance of assigned responsibilities.

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.):

Monitors, assess, and assists with the mitigation of cyber threats for the Patrol and for the criminal justice domain in the state of Missouri.

Documents cyber intelligence, cyber threats, and cyber incidents and remediations for the Patrol and Missouri's criminal justice agencies.

Maintains current knowledge of all applicable security procedures and policies per Patrol General Order, Patrol Security Policy, SIU procedure, and other applicable state and federal policies.

Participates in the cyber intelligence lifecycle, which may include cyber investigations/incident reviews.

Maintains current knowledge of federal and state laws and monitors regulatory changes to ensure organizational adaptation.

Participates in the development and delivery of cyber intelligence and cyber threat information to employees, contractors, and other appropriate third parties.

Participates in the performance of periodic assessments, to include analysis, mitigation recommendations and corrective action plans.

Participates in innovating, creating, maintaining, and researching technologies and processes.

May participate in user groups and professional organizations focused on information technology (IT) security and cyber intelligence.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Considerable knowledge of the principles, practices, and techniques of information security programs and cyber threat analysis, to include network, server, device, data, application, physical, and personnel security.

Considerable knowledge of security related issues of server hardware, operating systems and storage technologies.

Considerable knowledge of information security principles, as well as information security management and the cyber intelligence lifecycle.

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

Considerable knowledge of the agency's functions and their inter-relationships, to include MSHP's policies, procedures, rules and regulations.

Considerable knowledge of system analysis and design techniques.

Ability to deal effectively with various personalities.

Ability to extrapolate current situations and performance and to merge these with future software plans and technology.

Ability to respond quickly to emergency situations.

Ability to work closely as a cooperative team and display professionalism and team leadership in the training and supervision of others, to include the monitoring and evaluation of others.

Ability to work independently in an organized, efficient manner and exercise independent judgement and discretion.

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 from an accredited four-year college or university in mathematics, statistics, accounting, computer science, Cybersecurity, Information Assurance, or related field; AND two years of experience in the areas of information security, cybersecurity, or information assurance fields.

OR

One year of experience as a CIT II in the Security Intelligence Unit.

Preference may be given to those possessing current certification(s) in Information Security or Information Technology and/or work experience and knowledge in all areas of information security, to include security best practices, forensics, threat hunting, cyber intelligence, and the concepts vital to ensuring confidentiality, integrity and availability of protected data and systems.

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

Must possess and maintain a MULES Certification within one year of hire.

FLSA STATUS: Non-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.