Classification: Computer Information Technology Specialist (CITS) II
Security Intelligence Unit (SIU)

Title Code: V08005

Pay Range: 33

POSITION SUMMARY: This advanced position performs technical work and provides consultative expertise, as it relates to cyber security, to MSHP components, as well as local criminal justice agency staff. An employee in this position works closely with, and may assist, the Information Security Officer (ISO) with managing and assessing cyber threats to the Missouri State Highway Patrol. This position is responsible for assisting the ISO in the implementation, direction, and execution of a highly sophisticated information security program for the agency and Missouri's criminal justice agencies. This position requires frequent coordination and interaction with the troops, divisions of the Patrol, as well as other local, state, and federal agencies, vendors, and contractors. Work is performed under general supervision; however, the employee is expected to exercise initiative and independence in the use of extensive technical knowledge to meet goals and 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.):

Monitors for, assesses, 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.

Follows all applicable security procedures and policies as prescribed per Patrol General Order, Patrol Security Policy, SIU procedure, and other applicable state and federal policies.

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

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

Develops, and ensures delivery of cyber intelligence and cyber threat information to employees, contractors, and other appropriate third parties.

Performs periodic assessments, to include analysis, mitigation recommendations and corrective action plans.

Provides both written and oral reports on the status of the Patrol's cyber threat assessment program to the ISO.

Innovates, creates, maintains, and researches technologies and processes to ensure the effective management of information security controls to protect the Patrol's information assets.

Directs and coordinates the work of a staff of information security professionals.

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

Researches and oversees the selection of all cyber intelligence products, and manages their use and operation.

Provides direction to Patrol personnel on all cyber intelligence and threats and related products and endeavors.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Extensive knowledge of the principles, practices, and techniques of information security program management 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 in information security principles, as well as information security management and the cyber intelligence lifecycle.

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

Thorough knowledge of principles and practices of administration and supervision.

Thorough knowledge of the principles of project management, the procurement process, and the strategic planning process.

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

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

Working knowledge of systems analysis and design techniques.

Must be skilled in time management techniques and prioritization.

Must possess excellent interpersonal skills to deal effectively with various personalities.

Ability to comprehend, analyze, and research problems of a complex nature and make judgment decisions as to their solution.

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 analyze, direct, and manage the implementation of special projects, assignments, and programs.

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

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 demonstrate excellent management skills.

Ability to provide technical assistance and guidance in work methods and program procedures.

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 with specialization in mathematics, statistics, accounting, computer science, Cybersecurity, Information Assurance, or a closely related field; AND five years of experience in the areas of information security, cybersecurity, or information assurance fields.

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: 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.