Classification: Computer Information Technology Specialist (CITS) II
Cyber Forensics Investigative Unit (CFIU)
Title Code: V08005
Pay Range: 33

POSITION SUMMARY:

This is an advanced position providing technical and professional consultative work in cyber forensics and the examination of digital evidence during criminal investigations and cybersecurity incident response. An employee in this class works closely with the Chief Information Security Officer (CISO), the Missouri State Highway Patrol's Division of Drug and Crime Control (DDCC), Patrol component staff, local criminal justice agencies, as well as various federal and private partners in providing guidance and technical expertise on highly complex cyber forensic issues. Work includes assisting the Patrol with the creation, design, implementation and management of cyber forensic capabilities to aid the Patrol and partner entities in the investigation of incidents, both of a criminal and non-criminal nature. Work is performed independently under general supervision; however, the employee is expected to exercise independence in the performance of assigned responsibilities, as well as use extensive technical knowledge and initiative 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.)

Investigates complex security issues in diverse environments, proposes solutions, and works with technical and business staff to implement solutions.

Aids DDCC's Digital Forensics Investigative Unit (DFIU) Investigators with cyber forensic examinations in support of active criminal investigations.

Provides support to both Patrol and partners in complex cybersecurity issues.

Investigates security incidents, both internal and external to the Patrol.

Cross-references cyber intelligence with indicators from various information sources in order to assist Patrol Security Operations Center staff in network defense.

Prepares and participates in presentation of cybersecurity information to various audiences, to include meeting with technical and business staff of criminal justice agencies and partners with homeland security responsibilities.

Performs log scans of the Missouri Uniform Law Enforcement System (MULES) system for investigations, possible misuse, or administrative purposes.

Documents, reviews, and updates security policies and procedures for Patrol and local agencies by reviewing, interpreting, and applying industry standards, as well as local, state and federal statutes and regulations.

Coordinates with members of the local and state criminal justice community to discuss cybersecurity issues, to include working alongside partners to facilitate greater information sharing and cybersecurity defense.

Researches and reviews security infrastructure hardware and/or software to provide situational awareness regarding cyber incidents/issues to law enforcement and other stakeholders.

Provides situational awareness briefings to Patrol staff regarding cyber incidents or issues.

Serves as the liaison with the intelligence community and participates in initiatives aimed at broadening the level of understanding of cyber threat actors on a local, national and international level.

Collects, evaluates and produces intelligence products in order to fulfill strategic intelligence questions related to cyber activity.

Develops, coordinates and facilitates the statewide Cyber Intelligence Liaison Officer program in order to increase intelligence sharing among law enforcement and homeland security partners.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES:

Comprehensive knowledge of the principles of intelligence operations, classifications, as well as rules and procedures concerning proper presentation and dissemination of intelligence products.

Thorough knowledge of the general operating principles and capabilities of computer hardware and software.

Thorough knowledge of the elements of cybercrime and threat indicators.

Thorough knowledge of advanced cyber forensics techniques, evidence preservation and courtroom testimony.

Considerable knowledge of computer security best practice standards.

Considerable knowledge of computer operating systems.

Considerable knowledge of data protection methods.

Working knowledge of computer networking protocols.

Working knowledge of national information sharing tools and techniques.

Working knowledge of agency's functions and their interrelationships.

Working knowledge of the principles of disaster recovery.

Working knowledge of continuing trends and developments in information technology and cybersecurity.

Working knowledge of various computer platforms.

Working knowledge of the information strategic planning process.

Working knowledge of the systems management process.

Possess good organizational skills.

Possess research and analytical skills.

Possess leadership skills necessary to mentor junior level employees.

Possess public speaking skills.

Possess writing skills.

Ability to utilize highly technical analytical tools.

Ability to prepare and interpret system configuration documentation.

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

Ability to create and present materials for training programs.

Ability to train and assist less experienced personnel.

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 maintain a clean and orderly work environment.

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 Information Security, Cybersecurity, Information Assurance, Information Systems, or related field; AND five years of experience in the areas of information security, such as security best practices, standards, legal requirements, privacy policy, networking, servers, end user support, databases, web and application development, and concepts vital to ensuring confidentiality, integrity and availability of protected data systems.

Preference may be given to those possessing a current certification(s) in Information Security and/or work experience in information security, information technology, MSHP Security Intelligence, and/or cyber/criminal intelligence/forensics.

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 valid driver license.

Must be able to obtain and maintain MULES certification within twelve (12) months of appointment.

Must pass a comprehensive background check necessary to have access to criminal intelligence and other information in the Missouri State Highway Patrol

Must obtain a secret level Department of Homeland Security background/clearance or other federal background/clearance of equal security level.

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.