Classification: Computer Information Technologist (CIT) II
Digital Forensics Investigative Unit (DFIU)

Title Code: V08002

Pay Range: 25

POSITION SUMMARY: This is an intermediate-level position providing technical and professional consultative work in cyber forensics and the examination of digital evidence during criminal investigations and cybersecurity incident response. Work includes conducting forensic examinations of digital media (e.g. computer, cellular devices, etc.), which is believed to contain evidence relevant to the investigation and/or prosecution of a federal, state, or local crime, violation of law, or the protection of national security. This position is responsible for the forensic collection, recovery, processing, preservation, analysis, storage, maintenance, and/or presentation of digital evidence. An employee in this position also assists Patrol and other law enforcement officers in crime scene processing and the collection and preservation of evidence. Work is performed under general supervision within established policies and procedures; however, independent judgment is required.

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.):

Conducts forensic examinations of digital media to obtain evidence relevant to criminal investigations.

Determines the most appropriate method of recovery and protection of digital data that may have been deleted, erased, hidden, and/or encrypted.

Recovers, processes, and analyzes digital evidence for use in solving criminal investigations.

Preserves, stores, and maintains all recovered digital evidence.

Initiates and maintains liaisons with other law enforcement organizations in order to ensure an exchange of information on the latest forensic techniques and equipment.

Participates in the development and/or modification of computer systems to obtain more precise and accurate diagnostic examination capabilities.

Prepares digital evidence for the use of appropriate authorities in court proceedings.

Prepares appropriate reports for court proceedings; testifies in court as necessary.

Provides technical assistance and training to other forensic computer examiners to ensure proper recovery and handling of digital evidence.

Reviews reports written by Patrol officers and other law enforcement officers to obtain necessary information and stay abreast of criminal activity in the area of digital media.

Prepares reports, correspondence, and Patrol forms directed to Patrol members and authorities outside the agency.

Performs other work-related duties as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Working knowledge of the principles of intelligence operations, classifications, as well as rules and procedures concerning proper presentation and dissemination of intelligence products.

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

Working knowledge of the elements of cybercrime and threat indicators.

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

Working knowledge of computer security best practice standards.

Working knowledge of computer operating systems.

Working 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.

Knowledge of the information strategic planning process.

Knowledge of the systems management process.

Possess good organizational skills.

Possess research and analytical 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 function effectively in high-pressure and stressful situations.

Ability to work in varying climatic conditions.

Ability to work long hours, while sitting, without a break.

Ability to accommodate a non-standard schedule and to be on call.

Ability to transport equipment used in digital forensics investigations.

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 in Computer Science, Information Security, Cybersecurity, Information Systems, or related field; and one year of experience in the areas of networking, servers, end user support, databases, web and application development, and concepts vital to ensuring confidentiality, integrity and availability of protected data systems.

OR

One year of experience as a CIT I in the Digital Forensics Investigative Unit.

Preference may be given to those possessing a current certification(s) in computer forensics and/or work experience in computer forensics, information technology, 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 pass a comprehensive background check necessary to have access to criminal intelligence and other information in the Missouri State Highway Patrol

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.