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

Title Code: V08000

Pay Range: 18

POSITION SUMMARY: This is a trainee-level 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 position will receive formal and/or on-the-job training while 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 detailed direction and close supervision within established policies and procedures.

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.):

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

Learns to assist in determining the most appropriate method of recovery and protection of digital data that may have been deleted, erased, hidden, and/or encrypted.

Learns to recover, process, and analyze digital evidence for use in solving criminal investigations.

Learns to preserve, store, and maintain all recovered digital evidence.

Receives direction in initiating and maintaining liaisons with other law enforcement organizations in order to ensure an exchange of information on the latest forensic techniques and equipment.

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

Learns to prepare digital evidence for the use of appropriate authorities in court proceedings.

Learns to prepare appropriate reports for court proceedings; testifies in court as necessary.

Receives direction in providing technical assistance and ensuring proper recovery and handling of digital evidence.

Learns to review 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.

Learns to assist in preparing 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: Knowledge of or ability to learn the principles of intelligence operations, classifications, as well as rules and procedures concerning proper presentation and dissemination of intelligence products.

Knowledge of the general operating principles and capabilities of computer hardware and software.

Knowledge of or the ability to learn the elements of cybercrime and threat indicators.

Knowledge of or ability to learn advanced cyber forensics techniques, evidence preservation, and courtroom testimony.

Knowledge of or ability to learn computer security best practice standards.

Knowledge of computer operating systems.

Knowledge of data protection methods.

Knowledge of computer networking protocols.

Knowledge of or ability to learn national information sharing tools and techniques.

Knowledge of or ability to learn agency's functions and their interrelationships.

Knowledge of the principles of disaster recovery.

Knowledge of or the ability to learn the continuing trends and developments in information technology and cybersecurity.

Knowledge of various computer platforms.

Knowledge of or the ability to learn the information strategic planning process.

Knowledge of or the ability to learn the systems management process.

Possess good organizational skills.

Possess research and analytical skills.

Ability to or willing to learn to utilize highly technical analytical tools.

Ability to or willing to learn to prepare and interpret system configuration documentation.

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

Ability to or willing 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.

OR

Successful completion of an Associate Arts program (or at least sixty {60} credit hours) with at least fifteen (15) credit hours in Computer Science, Information Security, Cybersecurity, Information Systems, or related field.

OR

Possess a high school diploma or equivalent and four (4) years of experience in the duties associated with this position.

Preference may be given to those possessing a current certification(s) in Information Security and/or work experience in information security, 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.