Classification: Computer Information Technologist (CIT) Trainee (SACU)

Title Code: V08000

Pay Range: 18

POSITION SUMMARY: This is a trainee-level position providing professional and technical support as it relates to information security. The position works closely with the manager of the Security Audit and Compliance Unit (SACU), as well as Patrol components and local criminal justice agency staff, by providing guidance and technical support on highly complex information security issues and deployments. This position learns to assist the manager of the SACU with creating, designing, implementing and maintaining a statewide information security program for the criminal justice community. This position learns to serve as an information technology (IT) Security Auditor and assists in the review of cybersecurity software and hardware, investigation of cybersecurity issues and events, and in preparation of cybersecurity policies and procedures. As the IT Security auditor this position learns to design, execute, and review of the Patrol's IT Security audit program, pending final Information Security Officer (ISO) approval. The position reports to the manager of the SACU and works under detailed direction and close supervision, but is expected to use technical knowledge and initiative to meet goals and objectives. This position may be required to work after normal business hours, and may be on call.

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 provide technical support to the Patrol and to local agencies in computer systems analysis and design; database and/or network administration; systems programming; and/or other computer information technology specialties in terms of cybersecurity.

Learns to provide customer or technical support to both the Patrol and local agencies in regards to implementing highly complex cybersecurity solutions.

Learns to resolve security issues in diverse environments by investigating requirements and issues, proposing solutions, and working with technical and business staff to implement solutions.

Receives direction in documenting, reviewing, and updating security policies and procedures for the Patrol and local agencies by reviewing, interpreting and applying industry standards as well as local, state and federal statutes and regulations.

Receives direction in developing, updating, and maintaing the IT security audits based upon the CJIS Security Policy, statutory and regulatory requirements and industry standards provides peer-level review of audit findings prior to submission for final ISO approval.

Learns to participate in computer systems disaster recovery plan maintenance and implementation for the Patrol.

Receives direction in performing security testing and monitors the Patrol's security infrastructure.

Receives direction in the preparation of reports and documentation in regards to security audit findings to be presented to the ISO and upper management.

Receives direction in the design and testing of complex computer programs and clearly defined segments of highly complex programs in terms of cybersecurity.

Receives direction in reviewing system and application specifications and make recommendations for security enhancements.

Receives direction in the research and review of security infrastructure hardware and/or software.

Learns to participate in computer systems management plan development, maintenance, and implementation.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Knowledge of or ability to learn the areas of cybersecurity as well as networking, application development, server software and hardware.

Knowledge of or ability to learn the principles of computer programming and systems analysis, design, testing and documentation.

Knowledge of or ability to learn the general operating principles and capabilities of computer hardware and software.

Knowledge of or ability to learn the CJIS Security Policy

Knowledge of or ability to learn the MULES system as it relates to the technical connectivity and CJIS requirements.

Knowledge of or ability to learn the agency's automated information systems.

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

Knowledge of or ability to learn the principles of disaster recovery.

Knowledge of or ability to learn the principals of information system audits and security testing.

Knowledge of or ability to learn cyber-incident response management.

Knowledge of or ability to learn deep packet analysis tools, their configuration and use.

Knowledge of or ability to learn encryption methods and virtual private network (VPN) technologies.

Knowledge of or ability to learn cyber-threat analysis.

Knowledge of or ability to learn computer security systems and procedures.

Knowledge of or ability to learn the software reference libraries and related utility programs.

Knowledge of or ability to learn computer networking and telecommunications.

Knowledge of or ability to learn computer operating systems.

Knowledge of or ability to learn database management systems.

Knowledge of or ability to learn advanced authentication solutions.

Knowledge of or ability to learn the applicable Federal Information Processing Standards of (FIPS) encryption.

Knowledge of or ability to learn the Code of Federal Regulations (CFR) and applicable statutes.

Knowledge of or ability to learn the principles of cost benefit analysis.

Knowledge of or ability to learn the principles of project management.

Knowledge of or ability to learn the procurement process.

Knowledge of or ability to learn the continuing trends and developments in computer hardware and software.

Knowledge of or ability to learn the various computer platforms.

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

Knowledge of or ability to learn the systems management process.

Knowledge of or ability to learn the cyber-forensics techniques and digital evidence preservation.

Possess good organizational skills

Possess research and analysis skills

Possess good presentation skills

Ability to utilize project management tools.

Ability to learn to prepare and interpret computer program documentation.

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

Ability to learns to troubleshoot and resolve hardware and/or software problems.

Ability to learn to create and present materials for training programs

Ability to learn to plan and implement projects and audits necessary to ensure effective and efficient operations of security measures.

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

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.

OR

Successful completion of an Associate Arts program (or at least 60 credit hours) with at least 15 credit hours in in Information Security, Cybersecurity, Information Assurance, Information systems, Business Administration, Criminal Justice, or related field.

OR

Possess a high school diploma or equivalent and four years of experience in the areas of information security; cybersecurity; information assurance; in a business, financial, or academic environment, compiling data, analyzing findings, and writing comprehensive reports; and/or the duties associated with this position.

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, standards, legal requirements, privacy policy, networking, servers, end user support, databases, web and application development, 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.