



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

Title Code: V08002

Pay Range: 25

POSITION SUMMARY: This is an intermediate-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 also assists the manager of the SACU with creating, designing, implementing and maintaining a statewide information security program for the criminal justice community. This position serves as an information technology (IT) Security Auditor, reviews cybersecurity software and hardware, investigates cybersecurity issues and events, assists in preparing cybersecurity policies and procedures. As the IT Security auditor this position is directly responsible for assisting with the design, execution, 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 general 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.)

Provides 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.

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

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

Documents, reviews, and updates 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.

Assists in developing, updating, and maintaining 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.

Participates in computer systems disaster recovery plan maintenance and implementation for the Patrol.

Performs security testing and monitors the Patrol's security infrastructure.

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

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

Reviews system and application specifications and make recommendations for security enhancements. Assists in the research and review of security infrastructure hardware and/or software.

Participates in computer systems management plan development, maintenance, and implementation.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Working knowledge in all areas of cybersecurity as well as networking, application development, server software and hardware.

Working knowledge of the principles of computer programming and systems analysis, design, testing and documentation.

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

Working knowledge of the CJIS Security Policy

Working knowledge of the MULES system as it relates to the technical connectivity and CJIS requirements.

Working knowledge of agency's automated information systems.

Working knowledge of agency's functions and their interrelationships.

Working knowledge of the principles of disaster recovery.

Working knowledge of the principals of information system audits and security testing.

Working knowledge of cyber-incident response management.

Working knowledge of deep packet analysis tools, their configuration and use.

Working knowledge of encryption methods and virtual private network (VPN) technologies.

Working knowledge of cyber-threat analysis.

Working knowledge of computer security systems and procedures.

Working knowledge of software reference libraries and related utility programs.

Working knowledge of computer networking and telecommunications.

Working knowledge of computer operating systems.

Working knowledge of database management systems.

Working knowledge of advanced authentication solutions.

Working knowledge of applicable Federal Information Processing Standards of (FIPS) encryption.

Working knowledge of Code of Federal Regulations (CFR) and applicable statutes.

Knowledge of the principles of cost benefit analysis.

Knowledge of the principles of project management.

Knowledge of the procurement process.

Knowledge of continuing trends and developments in computer hardware and software.

Knowledge of various computer platforms.

Knowledge of the information strategic planning process.

Knowledge of the systems management process.

Knowledge of 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 prepare and interpret computer program documentation.

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

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

Ability to create and present materials for training programs

Ability 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 in Information Security, Cybersecurity, Information Assurance, Information systems or related field; AND one year of experience in the areas of information security, cybersecurity, or information assurance fields.

OR

One year of experience as a CIT I in the Cybersecurity and Technology Section.

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.