Classification: Computer Information Technologist (CIT) II
Information Security Unit (ISU)

Title Code: V08002

Pay Range: 25

POSITION SUMMARY: This intermediate-level position performs technical work and provides expertise, as it relates to information security (e.g. highly complex information security issues, deployments, static and dynamic code analysis, secure coding practices, etc.), to MSHP components, as well as local criminal justice agency staff . The position works closely with other Information Security Unit (ISU) personnel in creating, designing, implementing and maintaining a statewide information security program for the criminal justice community, to include performing and/or assisting in the review of cybersecurity software and hardware; the investigation of cybersecurity issues and events; the preparation of cybersecurity policies and procedures; and the presentation of cybersecurity solutions to MSHP components and local criminal justice staff; as well as the design, execution, and review of the MSHP IT Security Audit Program pending final approval. Work is performed under general supervision; however, the employee is expected to use technical knowledge and exercise initiative and independence in the performance of assigned responsibilities.

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 and/or anlysis to MSHP components, as well as local agencies, as it relates to information security, which may include: computer systems analysis and design; database and/or network administration; systems programming; application development and associated secure coding practices; cyber threat analysis and intelligence; and/or other computer information technology specialties in terms of cybersecurity.

Assists in providing customer or technical support to both MSHP components and local agencies in regards to implementing highly complex cybersecurity solutions, which may include: reviewing new and legacy applications for vulnerabilities; providing vulnerability assessments and mitigation recommendations; and/or system network defense.

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

Assists in performing programming and application development, to include creating and developing reports and forms as needed.

Learns to document, review, and update security policies and procedures for MSHP and local agencies by reviewing, interpreting, and applying industry standards, as well as local, state and federal statutes and regulations.

Assists with 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 Information Security Officer (ISO) approval.

Learns to prepare and present cybersecurity information through written documentation and oral presentation to various technical and business staff of criminal justice agencies.

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

Performs administrative duties over security control/protections related to application security, to include log scans for related investigations.

Performs security testing and monitors the MSHP security infrastructure.

Learns to prepare reports and documentation of security audit findings to be presented to the ISO and upper management.

Learns to design and test complex computer programs and clearly defined segments of highly complex programs in terms of cybersecurity.

Participates in meetings with members of the local and state criminal justice community to discuss cybersecurity issues.

Assists in the review of system and application specifications, and makes 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; to include elements of cybercrime and threat indicators.

Working knowlege of the principles of information security and information technology systems and analysis, design, testing, and documentation; to include secure coding practices and the secure software development lifecycle.

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, or the ability to learn, the Criminal Justice Information Services (CJIS) Security Policy, as well as various agency systems as they relate to technical connectivity and the CJIS Security Policy's requirements.

Working knowledge of software reference libraries and related utility programs.

Working knowledge of computer security best practice standards.

Working knowledge of computer networking protocols and operating systems.

Working knowledge of, or the ability to learn, the agency's automated information systems, as well as agency's functions and their interrelationships.

Working knowledge of the principles of cyber-threat analysis, data protection methods, disaster recovery, and cyber-incident response management.

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

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 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.

Working knowledge of cyber-forensics techniques and digital evidence preservation.

Knowledge of, or the ability to learn, the principles of project management, the information strategic planning process, and the systems management process.

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

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

Possess good organizational skills.

Possess research and analysis skills.

Possess basic code analysis skills.

Possess good presentation skills.

Ability to utilize project management and highly technical analytical 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 multi-task effectively.

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 from an accredited four-year college or univeristy 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.