Classification: Computer Information Technology Specialist (CITS) II
Information Security Unit (ISU)

Title Code: V08005

Pay Range: 33

POSITION SUMMARY: This advanced position performs technical work and provides consultative 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, and may assist, the Information Security Officer (ISO) with creating, designing, implementing and maintaining a statewide information security program for the criminal justice community. This position serves as a lead information technology (IT) Security Auditor, reviews cybersecurity software and hardware; investigates cybersecurity issues and events; prepares cybersecurity policies and procedures; and presents cybersecurity solutions to MSHP components and local criminal justice staff. As a lead IT Security Auditor this position is directly responsible for the design, execution and review of the MSHP IT Security Audit Program pending final ISO approval. When the ISO is unavailable this position may serve as a liaison from the MSHP to local and federal agencies, as well as may serve as the interim Security Incident Manager in the event of a cybersecurity incident until the ISO returns. Work is performed under general supervision; however, the employee is expected to exercise initiative and independence in the use of extensive technical knowledge to meet goals and objectives.

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 expertise 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.

Provides 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.

Performs programming and application development, to include creating and developing reports and forms as needed.

Documents, reviews, and updates 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.

Develops, updates and maintains 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.

Assists with preparing and participating in presenting 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.

Prepares 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.

Meets with members of the local and state criminal justice community to discuss cybersecurity issues.

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.

Serves as one of the technical experts on the ISU team, and may act as lead worker and/or provide peer-level review of work, as well as mentoring, to junior staff as it relates to complex technical functions and best practices.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Exentensive knowledge in all areas of cybersecurity as well as networking, application development, server software and hardware; to include elements of cybercrime and threat indicators.

Extensive 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.

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

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

Thorough knowledge of 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.

Thorough knowledge of software reference libraries and related utility programs.

Thorough knowledge of computer security best practice standards.

Thorough knowledge of computer networking protocols and operating systems.

Thorough knowledge of agency's automated information systems, as well as agency's functions and their interrelationships.

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

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

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

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

Considerable knowledge of computer operating systems.

Considerable knowledge of database management systems.

Considerable knowledge of advanced authentication solutions.

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

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

Working knowledge of the principles of cost benefit analysis, as well as the procurement process.

Working knowledge of the principles of project management, the information strategic planning process, and the systems management process.

Working knowledge of national information sharing tools and techniques.

Working knowledge of continuing trends and developments in computer hardware and software.

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

Possess good organizational skills.

Possess research and analysis skills.

Possess 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 train and assist less experienced personnel.

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 five years of experience in the areas of information security, cybersecurity, or information assurance fields.

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: Partial-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.