Classification: Computer Information Technology Specialist II (CITS II) - Security Unit
Title Code: V08005
Pay Range: 33

POSITION SUMMARY:

The position provides professional and advanced technical expertise as it relates to information security. The position works closely with the Information Security officer as well as staff within the MSHP troops and divisions and local criminal justice agency staff by providing guidance and technical expertise on highly complex information security issues and deployments. This position also assists the Information Security Officer with creating, designing, implementing and maintaining a state wide information security program for the criminal justice community. This serves as a lead IT Security auditor, reviews cybersecurity software and hardware, investigates cybersecurity issues and events, prepares cybersecurity policies and procedures and presents cybersecurity solutions to MSHP 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 serves as a liaison from the MSHP to local and federal agencies as well as serving as the interim Security Incident Manager in the event of a cybersecurity incident until the ISO returns. The position reports to the Information Security Officer and works under general supervision but is expected to use extensive technical knowledge and initiative 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 to MSHP ICTD 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 peer-level guidance and support to other security unit employees specifically those classified as a CITS I.

Takes the lead on performing and scheduling IT Security Audits at local agencies and at the MSHP, which involves meeting with senior civilians and command staff to go over areas of non-compliance and discuss possible technical and policy solutions to achieve compliance.

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

Resolves complex security issues in diverse environments by investigating requirements and issues, proposing solutions, and working with technical and business staff to implement solutions. Requires exentensive knowledge in all areas of cybersecurity as well as networking, application development, server software and hardware.

Investigates security incidents, which may include mis-use. Use sophisticated software, hardware and highly technical methods to investigate the incidents. This position may act as an interim security incident manager in the event of a cybersecurity incident during an absence of the ISO.

Performs log scans of the MULES system for investigations, possible misuse, or administrative purposes. Provides peer-level review of results from other security unit log scans.

Performs programming and application development, creates and develops 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 ISO approval.

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

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.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES:

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

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

Thorough knowledge of the CJIS Security Policy

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

Thorough knowledge of agency's automated information systems.

Thorough knowledge of agency's functions and their interrelationships.

Thorough knowledge of the principles of disaster recovery.

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

Thorough knowledge of cyber-incident response management.

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

Thorough knowledge of encryption methods and VPN technologies.

Thorough knowledge of cyber-threat analysis.

Thorough knowledge of computer security systems and procedures.

Considerable knowledge of software reference libraries and related utility programs.

Considerable knowledge of computer networking and telecommunications.

Considerable knowledge of computer operating systems.

Considerable knowledge of database management systems.

Considerable knowledge of advanced authentication solutions.

Considerable knowledge of applicable FIPS encryption standards.

Considerable knowledge of applicable statutes and CFR.

Working knowledge of the principles of cost benefit analysis.

Working knowledge of the principles of project management.

Working knowledge of the procurement process.

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

Working knowledge of various computer platforms.

Working knowledge of the information strategic planning process.

Working knowledge of the systems management process.

Working 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 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 four year degree in Information Security, Cybersecurity, Information Assurance, Information systems or related field or four years of experience in the information security, cybersecurity, or information assurance fields. Knowledge of all areas of information security is needed such as: 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

AND

Two years of experience as a Computer Information Technology Specialist I - Security Unit or comparable position working directly in the field of information security.

Current Certification as a CISA and/or work experience in the fields of information security or information technology is highly desired.

NECESSARY SPECIAL REQUIREMENTS:

Must possess and maintain a MULES Certification within one year of hire.

Must be a United States citizen.

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.