



Classification: Computer Information Technology Specialist I (CITS I)
Information Security Unit - Intelligence

Title Code: V08004

Pay Range: 30

POSITION SUMMARY:

This entry level position provides professional and technical expertise as it relates to information security intelligence. The position works closely with the Information Security Officer as well as staff within the Missouri State Highway Patrol's troops and divisions, and local criminal justice agencies 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 position prepares cybersecurity policies and procedures, and presents cybersecurity topics and briefings to Patrol and local criminal justice staff. This 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.)

Performs highly technical analysis of cyber related intelligence from a number of disparate data sources; disseminates reports as appropriate according to their classification level to the Patrol and various partners.

Cross references cyber intelligence data with indicators from various security related tools to assist the Patrol's Security Operations Center staff with system/network defense.

Provides support to both MSHP and partners in regards to implementing highly complex cybersecurity issues.

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

Assists with preparing and participating in presenting cybersecurity information through written documentation and oral presentation to different types of audiences; this includes meeting with technical and business staff of criminal justice agencies

Performs log scans of the MULES for investigations, possible misuse, or administrative purposes.

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

May assist with investigating security incidents, which may include misuse of official information; utilizes sophisticated software, hardware, and highly technical methods to investigate the incidents.

May assist with performing programming and application development, creating and developing reports and forms as needed.

Develops, updates, and maintains the IT security audits based upon the CJIS Security Policy, statutory and regulatory requirements and industry standards.

Participates in computer systems disaster recovery plan maintenance and implementation for MSHP.
Performs security testing and monitors the MSHP security infrastructure.

Classification: Computer Information Technology Specialist I (CITS I)

Title Code: V08004

Pay Range: 30

Page 2

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

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

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES:

Knowledge in all areas of cybersecurity as well as networking, application development, server software and hardware.

Knowledge of the principles of information security and information technology systems analysis, design, testing and documentation.

Knowledge of the general operating principles and capabilities of computer hardware and software.

Knowledge of the elements of cybercrime and threat indicators.

Considerable knowledge of software reference libraries and related utility programs.

Considerable knowledge of computer security best practice standards.

Considerable knowledge of computer networking protocols.

Considerable knowledge of computer operating systems.

Considerable knowledge of data protection methods.

Working knowledge of national information sharing tools and techniques.

Working knowledge of agency's functions and their interrelationships.

Working knowledge of the principles of cost benefit analysis.

Working knowledge of the principles of project management.

Working knowledge of the principles of disaster recovery.

Working knowledge of continuing trends and developments in information technology and cybersecurity.

Working knowledge of various computer platforms.

Working knowledge of the information strategic planning process.

Working knowledge of the systems management process.

Possess good organizational skills.

Possess research and analysis skills.

Ability to utilize highly technical analytical tools.

Classification: Computer Information Technology Specialist I (CITS I)

Title Code: V08004

Pay Range: 30

Page 3

Ability to prepare and interpret system configuration documentation.

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

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 create and present materials for training programs.

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.

Current Information Security related Certification and/or work experience in the fields of information security, information technology and/or cyber/criminal intelligence work is highly desired.

NECESSARY SPECIAL REQUIREMENTS:

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

Must be a United States citizen.

Must obtain a secret level Department of Homeland Security background/clearance or other federal background/clearance of equal security level.

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.