CONFIDENTIAL INVESTIGATOR (COMPUTER CRIMES)

DISTINGUISHING FEATURES OF THE CLASS: This is highly sensitive and confidential work primarily involving responsibility for providing advice to the Rockland County District Attorney regarding computer crime investigations and for conducting computer forensic investigations. This work may include cases related to child pornography and internet crimes against children, financial fraud, terrorism, public corruption, and other confidential matters, etc. The work is performed under the direction of the Rockland County District Attorney. Does related work as required.

TYPICAL WORK ACTIVITIES:
Analyzes computer crime investigations to offer insights and propose policies and procedures concerning forensic investigations and related matters;
Performs computer forensic investigations, including gathering financial fraud intelligence, monitoring active terrorism, analyzing criminal internet usage, addressing public corruption, and handling confidential matters;
Prepares reports on evidence and data and other reports, as assigned;
Detects similarities among offender, suspect, and victim profiles and offers insights to the District Attorney;
Facilitates the collection and exchange of information with various law enforcement agencies and other sectors within the criminal justice community;
Compiles diverse studies, reports and relevant information;
May review, analyze and categorize calls for service, crime and arrest data and prepares reports according to geographical region;
May identify emerging or existing crime problems and patterns;
May testify in court regarding information recovered during computer investigations.

FULL PERFORMANCE KNOWLEDGE, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS:
Thorough knowledge of the principles and techniques of computer forensic investigations; good knowledge of the principles, methods and techniques used in data collection and crime analysis*; working knowledge of the criminal justice system and criminal behavior, as it pertains to computer crime*; ability to collect, analyze and evaluate data as it pertains to computer crimes; ability to understand and interpret written material; ability to organize material and prepare effective narrative reports; ability to communicate effectively, both orally and in writing; ability to operate a personal computer and utilize standard office software programs (e.g. word processing, spreadsheet and databases)*; ability to establish and maintain cooperative relations with others.

MINIMUM QUALIFICATIONS: A Bachelor's degree in Computer Forensics, Cyber Security, Criminal Justice, Criminology, or comparable curriculum, and two (2) years of technical and/or professional experience in computer forensic investigations.

NOTES:
1. A Master's degree in Computer Forensics, Cyber Security, Criminal Justice, Criminology, or comparable curriculum may be substituted for one (1) year of the required experience.

2. Additional years of the required experience may be substituted for the Bachelor's degree on a year-for-year basis, up to four (4) years.

3. Thirty (30) credits in Computer Forensic courses (including Computer Forensic certification programs), or comparable curriculum, may be substituted for the Bachelor's degree.

SPECIAL REQUIREMENT:
Must have at least two (2) of the following certifications: Computer Forensic Certified Examiner (CFCE), Seized Computer Evidence Recovery Specialist (SCERS), Certified Fraud Examiner (CFE), Encase Certified Examiner (EnCE).

*To be demonstrated during the probationary period.

R.C.D.P   (07.15.2015)   04.09.2024
PJC/Non-competitive (Confidential/Policy influencing)