DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL
OFFICE OF GENERAL COUNSEL
OFFICE OF INFORMATION SECURITY & RESEARCH SERVICES
INFORMATION SECURITY BRANCH
NETWORK INFORMATION SECURITY UNIT

JOB TITLE: Information Security Specialist (ITS II)

POSITION NUMBER: 420-916-1414-001

INCUMBENT:

PRIMARY DOMAIN: Information Security Engineering: The security aspects of the initiation, design, development, testing, operation, and defense of information technology data and environments.

STATEMENT OF DUTIES: Under direction of the Information Technology Manager I (ITM I) in the Network Information Security Unit (NISU), the Information Technology Specialist II (ITS II) performs at the mastery level of this career series, directing the largest and most complex projects and initiating key actions on a wide variety of complex security related tasks. The incumbent performs various information security related tasks to ensure Department of Justice (DOJ) information security posture is in place. The ITS II utilizes various security solutions for performing functions such as vulnerability testing for all DOJ systems and participating on the DOJ Incident Response Team. The incumbent acts as a key participant on all technical matters and performs information security related duties in support of the DOJ mission. The incumbent works with the Electronic Recording Delivery System (ERDS) Program by both performing onsite inspections and conducting technical security audits of County Recorders' ERDS systems. The incumbent reviews and analyzes ERDS regulations and processes and provides recommendations for compliance.

The ITS II acts as a team member with other highly skilled IT Specialists and analysts and as a consultant and resource in support of the DOJ's Information Technology (IT) security infrastructure and investigations.

SUPERVISION RECEIVED: Under the general supervision of the Information Technology Manager I (ITM I).

SUPERVISION EXERCISED: None.

TYPICAL PHYSICAL DEMANDS: Ability to sit at a computer terminal for extended periods of time. May be required to lift, carry, or move up to 20 pounds.

TYPICAL WORKING CONDITIONS: In a remote work environment, home office, or similar environment in California. At the office, an enclosed windowed office with a smoke-free environment. May be required to sit at a computer terminal while performing research and other duties up to eight hours a day. Travel to designated offices may be required.

ESSENTIAL FUNCTIONS:

50% Provides regulatory and policy oversight including ERDS regulation review and updates for the ERDS to ensure the regulations with which County Recorders must comply are kept current with security standards and best practices. Provides onsite technical security inspections and auditing of the county recorder's ERDS system which requires statewide travel. Ensures County Recorder ERDS systems are compliant with DOJ Electronic Recording Delivery Act (ERDA) regulations. Acts as a technical security expert specialist in support of the DOJ ERDS Program. Audits the security controls of ERDS systems and their associated processes including, but not limited to, the technical review of desktop and server systems. Documents all findings and provides them to the ERDS program. Reviews County Recorders' responses to audit findings to ensure issues are addressed. Collaborates with ERDS program on regulations and audit findings, and provides assistance and direction as needed. Attends all ERDS Program and committee meetings.

Provides technical security review of criminal justice agencies' California Law Enforcement Telecommunications System (CLETS) applications for adherence to federal and state requirements. Provides expert specialist level technical direction to help determine CLETS security requirements and write CLETS security policy papers. Serves as a liaison between the DOJ and CLETS agencies to coordinate security requirements. Coordinates the Federal Bureau of Investigation (FBI) IT Security Audits. Provides training and consultation for DOJ's CLETS Administration Section and input on DOJ's NexTEST testing system. Provides technical security review of criminal justice agencies' MobileID applications for adherence to federal and state requirements.

40% Deploys, operates and securely maintains the security systems that support the Cybersecurity Branch mission. This includes:

- Implementing new security systems and performing various security system integration activities.
- Troubleshooting to ensure security systems are operationally sound.
- Monitoring and managing the more complex and critical Security technologies including but not limited to: 0- day and Advanced Persistent Treat (APT) (sandboxing, behavioral monitoring, etc.) packet capture and metadata analytic systems, Data Lost Prevention (DLP) technologies, email hygiene systems, vulnerability scanning, etc.
- Producing reports as instructed or as needed to adequately reflect performance and activities of the Cybersecurity Branch with regards to cybersecurity operations.
- Providing input to supervisor and/or security management on improvements that can be made to Cybersecurity branch operations and participating in those initiatives or efforts as required.
- Participating in systems evaluations and security audits of DOJ systems with the OGC/ISRS/Security Risk Management Unit.

- Analyzing and resolving events and incidents that are reported by end users or are observed through proactive network and system monitoring. Responding to incidents as an active participant in security incident response teams.
- Keeping abreast of the actions adversaries may take in order to prevent unauthorized access to DOJ's systems. Acting as a participant, along with the management and technical staff on the DOJ Incident Response Team (IRT), which requires planning, discussions, needs analysis and business risks. Participating in the design, development, and implementation of departmental and NISU Information Security plans, policies, and procedures. Formulating IT strategy and determining technologies needed to keep DOJ secure from latest tactics, techniques and procedures of threat actors. Performing and reviewing security vulnerability assessment on Departmental IT infrastructure.

10% Serves as one of the lead administrators for the Department's online security awareness training program including onboarding new DOJ employees and updating annual training modules.

Develops and maintains a working level knowledge of:

- Threat awareness, malicious actor techniques, indicators of compromise, analytic techniques and methods, and State of California workflow processes.
- Operating systems, network architecture and protocols security devices, database management systems, system design, implementation, and testing, as well as interoperability and interdependency issues.
- Security best practices and regulatory requirements. This requires attending formal training and conferences as well as personal research of periodicals, journals, the Internet, etc.

I have read and understand the essential functions and typical physical demands required of this job (please check one of the boxes below regarding a Reasonable Accommodation):

☐ I am able to complete the essential functions and typical physical demands of the job without a need for a reasonable accommodation.

☐ I am able to complete the essential functions and typical physical demands of the job, but will require a reasonable accommodation. I will discuss my reasonable accommodation request with my supervisor.

☐ I am unable to perform one or more of the essential functions and typical physical demands of the job, even with a reasonable accommodation.

☐ I am not sure that I will be able to perform one or more of the essential functions and typical physical demands of the job, and will discuss the functional limitations I have with my supervisor.

I have read and understand the duties and essential functions of the position and can perform these duties with or without reasonable accommodation.

Employee's Signature Date	Supervisor's Signature Date