

**CALIFORNIA DEPARTMENT OF TRANSPORTATION (CALTRANS)
DUTY STATEMENT**

CLASSIFICATION TITLE Senior Information Systems Analyst (Specialist)	DISTRICT/DIVISION/OFFICE D20/Information Technology/Security and Network Services Division	
WORKING TITLE Senior Forensics Specialist	POSITION NUMBER 900-170-1337-924	EFFECTIVE DATE

As a valued member of the Caltrans team, you make it possible for the Department to provide a safe, sustainable, integrated, and efficient transportation system to enhance California's economy and livability. The Department of Transportation is a performance-driven, transparent, and accountable organization that values its people, resources and partners, and meets new challenges through leadership, innovation and teamwork.

GENERAL STATEMENT:

Under the general supervision of the Assistant Information Security Officer, Systems Software Specialist II (Supervisory), incumbent is responsible for conducting digital forensics and technical analysis on technology systems and information assets in response to Departmental requests. The Senior Information Systems Analyst (Specialist) will lead and conduct digital forensic analysis on technology and information assets. The incumbent will document, research, develop reports and present forensic findings. The incumbent will preserve the chains of custody and evidence and represent the Department as expert witness in hearings and trials as a result of digital forensics investigations.

The incumbent is knowledgeable of the applicable Federal National Institute of Standards and Technology (NIST) policies, State Administrative Manual (SAM), the Department's Information Security policies and other security related policies such as Payment Card Industry (PCI) Privacy and the Healthcare Information Portability and Accountability Act (HIPAA).

TYPICAL DUTIES:

Percentage
Essential (E)/Marginal (M)

45% E The incumbent is the lead responsible for conducting forensic and technical analysis on technology and information assets in response to Department requests. The Senior Forensics Specialist will lead, research, and conduct forensic analysis on technology and information assets by detecting causes and/or violations of data security and policies and procedures, including workstations, laptops or personal computers, applications, software, hardware, and mobile devices. The incumbent will document, create reports and present forensic findings to the Information Security Officer, Senior Management, and Control Agencies.

15% E The incumbent will train Department staff in forensic data capture and high-level analysis and create precise procedures to preserve the chain-of-custody of evidence. The incumbent will provide leadership, instruction, and guidance during and after work hours to support staff. The incumbent will represent the Department as expert

witness in hearings and trials as a result of forensic and technology investigations as needed. The incumbent will use, maintain, and develop forensic software, hardware, and tools. The incumbent will evaluate and purchase equipment, tools, software, and supplies to support the Forensics Unit.

- 20% E Incumbent will develop and maintain metrics, systems, and processes for reporting, documenting, and coordinating responses to incidents. Monitor and review logs related to the operation and security of the Department's information assets, including the Internet, systems and equipment. Review and approve or deny non-employee access to the Department's information assets and maintain accurate logs.
- 10% E The incumbent will be knowledgeable of and evaluate project management documents to ensure appropriate security controls to meet the Department's information security policies, standards, industry best practices, regulations, and State and Federal policies and laws. The incumbent is responsible for special projects.
- 5% M Incumbent will participate in the Department's Cyber Incident Response Team.
- 5% M Incumbent will travel to the Department's twelve (12) District offices and other facilities to conduct forensic analysis.

SUPERVISION EXERCISED OVER OTHERS:

None. The employee will serve in a lead role, as a subject matter expert, and as a project leader to other staff and consultants assigned to the project under his/her span of control.

SUPERVISION RECEIVED

Reports to the Systems Software Specialist II (Supervisory), Assistant Chief Information Officer, and receives general direction to perform job duties.

SPECIAL REQUIREMENT:

In the event of a forensic case or trial, the employee may be required to work extended hours.

DESIRABLE EXPERIENCE/QUALIFICATIONS:

Certified Computer Examiner (CCE) or equivalent digital forensic certification.
Certified Information Systems Security Professional (CISSP) or equivalent information security certification.

KNOWLEDGE, ABILITIES AND ANALYTICAL REQUIREMENTS:

The incumbent must possess the ability to communicate in verbal and written format clearly, concisely, and in a manner that is easily understood by technical and non-technical staff including the ability to develop and document new processes. Excellent customer service and interpersonal skills are required to ensure effective communication with all levels in the organization as well as internal

and external customers. The incumbent must lead, develop and maintain effective working relationships with business customers, technical staff and co-workers. The incumbent must be dependable, discreet, and organized. The incumbent must be able to make rational and feasible decisions and effectively evaluate the results and consequences..

Knowledge of:

The incumbent must have a full understanding of forensic and information security technologies and products. The incumbent must have knowledge of electronic computer operating systems and applications; networking concepts, telecommunications; and Information Technology (IT) equipment.

The incumbent must be knowledgeable of the Federal NIST, Government Code, Penal Code and SAM sections regarding forensics and information security.

Ability to:

The incumbent must have the ability to analyze data; develop detailed documentation; reason logically and creatively to identify and resolve problems; the ability to participate in and perform systems analysis, cost/benefit analysis and risk analysis. The incumbent is expected to work independently as a technical expert, as part of a team on complex security and forensic issues, and interacts with all levels of management, internally and externally.

The incumbent must have the ability to establish and maintain cooperative relationships with other agencies, vendors and contractors; communicate effectively with technical and non-technical staff, both verbally and in writing; extend excellent customer service and interpersonal skills to ensure effective communication with all levels in the organization; provide leadership and guidance during and after work hours; work within a team environment that spans multiple disciplines; and work independently.

Analytical Requirements:

The incumbent must have a level of analytical ability and expertise to permit the employee's exercise of sound judgment. The incumbent must work well under pressure; effectively manage changing priorities and handle concurrent assignments; have a level of spelling, grammar, punctuation and Modern English usage, math and algebraic applications for use in development of documentation, cost/benefit analyses, metrics, and thorough deliverables.

CONSEQUENCE OF ERROR/RESPONSIBILITY FOR DECISIONS:

The Department will depend on the Senior Information Systems Analyst's work products to effectively and successfully implement the Departments IT Security and Network Services strategic goals and objectives. Failure to implement these objectives properly will cause the Department of Transportation to be out of compliance with regards to data security.

The incumbent will make recommendations and provide Forensic analysis that will impact and effect the operations of the Security and Network Services Division and the Forensics Office. Recommendations will influence Department policy, information security policy and practices.

PUBLIC AND INTERNAL CONTACTS:

The incumbent will routinely be in contact with members of the Department's management and staff and contractors. The incumbent will also be in contact with Federal, State and Local government agencies, control agencies and vendors.

PHYSICAL, MENTAL AND EMOTIONAL REQUIREMENTS:

The incumbent may be required to sit for long periods of time using a keyboard, video display terminal and telephone. The incumbent must be physically able to maneuver (lift, move, etc.) equipment. Incumbent must be able to travel throughout the State of California by a variety of modes of transportation.

Mental requirements include: openness to change and new information; ability to adapt behavior and work methods in response to new information, changing conditions, or unexpected obstacles. Employee must have the ability to multi-task, to adapt to changes in priorities, and complete tasks or projects with short notice.

Emotional requirements include: ability to value cultural diversity and other individual differences in the workforce; ability to adjust rapidly to new situations warranting attention and resolution; ability to consider and respond appropriately to the needs, feelings, and capabilities of different people in different situations; ability to be tactful and treat others with respect.

WORK ENVIRONMENT:

While at their base of operation, employee will work in a climate-controlled office under artificial lighting. The incumbent will be required to work for limited amounts of time in high noise level computer rooms with lower than normal temperatures. Employee may also be required to travel to district and outlying offices to conduct analyses and/or training.

I have read, understand and can perform the duties listed above. If you believe you may require accommodation, please discuss this with the hiring supervisor.

Employee's Name	Date	Employee's Signature	Date
-----------------	------	----------------------	------

I have discussed the duties with and provided a copy of this duty statement to the employee named above.

Victoria Craig Supervisor's Name (please print)	Supervisor's Signature	Date
---	------------------------	------