

POSITION DUTY STATEMENT

PM-0924 (REV 7/2014)

CLASSIFICATION TITLE Associate Information Systems Analyst	OFFICE/BRANCH/SECTION IT/Security & Network Services/ Information Security Office	
WORKING TITLE Associate Information Security Analyst	POSITION NUMBER 900-170-1470-nnn	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. Caltrans 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 direct supervision of the Assistant Information Security Officer in the Information Security Office (Office) within the IT Security and Network Services Division, the incumbent is responsible for working with Office staff across information security domains. The incumbent will work cooperatively with staff, coordinate data collection and analysis from disparate sources for event analysis and reporting and in support of forensic investigations, and conduct outreach to the Department to support the Department's Information Security Program. Areas of responsibility will include annual information security training, incident response and reporting, technology recovery planning, security compliance monitoring, analysis and review. The incumbent will participate in Department, IT, and Security projects, and research and develop applicable security policy.

TYPICAL DUTIES:

Percentage		Job Description
Essential (E)/Marginal (M) ¹		
45%	E	The incumbent will work collaboratively as a team member of the Office by conducting research in security and information technology, performing analysis, and applying broad knowledge of information technology and security practices, and participating in Information Security projects and programs. Such collaborative work will span information security methodologies and knowledge areas (Access Control; Architecture and Design; Business Continuity and Technology Recovery; Data Security; Forensics; Governance; Incident Management and Response; Network and Telecommunications; Policy Development and Compliance; Risk Management; Software Development).
40%	E	The incumbent will participate in the development and execution of Department Security Program including developing and calculating metrics and statistics, monitoring and reviewing logs related to the operation and security of the Department's network, information systems and equipment. Additional duties include preparing and presenting reports on the security, integrity and availability of information systems.
10%	E	The incumbent will develop and implement the Information Security Training Plan including preparation, dissemination, and maintenance of training materials. The incumbent will administer the Department Information Security on-line training and coordinate training completion information with the Department's Learning Management System. The incumbent will provide various reports to the Chief Information Security Officer, Management and supervisors in the Department. The incumbent will design, develop and maintain the content for the Caltrans Information Security Website. Activities include but are not limited to: working with key personnel to identify relevant content and preferred presentation, including improving design and adding features to the site, and maintaining the integrity of site information.
5%	M	Incumbent will participate in the Department's Cyber Incident Response Team. Incumbent will travel to the Department's twelve (12) District offices and other facilities; and training classes as deemed necessary.

¹ESSENTIAL FUNCTIONS are the core duties of the position that cannot be reassigned.

MARGINAL FUNCTIONS are the minor tasks of the position that can be assigned to others.

POSITION DUTY STATEMENT

PM-0924 (REV 7/2014)

SUPERVISION OR GUIDANCE EXERCISED OVER OTHERS

None

KNOWLEDGE, ABILITIES, AND ANALYTICAL REQUIREMENTS

- Familiarity with and broad understanding of computerized information processing systems, networks, system development life cycle (SDLC) and project management.
 - Understanding of business processes and business drivers of technology solutions and change.
 - Ability to participate in and perform systems analysis and risk assessments.
 - Ability to communicate with technical and non-technical staff in verbal and written form.
 - Excellent analytical and problem solving abilities along with the skills and knowledge to produce completed staff work.
 - Strong communication, presentation, negotiation, and relationship building skills. The incumbent must be skillful in approaching individuals or groups in order to obtain the desired results (e.g., obtain agreement where there is controversy and dissimilar goals.)
 - Ability to show initiative and to work both independently and in a team environment and produce well-documented results.
 - Spelling, grammar, punctuation, and Modern English usage; math and algebraic applications cost/benefit analysis and performance measurement
 - Effectively adjust to changing priorities and able to handle concurrent assignments.
 - Perform policy analysis in order to evaluate established methods and procedures and prepare recommendations for changes in methods and practices.
 - Familiarity with the Government Code, Penal Code, Federal and State Administrative Manual policy sections regarding Information Security and Privacy.
 - Familiarity with technology recovery processes and strategies for business recovery and continuity.
-

RESPONSIBILITY FOR DECISIONS AND CONSEQUENCES OF ERROR

The incumbent will make recommendations concerning the security and availability of Department information assets. The effect of those recommendations will affect the efficient and effective operation and performance of the Security and Network Services Division and the Department. Recommendations will influence Department policy and potentially operations. Failure to perform could result in the loss of departmental information assets and department trust.

PUBLIC AND INTERNAL CONTACTS

The incumbent will routinely be in contact with members of the Department's management, staff and the IT Division. Additionally the incumbent will interact with the State Information Security Office, control agencies, staff from State of California Departments performing similar duties and vendors or outside consultants who may be providing IT services to the Department.

PHYSICAL, MENTAL, AND EMOTIONAL REQUIREMENTS

The incumbent may be required to respond to technical emergency incidents that require extended work hours. The incumbent must be able to communicate orally and in writing to all levels of Department staff. Incumbent must be physically able to travel throughout the State by any mode of transportation (e.g. aircraft, train, bus, taxi, rental car, etc). The incumbent may be required to sit for long durations using a telephone, keyboard, and video display terminal.

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. Incumbent must have the ability to multi-task, to adapt to changes in priorities, and complete tasks or projects with short notice; provide leadership and guidance during and after work hours. Sustained mental activity is needed for planning, response, and recovery of technical disaster events and incidents, including the ability to focus on problem solving and analysis.

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. Additionally the incumbent must be dependable, organized and punctual.

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.

POSITION DUTY STATEMENT

PM-0924 (REV 7/2014)

I have read, understand and can perform the duties listed above. (If you believe you may require reasonable accommodation, please discuss this with your hiring supervisor. If you are unsure whether you require reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Reasonable Accommodation Coordinator.)

EMPLOYEE (Print)

EMPLOYEE (Signature)

DATE

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

SUPERVISOR (Print)

SUPERVISOR (Signature)

DATE
