CMD 900-54
(Rev. 09/2024)

DUTY STATEMENT

☐	Current
☐	Proposed

Position Classification: Information Technology Specialist I	**Working Title:** Security Analyst
Position Number: 006-177-1402-xxx	**CBID:** R01
Work Week Group: 2	**Work Hours:** 8:00 am – 5:30 pm
Command/Directorate/Unit: J6 – State Network Team - Security	**Physical Work Location:** 10601 Bear Hollow Drive, Rancho Cordova, CA 95670
Supervisor Name: Kalani Mertyris	**Supervisor Classification/Rank:** Information Technology Manager I
Current Incumbent:	**Effective Date:**

Position Requirements:

☐ Conflict of Interest Filer (Form 700)
☐ California Driver's License
☐ Class A ☐ Class B ☐ Class C
☐ Class C w/Endorsement: _____

☐ Travel to Multiple Locations
☒ Occasional Travel
☐ Other (Specify): _____

As an employee of the California Military Department (CMD), you are required to perform the essential functions of the position with or without reasonable accommodation. The incumbent is also expected to work cooperatively with internal staff/external partners and treat others fairly, honestly and with courtesy and respect. In addition to providing the highest level of customer service while meeting the CMD mission.

Position Identification:
Under the general direction of the Information Technology Specialist II, Security Engineer, the Information Technology Specialist I (ITS I), Security Analyst will perform risk assessments to identify, manage, and mitigate infrastructure architecture risk with potential to impact business objectives. The incumbent shall work with the CMD Information Security Officer (ISO) to perform duties related to Information Security Engineering, including, but not limited to: Incident Management, Privacy, Security Compliance, Security Risk Management, and development of policies, procedures, and training. The incumbent will also be responsible for evaluating incoming Risk Assessments and advising, accordingly, programs on security risks and mitigating controls. The ITS I will interface with management, team members, and vendors to develop and implement new solutions to meet business requirements. Additional duties will include developing/maintaining information security plans, policies/standards, as well as analyzing incoming suspicious emails and make recommendations to stakeholders. The ITS I will further develop, deliver, and maintain the information security awareness training to the State Workforce. The incumbent will perform incoming Legal Hold, Data Loss Prevention and computer investigations, as well as provide security expertise in areas including, but not limited to, System Development Life Cycle (SDLC) and contract language for security provisions.

Essential Functions:

30%	**System and Infrastructure Engineering**. Research, assess, evaluate, implement, and document security changes and implementations to manage the CMD Information Security posture. Assess the CMD Information Security Program for compliance with applicable laws, regulations, and established security frameworks and standards from National Institute of Standards and Technology (NIST) Special Publication 800 and California Department of Technology (CDT), identifying gaps and recommending remediation as needed. Provide support and guidance to patch management and incident remediation. Support and maintain security standards consistent with and in compliance with State Administrative Manual (SAM), State Information Management Manual (SIMM), CDT, and CMD policies and regulations and industry standards. Support secure cloud practices to support the CMD's expanding cloud infrastructure. Document best practices, security guidelines, training materials, plans, processes, procedures, and manuals in response to existing and new technology that have been deployed.
30%	**Vulnerability Management.** Performs information security continuous monitoring program activities utilizing a wide array of security tools. Maintain a host-hardening process for image hardening of switches,

	routers, firewalls, servers, workstations (desktop and laptops), and other network and user devices; conduct vulnerability scans of CMD systems; conduct ongoing system and account access audits; and respond to external data sources regarding CMD assets. Analyzes business impact and exposure based on emerging security threats, vulnerabilities, and risks, and recommends and develops solutions to mitigate risks. Complete all State, CDT, and CMD directed and implied audits and reports.
20%	**Incident Remediation and Triage**. Respond to incidents, fully document, and facilitate remediation. Utilize query languages to investigate security events, correlate logs, and support timely incident response. Work as a cooperative team member with all information technology staff and grow an environment that is easier to manage and troubleshoot for all teams. Build alerts, dashboards, and other tools to provide enhanced system management and visibility. Interface with the state information security office via mandated incident reporting portals, email, and other communications methods. Review and investigate notable events based on correlation searches and analyzes, assesses, and reports findings to the ISO. Requires occasional weekend availability to check email and provide timely responses to CDT Security Operations Center alerts when necessary.
10%	**Research and Continuous learning.** Research and evaluate new technology releases for hardware and software and make recommendations for systems and equipment that would allow the CMD to meet its information technology goals. Ensures security tools and systems are functioning effectively and efficiently, managing issues, problem resolution, troubleshooting, and patch management, and participates in the change management process. Maintain a working knowledge of current information security events and trends. Make use of all available training opportunities to grow and share that knowledge with coworkers. Develop training materials and manuals for users and technical staff regarding security and support functions; training staff on security technologies or topics; lead technical reviews or seminars that increase staff awareness and knowledge regarding specific CMD security policies and procedures; provide knowledge transfer to management and technical staff on security technologies employed at the CMD. Attend annual security exercise and training provided by CMD and external seminars.
5%	Privacy Program Coordinator Back-Up. Back-up point of contact for privacy complaints and record of handled complaints, meeting agendas and minutes for reviews with business areas and project teams, documentation for internal auditors or independent third-party reviews, etc.). Perform necessary Privacy Impact Assessments (PIAs) and Privacy Threshold Assessments (PTAs) for CMD information systems.

Non-Essential/Marginal Functions:

5%	• Other duties as assigned.

Knowledge, Skills, and Abilities:

Knowledge of:
Principles, techniques, and procedures related to the delivery of information technology services; the System Development Lifecycle including the associated methodologies, tools, and processes; the organization's business processes and procedures; education tools and techniques; performance monitoring tools and techniques; and data administration techniques and best practices.

Skills: N/A

Ability to:
Use initiative; act independently with flexibility and tact; use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems; perform technical analysis of proposed technology solutions; comprehend technical documents to interpret specifications, system implementations, capabilities, interdependencies, and compatibilities; serve as a technical liaison; develop and effectively utilize all available resources; develop end-user training materials; and gather data to perform statistical analysis and report outcomes.

Required Qualifications:

Desirable Qualifications:

Applicants must demonstrate the ability to perform with a high level of administrative and policy expertise – serving as a highly independent non-supervisory manager. Such overall ability requires possession of the following specific knowledge and abilities:

- Knowledge of Principles, practices, and trends of public and business administration, including management and supportive management analysis, planning, program evaluation, or related areas; principles and practices of policy and plan development, and training; program management; formal and informal aspects of the legislative process; the administration of the department's goals and policies; governmental functions and organization at the State and local level.
- Exercise knowledge and application in evaluation, measurement and data collection techniques in support of performance management and process improvement; use analytical and problem-solving skills; and familiarity with concepts of establishing policy and procedures, planning, and process improvement strategies and tools.
- Ability to investigate security events, analyze logs, and support incident response using Kusto Query Language or have general knowledge of query languages.
- Reason logically and creatively and utilize a variety of analytical techniques to resolve complex governmental and managerial problems; develop and evaluate alternatives; analyze data and present ideas and information effectively both orally and in writing; consult with and advise administrators or other stakeholders on a wide variety of subject-matter areas; gain and maintain the confidence and cooperation of those contacted during the course of work; review and edit written reports, utilize interdisciplinary teams effectively in the conduct of studies; manage a complex Staff Services program; establish and maintain project priorities; develop and effectively utilize all available resources.
- Establish and maintain cooperative working relationships with staff at all levels both within and outside the CMD to complete work assignments related to policies and plans.
- Ability to independently make decisions and perform actions having broad implications on various aspects of policies and plans.
- Assume and demonstrate independent responsibility for decisions and actions having departmental impact on various aspects of policies and plans.
- Ability to give presentations to and interact with a wide range of audiences, facilitate workgroups to accomplish goals, and design and deliver systematic training tailored to the needs of stakeholders.
- The incumbent must demonstrate the ability to use internet, email, desktop applications and presentation software to complete assignments.
- Develop and maintain knowledge and skills related to specific tasks, methodologies, materials, tools, and equipment.
- Complete assignments in a timely and efficient manner; adhering to department policies and procedures.
- Knowledge of State Civil Service processes, trends, techniques, and technology.
- Experience providing technical guidance related to the drafting and implementation of policies and plans and various strategies, including interpretation of laws, rules and regulations.
- Ability to be dependable, flexible, open minded, patient, professional, and tactful.
- Ability to think creatively and logically; analyze and solve difficult technical problems; provide sound recommendations and solutions; analyze data and present ideas and information effectively to leaders and stakeholders; meet established project deadlines.
- Willingness to work in a military environment.

Work Environment:

- Occasional travel to work sites, training, etc., may be required.
- Work is primarily sedentary in a temperature-controlled office environment.

Physical/Mental Abilities:

- Able to walk, stand, bend, or carry light items, such as small boxes, files, etc.

- Ability to be dependable, flexible, patient, professional, and tactful.
- Ability to communicate both verbally and in writing, think clearly and creatively, and give recommendations.
- Ability to meet established project deadlines.
- Ability to solve complex problems, analyze and present information clearly, communicate effectively, advise others, lead teams, manage programs, set priorities, and use resources efficiently.
- Ability to give presentations, facilitate workgroups, and design and deliver training.

Equipment Used:

- Telephone, computers with office automation, printer, keyboard, mobile devices (iPad, iPhone, etc.) Telecommunications and electronics equipment; personal and commercial vehicles

Employee Certification:

This duty statement reflects the typical duties of the essential functions described for the position. It is not considered an all-inclusive list of work requirements. I have read and discussed the duties of this position with my supervisor and understand I may perform other duties as assigned, including but not limited to, work in other functional areas to cover absences, peak work periods, or balance workload.

I certify I possess qualifications, including but not limited to, integrity, initiative, dependability, good judgment, and the ability to work cooperatively with others. Additionally, I am able to perform the assigned duties with or without reasonable accommodation. Should I have any concerns performing the assigned duties, I will discuss them with the hiring manager who will provide information for the Return-To-Work Coordinator.

I have read the duty statement and discussed the duties with my supervisor.

Employee Name (Print)	**Signature**	**Date**

Supervisor Statement:
I have discussed the duties outlined in the duty statement and provided a copy to the employee.

Supervisor Name (Print)	**Signature**	**Date**

State Personnel Office Use Only

State Personnel Certification: Approval

C&P Analyst Name (Print)	**Signature**	**Date**