



**DEPARTMENT OF MOTOR VEHICLES
POSITION DUTY STATEMENT**

702-1402-013

ACTIVE

CURRENT
 PROPOSED

1. DIVISION Information Systems Division		2. REGION OR BRANCH Information Security Services Branch	
3. REPORTING UNIT NAME Information Security Office		4. POSITION CITY Sacramento, CA	
5. CLASSIFICATION TITLE Information Technology Specialist I		6. WORKING TITLE Security Analyst	
7. POSITION NUMBER 702-1402-013		8. PREVIOUS POSITION NUMBER	
9. CBID/BARGAINING UNIT R01	10. WORK WEEK GROUP E	11. TENURE Permanent	12. TIME BASE Full-Time

13. CONFLICT OF INTEREST CLASSIFICATION (GOV. CODE 87300, ET SEQ.)? Yes No
 This position is designated under the Conflict of Interest Code. This position is responsible for making or participating in the making of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete Form 700 within 30 days of appointment. Failure to comply with the Conflict of Interest Code requirements may void the appointment.

14. CPC ANALYST APPROVAL **T. Cortez-Guardado** **15. DATE APPROVED** **7/29/2021**

Effective on the date indicated, the following duties and responsibilities were assigned to the position identified above.

16. DIRECTION STATEMENT AND GENERAL DESCRIPTION OF DUTIES
 Under direction of the Information Technology Manager I, the Information Technology Specialist I will perform duties related to Information Security Engineering, including, but not limited to: Incident Management, Privacy, Security Compliance, Security Risk Management, and Policy & Procedure Development & Training.

17. ESSENTIAL/MARGINAL FUNCTIONS

Relative % of time required
(in descending order)

- 45% **(E)**
Lead analyst responsible for the administration of the department's information security incident reporting program. Prepares reports designed to identify inconsistencies and develop mitigation strategies to improve the effectiveness of the information security incident reporting process. Applies expert information security incident knowledge to develop new methods and innovative solutions used in responding to complex, multifaceted information security incident challenges. Performs extensive, expert analysis of security incidents to identify trends and shares results with departmental information security liaisons. Reviews, evaluates and reports on enterprise wide risk reporting mitigation efforts to DMV executive and Office of Information Security (OIS) management to ensure the department complies with State Administrative Manual (SAM) section 5300 requirements and standards. Upon request, compiles statistical information security incident information used to response to inquiries received from internal departmental business units, the DMV Privacy Protection Office (DMV PPO) and the Office of Information Security (OIS).
- 25% **(E)**
Lead analyst responsible for the administration, maintenance and updates to the DMV Information Security Office (DMV ISO) incident reporting standard operating procedures (SAP). Perform extensive, expert analysis of DMV Information Security Office (DMV ISO) incident reporting SAPs and process workflows to ensure its alignment and compliance with State Administrative Manual (SAM) and State Information Management Manual (SIMM) policies and procedures. Conducts analysis and interpretation of State Administrative Manual (SAM) Section 5300 and State Information Management Manual (SIMM) incident reporting policies to provide internal departmental business

**DEPARTMENT OF MOTOR VEHICLES
POSITION DUTY STATEMENT**

units and external customers information that is used to incorporate information security practices into their business processes.. Collaborates with DMV internal business units and external customers to conduct various types of incident reporting assessments. Prepares various project and security risk assessment documentation and presents findings and resolutions to DMV internal business units and external customers at various levels.

25%

(E)

Provide expertise, leadership, guidance and training to departmental staff in the areas of information security awareness, incident reporting, risk management, mitigation and business continuity. Works with unit members in providing information security incident reporting subject matter expertise. Collaborates with the departmental headquarters and field office staff, and DMV executives in preparing appropriate information security incident reporting training documentation, other miscellaneous project related information to ensure the confidentiality, integrity and availability of DMV's computing assets complies with departmental, state, federal and information security policies and standards.

5%

(M)

Perform other job-related duties as required.



**DEPARTMENT OF MOTOR VEHICLES
POSITION DUTY STATEMENT**

702-1402-013

18. SUPERVISION RECEIVED

The Information Technology Specialist I is under direction of the Information Technology Manager I.

19. SUPERVISION EXERCISED AND STAFF NUMBERS

None.

20. WORKING CONDITIONS AND PHYSICAL REQUIREMENTS

Works in an office setting, in cubicles with raised and lowered walls. May be sitting and using a computer for long periods.

21. SPECIAL REQUIREMENTS AND DESIRABLE QUALIFICATIONS

Comply with security policies and procedures established by the data owners and the Information Security Officer. Implement the technical means to preserve the confidentiality, integrity and availability of the department's information assets and manage the risks associated with those assets. Advise the data owners and the Information Security Officer of control vulnerabilities and recommendations for alternatives that enhance data security for existing and developing systems.

22. PERSONAL CONTACTS

Will interact with staff from the DMV, other state or government agencies, external entities and contractors by phone, Email, written correspondence, presentation or in-person, as needed. Interactions may be general, informative, technical, confidential, sensitive or private.