DMV

DEPARTMENT OF MOTOR VEHICLES

POSITION DUTY STATEMENT

Division: Information Systems Division	**Classification Title**: 1414 Information Technology Specialist II
Branch: Information Security Services Branch	**Working Title**: Lead Security Analyst
Unit: Information Security Services Branch	**Tenure/Timebase**: Permanent Fulltime
Position City: Sacramento	**Position County**: Sacramento County
Position Number: 702-1414-011	**CBID/Bargaining Unit**: R01

Conflict of Interest Classification: Yes

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.

Medical Evaluation: No	**Bilingual Language**: Unknown
Sensitive Position: No	**DMV Employee Pull Notice**: No
Fingerprint/Live Scan: Yes	**Professional License**: No
Work Week Group: E	**Effective Date**: 10/04/2019

Direction Statement and General Description of Duties: Under general direction of the Information Technology Manager I, the Information Technology Specialist II (Firewall) will perform duties related to Information Security Engineering, System Engineering and Client Services, including but not limited to: Asset Protection, Contingency Planning, Incident Management, Security Engineering and Architecture, Security Operations, Security Risk Management, Security Testing and assessment, Network Operations and Service Desk.

Percentage and Essential/Marginal Functions:

45%	**Monitor, Analyze, Take Action (E)**

	Acts as lead to monitor, analyze and take action on alerts, notifications and findings from hunting campaigns to protect and secure DMV's information assets, systems and infrastructure, on premise and at our data center, from internal and external threats as alerts and notifications are received or as events are discovered. Acts as lead to monitor, analyze and take action on mainframe systems for processing, maintenance, support and fraud correlation as the needs arise. Acts as lead to monitor, analyze and take action on firewall logs to protect and secure information assets, systems and infrastructure at DMV and off premise, from internal and external threats on a daily basis. Provides mentorship to staff in the unit related to this function.
20%	**(E)** Incident Response Acts as lead to initiate incident response to identify, contain and remediate events using all availabletools and resources as the needs arise. Acts as lead to examine equipment such as hard and externaldrives to determine threat or malicious activity or establish forensics as events are requested ordiscovered. Provides mentorship to staff in the unit related to this function.
10%	**(E)** Recommendations Acts as lead to recommend hardening strategies and security best practices to protect and secureDMV's information assets, systems and infrastructure, on premise and at our data center, based onindustry standards and compliance regulations as the needs arise. Provides mentorship to staff in theunit related to this function.
10%	**(E)** Reporting and Documentation Acts as lead to disseminate threat intelligence for information-sharing with internal and external supportareas or entities using all available tools and resources as alerts and notifications are received or asevents are discovered. Acts as lead to create security-related reports to provide metrics for the Security Operations Center (SOC) on a regular basis. Acts as lead to document all actions taken, configurations reviewed, software versions, rule sets, policies, procedures and other relevant information in a secured library to provide a SOC archive on a daily basis. Provides mentorship to staff in the unit related to this function.
10%	**(E)** Installation, Programming and Support Configures and manages security software and hardware to protect and secure DMV's informationassets, systems and infrastructure, as the needs arise. Develops scripts, programs or applications that will identify vulnerabilities and help with investigations, as the needs arise. Responds to alerts

	andnotifications like verbal discussions, telephone calls or e-mails to provide off-hour Help/Service Desksupport as alerts and notifications are received or events are discovered.
5%	**(M)** Miscellaneous Performs other job-related duties as required.

Supervision Received: The Information Technology Specialist II works under general direction of the Information Technology Manager I.

Supervision Exercised and Staff Numbers: None.

Physical Requirements: Works in an office setting, in cubicles with raised and lowered walls. May be sitting and using a computer for long periods. This is a 24X7X365 operation. May be required to work any shift (day, swing, or grave), and extended hours, based on business needs and operational support. Will be required to carry and monitor a mobile device.

Special Requirements: Must possess knowledge and experience administering firewall. Comply with security policies and procedures established by the data owners and the Information Security Officer. Implement the technical means to preserve the integrity and security 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 and integrity for existing and developing systems. Advance-level knowledge of and experience with the following: security information and event management (SIEM) solutions, cybersecurity, URL filtering and content management, end point protection, network security, machine learning, user behavior, artificial intelligence, malware analysis, forensic analysis, intrusion prevention systems, threat intelligence feeds, IT service management tools, information security industry standards and best practices, and compliance regulations.

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.

EMPLOYEE ACKNOWLEDGMENT

I have read and understand the duties listed above and I certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and the ability to work cooperatively with others; and a state of health consistent with the ability to perform the assigned duties as described above with or without reasonable accommodation. (If you believe you may need to request reasonable accommodation to perform the duties of this position, discuss your request with your manager/supervisor who will engage with you in the interactive process.)

EMPLOYEE NAME	EMPLOYEE SIGNATURE	DATE

MANAGER/SUPERVISOR ACKNOWLEDGMENT

I certify this duty statement represents a current and accurate description of the essential functions of the position. I have discussed the duties of this position with the employee and provided the employee a copy of this duty statement

MANAGER/SUPERVISOR NAME	MANAGER/SUPERVISOR SIGNATURE	DATE