STATE OF CALIFORNIA
DEPARTMENT OF CALIFORNIA HIGHWAY PATROL

DUTY STATEMENT

CHP 129 (Rev. 5-19) OPI 097

PROPOSED

COMMAND/ORGANIZATIONAL UNIT Information Management Division (IMD)	DIVISION Information Management Division (IMD)			
CIVIL SERVICE CLASSIFICATION TITLE Information Technology Specialist III	BARGAINING UNIT M01	TENURE Permanent	TIME BASE Full-Time	INTERMITTENT HOURS PER MONTH
POSITION NUMBER 388-040-1415-XXX	CURRENT DATE 05/14/2024			
DESIGNATED POSITION FOR CONFLICT OF INTEREST □ YES ☑ NO	CONFIDENTIAL DESIGNATION □ YES ☑ NO	FOR SELECTION STANDARDS AND EXAMINATIONS SECTION USE ONLY APPROVED BY	DATE	

FUNCTION OF POSITION

Under the administrative direction of the Chief Information Officer (CIO), the Information Technology Specialist III is responsible for coordinating the investigation, resolution, and reporting, through channels, of all information security incidents throughout the Department and serves as the enterprise information security administrator for the Information Management Division's (IMD) Information Security Office. The incumbent serves as the Department's Information Security Officer (ISO) and top project leader for the designing, planning, developing, documenting and maintaining the Department's Information Security Program. Provides mastery level expertise in assessing and recommending information security practices, policies, and methodologies for statewide operations, and represents the Department when interacting with the Office of Information Security (OIS) within the California Department of Technology. The ITS-III is utilized as an industry expert in their area of specialization, exhibits a mastery-level knowledge in formulating technological strategy and policy, and demonstrates a mastery level of team leadership and influence. The ITS-III practices extensive decision-making authority and directs the most sensitive critical/complex information security projects including but not limited to: coordinate comprehensive development and review of technology recovery plans and Department-wide risk assessments; coordinate, develop, conduct, and document information security awareness training for all 11,000+ departmental employees on an annual basis; report security metrics using methodologies developed by the OIS; and participate in activities coordinated by the OIS in order to better understand and address security incidents and critical cybersecurity threats to the state.

SUPERVISION RECEIVED

The Information Technology Specialist III reports directly to and receives the majority of their assignments from the IMD Chief. However, direction and assignments may also come from the IMD Assistant Chiefs.

SUPERVISION EXERCISED

N/A

WORKING CONDITIONS

This position may require over night state wide travel, this position is subject to being on call nights and some weekends.

SPECIAL PERSONAL CHARACTERISTICS

PERCENTAGE OF TIME PERFORMING DUTIES

Essential Functions

25% INFORMATION SECURITY ENGINEERING:
Leads, plans, and provides mastery-level expertise and guidance in the development and enforcement of enterprise security policies and procedures designed to protect information assets, as well as procedures to monitor and ensure compliance with SAM 5300 and related state directives and associated reporting requirements. Provide guidance and direction during information security incident responses, including cybersecurity incidents, and California Law Enforcement Telecommunications System (CLETS) use incidents. Coordinates closely with supervisors and managers through IMD regarding the overall enterprise security efforts for the CHP information technology operations statewide.

20% IT PROJECT MANAGEMENT:
Review new and ongoing departmental information systems projects to ensure commonly accepted and best practice security requirements are met, including analysis of documents prepared as part of the Project Approval Lifecycle (PAL) and Post Implementation Evaluation Reports (PIERs). Facilitates collaboration amongst working groups, internal stakeholders, and Office of Primary Interest (OPI) business owners to understand business process requirements to meet the operational needs through technology. Serve as reviewing authority for requests to install data connections, communication lines of service, and hardware/software system procurements and upgrades statewide. Coordinate the development, review and approval of data exchange agreements with state and non-state entities [e.g., Memorandum of Understanding (MOU)

and Interconnection Sharing Agreement (ISA) documentation related to data sharing agreements with external entities.] Provides mastery-level recommendations regarding information security considerations for new and emerging technologies needed to achieve operational objectives in alignment with the organization's strategic plan and information technology strategic plan.

15% INFORMATION SECURITY ENGINEERING:
Continually evaluate new network security exposures and cybersecurity threats; coordinate and monitor appropriate response and systems upgrades to mitigate vulnerabilities. Develop policies and procedures for the reporting of all such incidents involving intentional or unintentional modification, access or destruction of departmental information assets. Investigate and report any compromise of systems security as mandated by the SIMM and SAM. Coordinate the security evaluation of new proposed software products and provide a recommendation regarding suitability for the organization's technology environment. Plan and develop a road-map for organizational information security maturity to improve compliance with state mandates.

10% INFORMATION SECURITY ENGINEERING:
Provides guidance and direction to the Recovery and Continuity Coordinator (RCC), actively participate in the planning cycle for the Department's Technology Recovery Plan (TRP); structure and implement required testing methodologies to assure viability, and mitigate inherent systems security vulnerabilities affecting TRP implementation. The ISO will lead, guide, and support the RCC with TRP implementation during recovery operations.

10% IT PROJECT MANAGEMENT:
Provides guidance and direction to the departmental Privacy and Risk Management Administrator (PRMA), supports the efforts of the Department's Risk Analysis Team; a multi-disciplinary group of Headquarters' managers responsible for assessing information systems risks and developing mitigation strategies. Provide advice/counsel to the CIO regarding recommendations stemming from this team and implement action plans.

10% INFORMATION SECURITY ENGINEERING:
Provides guidance and direction to the departmental Senior Security Engineer, supports the efforts of continuous scanning and monitoring of enterprise systems, services, logs and special network directories to conduct technical investigations and/ or administrative audits for potential security incidents as well as appropriate use compliance. Leads and coordinates the design and implementation of advanced automated processes to manage security vulnerability notification, assessment and remediation tracking.

5% INFORMATION SECURITY ENGINEERING:
Proficiently communicate intricate technological concepts and issues to executive leadership, present information security awareness briefings during departmental training forums and/or systems administrator meetings. Maintain effective communication and working relationships with team members, business customers, multiple management levels, executive leadership, State control agency staff, and State, Federal and local government entities. Represent the Department in information security committees/groups such as the Federal Bureau of Investigations INFRAGARD group.

Non-Essential Functions

5% Other job related duties within the scope of the classification as assigned.

TOTAL 100%

STATE OF CALIFORNIA
DEPARTMENT OF CALIFORNIA HIGHWAY PATROL

DUTY STATEMENT

CHP 129 (Rev. 5-19) OPI 097

Information Management Division (IMD)

Information Technology Specialist III

388-040-1415-XXX

The duties of this position are subject to change and may be revised as necessary. I have read and understood the duties listed above and I can perform these duties with or without reasonable accommodation. I have discussed the duties of this position with my supervisor and have received a copy of the duty statement.

PRINT EMPLOYEE'S NAME	EMPLOYEE'S SIGNATURE	DATE

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

PRINT SUPERVISOR'S NAME	SUPERVISOR'S SIGNATURE	DATE