

Per California Code of Regulations, title 2, section 548.5, the following information will be posted to CalHR's Career Executive Assignment Action Proposals website for 30 calendar days when departments propose new CEA concepts or major revisions to existing CEA concepts. Presence of the department-submitted CEA Action Proposal information on CalHR's website does not indicate CalHR support for the proposal.

A. GENERAL INFORMATION

1. Date

2026-06-18

2. Department

California Highway Patrol

3. Organizational Placement (Division/Branch/Office Name)

Information Management Division

4. CEA Position Title

Chief, Information Management Division

5. Summary of proposed position description and how it relates to the program's mission or purpose. (2-3 sentences)

The Chief of the Information Management Division (IMD) serves as the Chief Information Officer, the highest Information Technology position within the Department responsible for the policies, technology, personnel, and equipment utilized to facilitate the mission of the California Highway Patrol. Specifically, the Chief provides strategic leadership over mission-critical public safety systems, statewide emergency communications infrastructure, criminal justice information systems, and enterprise technology including the California Law Enforcement Telecommunications System (CLETS), California Statewide Integrated Traffic Records System (SWITRS), 1800-TELL-CHP, Communication Operations Manual, networks, servers, cybersecurity, Computer Crimes Investigations, and mission-related software.

6. Reports to: (Class Title/Level)

Assistant Commissioner, Staff.

7. Relationship with Department Director (Select one)

- ☐ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.
- ☒ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

(Explain):

Managerial level is third. The Chief would not be a member of CHP's Executive Management team but will have near daily collaboration with Executive Management, External/Internal Stakeholders, Allied Law Enforcement Agencies, and State Control Agencies. The Chief will act as principal policy maker tasked with establishing, implementing, and interpreting policies department-wide respective to Communications Operations, Communications Training and Evaluation Program, Computer Crimes Investigations, Mobile Digital Computer Oversight and Use, Telecommunication Facilities, to name a few. All of which directly tie to facilitating CHP's mission.

8. Organizational Level (Select one)

- ☐ 1st ☐ 2nd ☒ 3rd ☐ 4th ☐ 5th (mega departments only - 17,001+ allocated positions)

B. SUMMARY OF REQUEST

9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

The Chief serves as CHP's principal executive advisor regarding enterprise technology strategy, cybersecurity governance, communications interoperability, digital evidence management, data governance, criminal justice information systems, and emerging technologies. The Chief establishes statewide policy, develops strategic initiatives, and provides executive oversight of programs supporting all CHP personnel, communications centers, investigative units, and allied agency partners at all levels of government.

The Chief directs statewide modernization initiatives including emergency communications systems, law enforcement information-sharing platforms, digital evidence technologies, mobile computing environments, cybersecurity programs, and enterprise infrastructure investments. The Chief routinely collaborates with executive leadership, state control agencies, federal partners, local law enforcement organizations, and technology stakeholders to ensure CHP remains compliant, secure, operationally effective, and aligned with statewide public safety priorities.

The Chief will have authority of the 119.8 million-dollar operating budget including but not limited to assigning operating budgets to subordinate commands, approving expenditures needing Division level authorization, and conducting periodic audits to investigate and ensure discrepancies are resolved. Forecast future equipment, personnel, and/or service needs to ensure continuity and expansion of operations for the Information Management Division (IMD).

The Chief is responsible for the implementation of departmental communications policies and procedures, and resolves any operational problems or staffing needs. Ensure equipment requests are processed timely to provide delivery of services to end users. Additionally, the Chief is responsible for the control and inventory of emergency communications equipment needed for local or national emergencies and/or natural disasters. Conducts audits for compliance with Federal Communications Commission rules and departmental procedures.

The Chief sits on the CLETS Advisory Board (nominated and serving at the pleasure of the Attorney General), various committees as part of the International Association of Chiefs of Police, OTS Traffic Records Coordinating Committee (TRCC), State Electronic Data Collection (SEDC) Executive Steering Committee (ESC), Body-Worn Camera ESC, and Mark 43 ESC.

The Chief plays a critical leadership role in coordinating and aligning departmental priorities with external partners such as the California Office of Emergency Services (CalOES), the Governor's Office, and the California State Transportation Agency (CalSTA). Through regular engagement, strategic planning discussions, and participation in inter-agency working groups, the Chief ensures that departmental capabilities, policies, and technologies support statewide public safety, emergency response, and transportation initiatives. This includes advising on policy development, contributing operational and technical expertise during emergencies or large-scale incidents, and helping integrate communication and telecommunications/data systems across agencies. The chief's participation and guidance is particularly important when it comes to the interactions with CalOES regarding the large scale multi-million dollar California Radio Interoperable System (CRIS) radio system. This system is designed to replace the Department's current low band radio system and is critical to communication statewide for the next quarter century. By maintaining strong collaborative relationships and a clear understanding of each entity's priorities, the Chief helps ensure a unified, effective approach to public safety, infrastructure, and crisis management efforts across the state.

The Chief of the CHP's IMD plays a central role in shaping vehicle configurations and personally works with the Enforcement Vehicle Technology Section, and the Chief of Administrative Services Division by ensuring that technology, communications systems, and data capabilities are fully aligned with operational needs. This is accomplished through close collaboration with Fleet Operations and procurement teams, where IMD provides subject matter expertise on emerging technologies, interoperability requirements, cybersecurity standards, and life-cycle management of in-vehicle systems. By participating in specification development, vendor evaluations, and testing, IMD helps ensure that patrol vehicles are equipped with reliable, integrated tools such as mobile data computers, radio systems, cameras, and connectivity solutions that support officer safety and efficiency. This collaborative approach ensures that vehicle procurement decisions are not made in isolation, but rather reflect a unified strategy that balances operational demands, technological advancement, cost-effectiveness, and long-term maintainability.

The Chief has significant influence in facility design/updates to current facilities to accommodate tech equipment. For CHP-owned facilities the Department has the authority to add or remove design spaces when funding is available. In co-located facilities we have only what our lease permits (i.e.: LACC and Sac CC are Caltrans facilities where we lease space PSC also has space allocated to them by Caltrans). For a radio sites, aka "mountain tops" that we own, CHP provides the space and equipment; CalOES Public Safety Communications (PSC) provides the service.

B. SUMMARY OF REQUEST (continued)

10. How critical is the program's mission or purpose to the department's mission as a whole? Include a description of the degree to which the program is critical to the department's mission.

- ☒ Program is directly related to department's primary mission and is critical to achieving the department's goals.
- ☐ Program is indirectly related to department's primary mission.
- ☐ Program plays a supporting role in achieving department's mission (i.e., budget, personnel, other admin functions).

Description: The Information Management Division (IMD) is critical for achieving the CHP's mission of providing the highest level of safety, service, and security. Virtually every operational component of the CHP would be impeded if the Chief was not effective in their role establishing and implementing the technology, communications, data systems, and information-sharing capabilities governed by IMD. This includes implementing up-to-date and comprehensive policies, providing effective department-wide training, ensuring CHP's compliance with statutes, preserving CHP's continued access to mission critical law enforcement communication and law enforcement information sharing databases, leading the IMD team to provide a strong, reliable, and secure processing network; and ensuring all equipment is operational and compatible with the most recent law enforcement software to facilitate CHP's state-wide daily operations of providing public safety.

The policies and program authority the Chief will exercise is directly tied to the facilitation of CHP's mission through computer information security, cyber security, crimes investigation, hardware and infrastructure implementation, 1-800-TELL-CHP (non-emergency phone number), communication operations, communications training and evaluation program, CLETS, SWITRS, public safety, and allied agency dependence on the accuracy of CHP's shared data. The policies, programs, devices, and services under the Chief's governance are utilized state-wide by CHP personnel from every rank.

Additionally, failure of the policy and decision-making authority exercised by the Chief, could impair the CHP's ability to perform its mission, disrupt statewide public safety operations, compromise critical communications, expose sensitive criminal justice information, and negatively affect the Department's credibility with the public, elected officials, and allied agencies such as the Office of Traffic Safety, Department of Motor Vehicles, and California Department of Transportation; loss of public trust in law enforcement, heightened scrutiny from the Governor's office and Legislature potentially resulting in a decrease of operating budget, and/or negative attention from the media.

B. SUMMARY OF REQUEST (continued)

11. Describe what has changed that makes this request necessary. Explain how the change justifies the current request. Be specific and provide examples.

The CHP has undertaken an organizational review of top leadership positions, specifically the policy, programs, and department-wide impact under each position's purview. The complexity, scope, and strategic importance of information technology within public safety have evolved significantly over the last decade. Modern law enforcement operations now depend upon interconnected communication systems, cybersecurity protections, digital evidence platforms, criminal justice information systems, statewide data exchanges, cloud technologies, mobile computing environments, and enterprise infrastructure that require specialized top leadership.

The CHP determined the policy authority, statewide impact, budget responsibility, regulatory compliance obligations, and strategic planning requirements associated with this position exceed those traditionally exercised by a uniformed classification. Establishing a CEA position commensurate with the high-level policy authority, sizable scope of work, and autonomy will allow the ability for CHP to attract industry talent with technical acumen, technical literacy, and liaison experience. This will ensure CHP's policies and technology can incorporate current industry trends, ensure CHP's compliance with statutes, enhance public safety, reduce fatal collisions, provide dependable and accurate data, and facilitate CHP's ability to deliver its mission.

The Chief will maintain the organizational capability and expertise required to meet policy and program objectives and must create a synergy between the information technology and law enforcement industries to enhance our emergency communications and data processing and security. The Chief will have to stay current on industry trends, technology, and establish initiatives to incorporate the latest technology to accomplish operational goals and enhance the public services CHP provides. The decisions this Chief will exercise will directly impact the CHP's 24 hour a day, 7 days per week operations, statewide public safety, and external stakeholders such as Office of Traffic Safety, Department of Motor Vehicles, California Department of Transportation. In short, the Chief's policy responsibility and scope of work exercised will allow necessary policies to be established, revised, and implemented; leverage the necessary technology; and provide the requisite expertise to ensure there are no interruptions to the safety, service, and security CHP provides.

C. ROLE IN POLICY INFLUENCE

12. Provide 3-5 specific examples of policy areas over which the CEA position will be the principle policy maker. Each example should cite a policy that would have an identifiable impact. Include a description of the statewide impact of the assigned program.

Computer Crimes Investigation -CHP as codified in the California Code of Regulations Title 13, section 1875 requires representatives of state agencies to notify CHP upon discovery of all computer related crimes. This requires CHP to investigate any criminal activity in violation of section 502 of the California Penal Code. These requirements place CHP in a unique position requiring skilled IT expertise in addition to law enforcement investigatory prowess. Serving as the state-level computer crimes intake and investigatory processor, raises the consequence of error on CHP to ensure investigations are conducted with the utmost care, expediency, and are accurate.

Cybersecurity Governance -Cybersecurity policies governing the protection of criminal justice information, compliance with CJIS requirements, cybersecurity incident response, managing vulnerabilities, identity management for users, and security architecture affecting all CHP personnel, internal systems, and shared systems is critical for daily operations and mission completion.

Digital Evidence Management -The policies, technology, and systems supporting body worn cameras, in-vehicle camera systems, evidence tracking and custody, public records compliance, and sharing of evidence is mission critical, required by statute, and is necessary for public safety.

Enterprise Technology Governance -Modern, ever-evolving technology and the need for software updates requires strong governance of information technology architecture, procurement standards, system interoperability, cloud computing initiative, Artificial Intelligence management, and modernization efforts. These requirements impact every component of the CHP as an organization and thus directly impact mission accomplishment.

California Law Enforcement Telecommunication System (CLETS) - Is a Department of Justice operated system used by CHP to query and input law enforcement data via CAD (in all 24 communication Centers statewide), MDC (computer in all enforcement vehicles), Web (in all CHP tablets, and or computers who's users require CLETS access to conduct their daily tasks). CHP provides CLETS services to Department of Motor Vehicles and CA Dept of Alcohol Beverage Control through a reciprocity agreement, rises to the CEA C level. Due to stringent usage and training CLETS regulations, CHP, designed two applications. The first is CERT used to track and ensure all CLETS activity is within compliance with CLETS user agreements, used to locate and audit CLETS misuse, and used to also ensure information inputted into CLETS is verified within 7 calendar days. The second CHP designed application is CTARS, the on-line training system for CLETS users and ensures compliance based on the user's level of access. Due to the access and/or proximity to CLETS, all CHP employees are required to be fingerprinted prior to appointment and upon hire complete CLETS training due to their exposure and/or proximity to law enforcement data and/or materials. The CHP has approximately 11,3005 personnel statewide this Chief must ensure has completed the training and those who input data or query data are doing so within compliance. The misuse of CLETS is paramount impact on CHP. The CHP can lose its ability to utilize CLETS as an entire entity and would need to work through an allied agency which would severely impede CHP's ability to carry out its daily operations. Specific CHP personnel misusing CLETS could receive adverse actions, civil action against the department and employee, revocation of CLETS access, and or letter of censure.

California Statewide Integrated Traffic Records System (SWITRS) - Established by the National Highway Safety Act of 1966, SWITRS is owned and managed by CHP. SWITRS is a single uniformed data base for collection and processing of data from a collision scene. The California Vehicle Code (CVC) 20008, mandates all law enforcement agencies (for collisions in CA) to forward a copy of every traffic collision report involving an injury to death to CHP. There are over 550 city police departments, sheriff offices, State Department of Parks and Recreation police departments, and State University police departments and over 100 CHP Areas investigate and report these collisions. Approximately, CHP receives 2,000 collision reports for processing daily being entered into SWITRS. The accuracy of the data entered SWITRS is crucial as state entities such as California Department of Transportation (CalTrans), California Department of Motor Vehicles (DMV), CHP, Office of Traffic Safety, and City planners are a few examples of external stakeholders who utilize SWITR's data to make business decisions. CHP may decide to deploy additional officers to major activity areas to reduce fatal accidents based on this data. The Office of Traffic Safety, DMV and CalTrans can utilize SWITRs data to prioritize roadway improvement projects and safety funding.

1-800-TELL-CHP- Per CVC 10902, CHP established Cal HEAT (Help Eliminate Auto Theft) a toll-free non-emergency line for tips to be received by CHP dispatch personnel 24 hours per day, 7 days per week. The policy has evolved to encompass a nonemergency line for anyone to call and report or request nonemergency information and/or services from CHP via a singular point of contact. This policy directly ties to CHP's mission providing the highest levels of safety, service, and security combined with the continued collaboration between CHP and allied agencies. The IMD Chief has the ultimate authority for this policy and must ensure active and appropriate participation to remain in compliance with CVC 10902.

Communications Operations - An evolving manual consisting of 14 policy chapters utilized primarily by CHP's approximately 975 statewide dispatch personnel. These policies are essential to ensure uniform, consistent, and expeditious emergency communication processing across CHP's 24 state-wide Communication Centers.

C. ROLE IN POLICY INFLUENCE (continued)

13. What is the CEA position's scope and nature of decision-making authority?

The Chief will exercise independent executive authority regarding the CHP's statewide technology governance, communications policy, cybersecurity, information sharing, digital evidence systems, enterprise architecture, technology recovery, information systems, software, technology modernization, Computer Crimes Investigations, California Statewide Integrated Traffic Records System (SWITRS), Communications Training and Evaluation Program, California Law Enforcement Telecommunications System (CLETS) usage, Radio Systems, 1-800-TELL-CHP, and Mobile Digital Computer Oversight and Use. This Chief will serve as primary advisor to the Executive Management team to interpret policies for the most complex and highly sensitive scenarios. This Chief role within CHP requires industry knowledge of Information Technology; however, the Chief independently establishes, interprets, and implements statewide policy concerning law enforcement data and communication systems, their regulatory statutes, how our network and radio system needs all synergize into seamless daily operations which facilitate CHP's ability to carry out its mission. The policy authority this Chief will exercise must ensure CHP's compliance with statutes and affects statewide operations, specifically the officers who enforce traffic laws and the dispatchers who provide life sustaining services to the public. Additionally, the policies under this Chief's purview governs allied agency data CHP receives, processes, and shares with major external stake holders such as Department of Motor Vehicles, California Department of Transportation, the Office of Traffic Safety, Department of Justice amongst others utilize said data to make business decisions that affect Californians, and those who travel on California's roads. The policy implementations under this Chief are statewide, directly tie to public safety, external stakeholder decision making ability, and most importantly CHP's ability to carry out its mission. The policies this Chief is responsible for go above and beyond the guidelines provided by control agency policy since they are unique to CHP.

14. Will the CEA position be developing and implementing new policy, or interpreting and implementing existing policy? How?

The Chief is responsible for both developing policy and interpreting existing policy. Due to rapidly evolving technology, cybersecurity threats, communications requirements, regulatory mandates, and criminal justice systems, the chief must continually evaluate emerging risks and technologies. Establishing and interpreting policies is necessary to maintain operational effectiveness, regulatory compliance, and public trust. Specific examples of evolving law enforcement policies unique to CHP are; Computer Crimes Investigations, cybersecurity governance, digital evidence management, communications interoperability, enterprise architecture, artificial intelligence, information sharing, cloud technologies, mobile computing environments, statewide modernization initiatives, SWITRS, CLETS, 1-800-TELLCHP, Communications Operations, Communications Training and Evaluation, and Mobile Digital Computer Oversight and Use. Furthermore, this CEA will provide subject matter expert policy interpretative and consultative assistance to Executive Management, Chiefs, and Assistant Chiefs throughout the state regarding sensitive and highly complex scenarios. The established and evolving policies under this Chief's purview directly tie to CHP's ability to carry out its mission, to statewide public safety, CHP personnel safety, and state and federal allied agency impacts.