CEA ACTION PROPOSAL

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: 2026-03-23

2. Department: California Highway Patrol

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

Information Management Division

4. CEA Position Title

Assistant Chief

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

This position will support the California Highway Patrol's (CHP) mission of providing the highest level of safety, service, and security serving as principal policy developer, implementor, reviser, and interpreter for Information Technology (IT) policies specific to cyber security, IT device and software procurement, IT Helpdesk, systems and networks. The policies, devices, and services under this CEA's purview are utilized by every member of CHP facilitating CHP's ability to deliver its mission. Additionally, the CEA will provide oversight for IT training, continually procure the latest technologies and devices, conduct and resolve encompassing IT risk, exercise high-level vendor negotiating authority, implement department wide IT initiatives, and ensure overall IT health of CHP.

6. Reports to: (*Class Title/Level*)

Chief, Information Management Division

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 level. The CEA will not be a member of CHP's Executive Management (EM) team but will have routine collaboration with EM. The CEA will act as principal policy maker tasked with establishing, implementing, and interpreting policies department-wide respective to cybersecurity, infrastructure and network architecture, software and hardware initiatives, IT services and device procurement. The CEA administers regular policy briefings, advises on major IT projects, compliance requirements, pending regulatory impacts, technology advisory board initiatives (the CEA will serve as Chairperson), and presents findings of IT security threat assessments and their resolutions to EM.

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 Assistant Chief directs and controls the distribution and use of personnel, fiscal, and material resources to meet the needs and priorities of the Department's mission, programs, and objectives. Establishes goals and objectives for IMD sections to ensure the achievement of major program responsibilities. Exercises strategic alignment, portfolio governance, resource allocation, risk management, stakeholder communication, post project review. This includes establishing the vision and strategic operating goals for IMD. Reviews and negotiates security-related clauses in multi-million-dollar contracts and agreements with vendors, state agencies, and other external entities to ensure alignment with CHP's security policies and compliance requirements. Ensures operations meet all applicable requirements of the State Administrative Manual (SAM), Statewide Information Management Manual, National Institute of Standards and Technology, Cybersecurity Framework, National Institute of Standards and Technology (NIST), NIST Cybersecurity Framework, NIST Secure Software Development Framework, and other binding Federal and State regulations. Serves as the principal policy maker, advisor, implementor, and interpreter regarding policies for the formation and support of CHP's cybersecurity, departmental employee information technology training, IT device deployment and maintenance, Departmental Technology Advisory Board, and IT procurement services. Additionally, formulates policies for IT processes specifically cybersecurity, IT software, and CHP HelpDesk activities and services. Conducts reviews and provides subject matter expert review and advice on all pending IT policy. Provides policy interpretative and consultative assistance to Executive Management regarding sensitive and highly complex scenarios encompassing IT services and/or programs.

Responsible for the administration and governance of a 51.6+ million-dollar IT operating budget. Forecasts evolving needs for IT programs, equipment, and devices. Establishes and administers spending plans for subordinate sections/programs. Reviews and approves reconciled expenditures ensuring allocated spending is within budget. Conducts periodic audits to ensure compliance and documents are aligned with departmental policy and control agency regulations. Identifies and resolves irregularities to conclusion. Reviews, approves, and/or denies expenditure requests and through administrative staff coordinates with Fiscal Management Section and/or Business Services Section to ensure compliance with all SAM manual and Department of Technology procurement, contract, and other miscellaneous requirements. Facilitates discussions with Executive management, Chief, and Commanders to relay budget health and if or where budget cuts must be made, or funds must be shifted to maintain optimal IMD operations. Collaborates with Executive management and forecasts future budget needs by providing trend analysis of historical expenses and incorporating estimations of future monies needed.

Serves as chair of CHP's Technology Advisory Board through facilitation of meetings, fostering collaborative and effective working relationships with Executive management, Chiefs, Assistant Chiefs, Commanders, and other internal/external stakeholders to close the gap between IT operations and field operations; and provide consistent information updates on current and proposed IT project initiatives. Establishes working groups with subject matter experts to define the scope of major projects, ensure end user needs are met, and develops comprehensive trainings to implement statewide operating systems, database management systems, and/or devices. Delivers IT risk management briefings, policy impact analysis, program performance analysis, and strategic resolutions to Executive Management that influence decision making resulting in department wide impacts. Maintains the organization's effectiveness and efficiency by defining, delivering, and supporting IT centered strategic plans. Directs technological research by establishing and leading working groups studying organization goals, strategies, practices, user projects, to launch initiatives. Monitors IT project milestones and design of technical status reports. Amends project timelines and allocates resources accordingly to ensure projects remain within budget, delivered timely, implemented with comprehensive training, and appraises Executive Management concerning any delays with resolutions to impediments.

Maintains the organizational capability and expertise required to meet policy and program objectives. Stays current on industry trends technology and finds ways to incorporate the latest technology to accomplish operational goals. Reviews and guides initiatives to ensure conformity to policy and effective approaches. Leads the development, implementation, and validation of technology recovery plans, continuity strategies, and operational resiliency frameworks. Conducts privacy threshold assessments and privacy impact assessments, statewide security assessments, and compliance reviews; ensuring corrective actions are implemented consistently, sustainably, and align with policy. Ensures IT environments maintain readiness for disruptive events and corrective contingencies are in place to minimize outages. Develops initiatives secure solutions that enhance the resilience, performance, and security of CHP’s information systems and technology service.

Promotes and supports equal employment opportunity principles; ensures compliance with nondiscrimination requirements; and fosters a professional work environment consistent with departmental policy. Fosters and maintains a business culture and work environment that is fair, inclusive, and free of discrimination and harassment.

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 policy and program authority the CEA will exercise is directly tied to the facilitation of CHP's mission through technology infrastructure, IT devices used directly for and which facilitate enforcement and allied agency operations, network security and collected data protection, software which facilitates the Officer's citations, and establishment of dashboards for presentation of analytics to EM for determination of resource allocation and operational strategies. The policies, programs, devices, and services under this CEA's governance are utilized by department-wide personnel from every rank. The CHP's mission of providing the highest level of safety, service, and security would be impeded greatly if this CEA was not effective in their role establishing current and comprehensive policy, procuring and implementing the latest devices and technology software systems, ensuring a strong reliable processing network and resolving outages immediately, and maintaining a cybersecure and encrypted portals for enforcement operation executing. Additionally, the policy and decision making this CEA will exercise if done so erroneously, has the potential to result in direct loss of life, monetary damages as a result of lawsuits, exposure of confidential law enforcement sensitive information and/or cyber hacks to federal systems CHP imports/exports data from, discredit to CHP and loss of public trust of law enforcement, heightened scrutiny from the Governor's office and Legislature potentially resulting in a decrease of operating budget, loss of procurement delegated authority, 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 is actively reviewing high-level positions in various capacities to determine if continuing to utilize a uniformed classification best aligns with the ability to support the evolving operational needs of the Department, specifically the policy, programs, and department wide- impact under each position's purview. Information Technology is a specialized field with near constant change and at CHP include evolving operational demands. The CHP determined establishing a CEA position commensurate with the high-level policy authority, sizable scope of work, and autonomy is the best option at this time for a vacant Information Technology Assistant Chief position.

If approved, the established CEA will allow the ability for CHP to attract industry talent who can speak the IT language and ensure CHP's technology can incorporate current industry trends. The CEA will maintain the organizational capability and expertise required to meet policy and program objectives. Stay current on industry trends technology and finds ways to incorporate the latest technology to accomplish operational goals. Analyzes review, and measure service level performance against agreed upon service level agreements. The CEA will Manage, evaluate, plan, and implement integrations with current and future enterprise systems. Review and guide initiatives to ensure conformity to policy and effective approaches. Lead the development, implementation, and validation of technology recovery plans, continuity strategies, and operational resiliency frameworks. Conduct privacy threshold assessments and privacy impact assessments, statewide security assessments, and compliance reviews; ensuring corrective actions are implemented consistently, sustainably, and align with policy.

The statewide operations CHP exercises requires 24 hour a day 7 days per week operational infrastructure demanding this CEA ensures IT environments maintain readiness for disruptive events and corrective contingencies are in place to minimize outages. The policy and scope of work this CEA will exercise will allow necessary policies to be established, leverage of the necessary tech, devices, experts, to ensure there is 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.

Information Security and Administration Manual – This manual contains policies covering CHP's network administration, CHP's e-mail, malware prevention and protection, information technology project management and oversight, information systems account management, division network administrators, remote computing, CHP intranet/internet, media sanitation and disposal, acceptable use policy, OneDrive for business.

Enforcement Documents Manual – This manual contains policies regarding the automated citation device utilized to generate enforcement citations electronically (in addition to the standard paper citations), necessary training, appropriate device usage, system and device troubleshooting, operating equipment used in tandem with the device, enforcement vehicle compatibility and installation, maintenance repair and replacement of devices, security and information obtained confidentiality directives.

Information System Documentation Manual – This manual contains policy regarding requests for information systems development and establishes policy for Information system documentation standards. Specifically, this policy establishes procedures, practices, and guidelines governing the concept development, planning, requirements analysis, design, development, integration and test, implementation, operations, manages custom application development from concept to completion, and maintenance and disposition of information systems within the CHP.

Materials Management Manual – This manual contains policies regarding CHP's copier program (multifunction printers [MFP]), and information technology goods and services acquisition. The policy contained within ensures the MPFs are effectively managed, maintenance information is communicated and accessible, and appropriate equipment is procured. Furthermore, the information technology goods and services acquisition policies provide departmental personnel with instructions for purchasing information technology (IT) goods and services. Any procurement meeting the criteria defined in SCM, Volume 2, Section 1000, Defining an IT Procurement, and SAM 4819.2, must be classified as IT. In addition, this chapter outlines the policy and procedures for the approval, budget, procurement, shipment, receipt, configuration, repair, and disposition of all departmentally owned computers and IT devices, equipment, and software.

Technology Advisory Board (TAB) Policy – This CEA will serve as the TAB Chair sets the vision, objectives, and facilitates the effectiveness of the TAB. At a high level this policy governs the activities of the TAB which provide cohesive planning and communication throughout the Department, bridging the information sharing and feedback gap between IT operations and field operations, and to provide consistent information updates on current and proposed IT related project initiatives. The TAB will solicit suggestions for IT related improvements to provide the highest level of safety and efficiency for the end users of technology.

This CEA will serve as the principal policy maker, advisor, implementor, and interpreter regarding policies for the formation and support of CHP's cybersecurity (CHP ties into multiple law enforcement databases and systems daily), departmental employee information technology training (every CHP employee is required to complete this training annually), IT device deployment and maintenance (statewide oversight for 2,328 automated citation devices, 18,914 laptops, and 5,390 printers), Departmental Technology Advisory Board, and IT procurement services (CHP has a tier 3 procurement delegation and is in process of obtaining tier 4 delegation authority). Additionally, formulates policies for IT processes specifically cybersecurity, IT software, and CHP HelpDesk (receives and processes over 40k+ help tickets on average per year) activities and services. Conducts reviews and provides subject matter expert review and advice on all pending IT policy. Provides policy interpretative and consultative assistance to Executive Management regarding sensitive and highly complex scenarios encompassing IT services and/or programs. The consequence of error tied to the policies under this CEA's purview can directly impede CHP's ability to administer safety, service, and security. Specifically, the policy and decision making this CEA will exercise if done so erroneously, has the potential to result in direct loss of life, monetary damages as a result of lawsuits, exposure of confidential law enforcement sensitive information and/or cyber hacks systems CHP imports/exports data from, judicial impediments if the devices and or systems CHP utilizes to send enforcement information to court systems and/or portals, discredit to CHP and loss of public trust of law enforcement, heightened scrutiny from the Governor's office and Legislature potentially resulting in a decrease of operating budget, loss of procurement delegated authority, and/or negative attention from the media.

C. ROLE IN POLICY INFLUENCE (continued)

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

This CEA will serve as the principal policy maker, advisor, implementor, and interpreter regarding policies for the formation and support of CHP's cybersecurity, departmental employee information technology training, IT device deployment and maintenance, Departmental Technology Advisory Board, and IT procurement services. Additionally, formulates policies for IT processes specifically cybersecurity, IT software, and CHP HelpDesk activities and services. This CEA will serve as primary advisor to the Executive Management team.

The CEA will have authority of the 51.6-million-dollar operating budget including but not limited to resource allocation, approval of expenditures, ensure allocations are not surpassed, conducting periodic audits to investigate and resolve any discrepancies. Forecast future equipment, personnel, and/or service needs to ensure continuity and expansion of operations.

The CEA will exercise strategic visioning by establishing objectives, collaborating with internal and external stakeholders on deliverables, lead risk assessments and implement resolutions, IT project MGMT, technology advancement, IT services expansion. Developing contingency plans and improving software systems to reduce outages and minimize reactivation timeframes when outages occur. Continually be engaged with teams to improve HelpDesk services, by running analytics and highlighting trends amongst help tickets for innovative solutions to reduce future occurrences.

This CEA will have direct authority regarding policy, procurement, replacement, maintenance, and budgetary governance of the physical statewide IT device inventory consisting of 18,914 laptops, 5,390 multifunction printers, and 2,328 citation devices all of which facilitate CHP’s ability to deliver its mission of providing the highest level of safety, service and security.

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

Information technology is a constantly evolving industry requiring a top expert who is equipped to provide associated policy, programs, and services to facilitate CHP’s ability to carry out its mission. With this industry fluidity, this CEA will serve as the principal policy maker, advisor, implementor, and interpreter regarding policies for the formation and support of CHP's cybersecurity, departmental employee information technology training, IT device deployment and maintenance, Departmental Technology Advisory Board, and IT procurement services. This CEA will formulate evolving policies for IT processes specifically regarding cybersecurity, IT software, and CHP HelpDesk activities and services. This CEA will establish implementation initiatives to launch newly established policies and as necessary develop training for end users. 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 policies established and under this CEA’s purview result in statewide impact throughout CHP as each employee will refer, be subjected to, and utilize the guidance contain within the policies exercised under this CEA.