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

<table>
<thead>
<tr>
<th>1. Date</th>
<th>2. Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 22, 2022</td>
<td>California Privacy Protection Agency</td>
</tr>
</tbody>
</table>

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

4. CEA Position Title
Chief Information Officer

5. Summary of proposed position description and how it relates to the program's mission or purpose.
(2-3 sentences)
The California Privacy Rights Act of 2020 (CPRA) charges the California Privacy Protection Agency (CPPA) with protecting Californians’ privacy rights. The CPPA’s responsibilities include: 1) rulemaking in a highly complicated, technical, sometimes contested, and nuanced area; 2) supporting awareness across California’s diverse population on issues related to privacy and data security, including the new rights provided to them by the law; and 3) preparing for meaningful administrative enforcement of those rights. Under administrative direction of the Deputy Executive Director, the Chief Information Officer (CIO) is a key member of the Executive team will be responsible for providing vision and leadership, in addition to administering the CPPA's Information Technology (IT) strategic planning process and developing and implementing IT policies to meet the needs of the Agency.

6. Reports to: (Class Title/Level)
Deputy Executive Director

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): 

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.

Under the direction of the Deputy Executive Director, the CIO will address the most complex and sensitive assignments related to the Agency’s IT policies. The CIO will serve as the lead advisor to the Executive Director and Deputy Executive Director on all IT and Information Security matters relating to CPPA. The CIO will create and oversee the Information Technology Division as well as provide executive oversight of CPPA IT/Security policy and multiple technology projects. Direct IT vendor/contract management. Meet with contractors on a regular basis to ensure appropriate level of service delivery. Develop and implement technology strategy in support of CPPA business strategy.

The CIO will lead the Executive IT Governance process, including development of common goals that align with the Agency’s strategic priorities and operational plans for various business units.

Lead and support various committees to ensure IT systems are aligned to strategic directions; develop and enhance appropriate and necessary security and follow appropriate change management policies. Participate as a key member of CPPA enterprise governance and provide critical support and information to business leaders in support of governance decisions. Provide leadership in the Agency’s communication strategy pertaining to IT.

Oversee IT operations, infrastructure development, security, maintenance, procurement, data, and support. Oversee the effective and efficient development, implementation, maintenance, and operations of all CPPA systems. Plan, organize, and direct the development and implementation of data and technology in support of CPPA business strategy. Monitor progress, scope, and costs of new and existing IT systems. Develop and influence IT policy development for CPPA in the areas of IT Service Management, enterprise architecture, IT infrastructure, application development, governance support, project portfolio management, and current/future technology. Enforce IT/Security policies and practices to support the technology strategy and direction to protect and efficiently manage IT systems and data. Ensure policies and procedures are in compliance with federal and State mandates. Set goals and objectives for the IT Division that are consistent with the Agency’s mission; secure the appropriate staffing levels and classifications, and obtain the necessary tools (computer hardware and software, IT infrastructure and architecture, etc.) to effectively support the Agency’s workforce.

Meet and confer with oversight agencies on IT matters, IT vendors on project development and implementation issues, and program stakeholders. Responds to requests from control agencies related to the IT functions of CPPA. Builds and maintains relationships with oversight agencies, internal program customers, external partners and stakeholders.
## 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.

- [x] 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 California Privacy Rights Act of 2020 (CPRA) charges the California Privacy Protection Agency (CPPA) with protecting Californians' privacy rights. The CPPA’s responsibilities include: 1) rulemaking in a highly complicated, technical, sometimes contested, and nuanced area; 2) supporting awareness across California’s diverse population on issues related to privacy and data security, including the new rights provided to them by the law; and 3) preparing for meaningful administrative enforcement of those rights.

The Chief Information Officer (CIO) is a key member of the executive team and is responsible for providing vision and leadership to the Information Technology Division. The CIO administers CPPA’s IT strategic planning process and develops and implements IT policies to meet the needs of the Agency. Additionally, the CIO provides advice and guidance to the executive leadership and the Board on IT related matters and represents the Agency at statewide IT initiatives.
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 California Privacy Protection Agency (CPPA) is a newly established agency created by the California Privacy Rights Act of 2020 (CPRA). The CPRA directs the Agency to fulfill a wide variety of responsibilities involving complex and constantly changing business, social, and technological issues. (Civil Code, § 1798.199.140(a)(l)). These responsibilities include: (a) administering, implementing, and enforcing through administrative actions the CPPA; (b) engaging in extensive rulemaking to adopt, amend, and rescind regulations that implement the CPPA; (2) analysis of problems (c) protecting the fundamental privacy rights of natural persons with respect to the use of their personal information.

The Chief Information Officer (CIO) is essential in ensuring support of CPPA by advising the Deputy Executive Director and Executive Director on Information Technology and Information Security policies to support the mission of CPPA. The CIO will also serve an essential role in establishing the Information Technology Division as well as guaranteeing the continuous success of CPPA.
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.

The CPPA provides vital input into high level policy and program decisions for IT services and routinely works with other high level administrators and influences broad policies and procedures. The incumbent is responsible for reviewing, developing, creating, and implementing policies, standards, and procedures.

The CIO will be responsible for overall policy formulation and decision making relative to the management and use of Information Technology within the Agency. The CIO will chair internal Information Technology governance committee charged with formulating technology strategy and policy recommendations for CPPA.

The CIO will establish Information technology policies to ensure compliance with the information security and privacy policies, standards and procedures issued by the Office of Information Security. In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the OIS, the CIO shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of CPPA Programs in accordance with Government Code section 11549.3.

The CIO will serve as the principal policy maker to ensure business continuity with technology recovery for CPPA per the State Administrative Manual (SAM) Section 5325. The CIO will develop CPPA recovery policies and strategies to ensure systems, functions and infrastructure can be brought on-line quickly, as well as develop the Business Continuity Plan to include procedures for how the Agency will stay functional and how critical infrastructures will continue providing necessary services in a disastrous state.
C. ROLE IN POLICY INFLUENCE (continued)

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

The California Privacy Rights Act of 2020 (CPRA) charges the California Privacy Protection Agency (CPPA) with protecting Californians’ privacy rights. The CPPA’s responsibilities include: 1) rulemaking in a highly complicated, technical, sometimes contested, and nuanced area; 2) supporting awareness across California’s diverse population on issues related to privacy and data security, including the new rights provided to them by the law; and 3) preparing for meaningful administrative enforcement of those rights.

The Chief Information Officer (CIO) is a key member of the executive team and is responsible for providing vision and leadership to the Information Technology Division. The CIO administers CPPA’s IT strategic planning process and develops and implements IT policies to meet the needs of the Agency. Additionally, the CIO provides advice and guidance to the executive leadership and the Board on IT related matters and represents the Agency at statewide IT initiatives. The CIO is responsible for building and managing the CPPA IT organization, leading the development and management of CPPA IT strategy, supporting CPPA's enterprise governance, supporting and leading the management of project delivery, overseeing and managing CPPA’s enterprise architecture, vendor/contract management, and overseeing IT administration activities. Develops information security programs to ensure the confidentiality, integrity, availability, and appropriate use of CPPA information assets. The CIO is responsible for leading delivery of critical customer support services, driving solution architecture for the enterprise, leading IT operations governance processes, and supporting various customers in support of departmental business needs. The CIO organizes, directs, and evaluates the activities of IT staff and contractors. A key focus is supporting the Agency in achieving strategic and tactical outcomes through the interactions between architecture, projects, vendors, and state teams.

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

Yes. The CIO directs the CPPA Information Technology Division. Provides executive oversight of CPPA IT/Security policy and multiple technology projects. Oversees the effective and efficient development, implementation, maintenance, and operations of all CPPA systems. Plans, organizes, and directs the development and implementation of data and technology in support of CPPA business strategy. Monitors progress, scope, and costs of new and existing IT systems. Develops and influences IT policy development for CPPA in the areas of IT Service Management, enterprise architecture, IT infrastructure, application development, governance support, project portfolio management, and current/future technology. Enforces IT/Security policies and practices to support the technology strategy and direction to protect and efficiently manage IT systems and data. Ensures policies and procedures are in compliance with federal and State mandates.