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>06/17/2022</td>
<td>California Department of Corrections and Rehabilitation</td>
</tr>
</tbody>
</table>

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

- Office of Legal Affairs

4. CEA Position Title

- Chief Privacy Officer

5. Summary of proposed position description and how it relates to the program's mission or purpose.

   The California Department of Corrections and Rehabilitation (CDCR) is requesting establishment of a CEA to serve as the department's Chief Privacy Officer (CPO). The position reports to the Assistant Secretary, Office of Legal Affairs (OLA), and is responsible for developing, reviewing and implementing complex and critical privacy policy and business practices designed to protect data from unauthorized access and to ensure that the department complies with federal and state privacy laws and regulations. The CPO serves in a leadership role for privacy compliance as the highest level advisor to the Assistant Secretary, OLA and Executive Leadership on laws, regulations and best practices for departmental privacy-related issues.

6. Reports to: (Class Title/Level)

- Assistant Secretary, Office of Legal Affairs (Exempt)

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.
   - [x] Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

   **(Explain):** The CPO will serve as the department’s subject matter expert on privacy laws, regulations, policy, and industry best practices and work closely with executive management in developing, implementing and maintaining the Department’s Privacy Policy, and resolving privacy issues.

8. Organizational Level (Select one)

   - [ ] 1st
   - [ ] 2nd
   - [x] 3rd
   - [ ] 4th
   - [ ] 5th (mega departments only - 17,001+ allocated positions)
9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

Under the general direction of the Assistant Secretary, California Department of Corrections and Rehabilitation (CDCR), Office of Legal Affairs (OLA), the Chief Privacy Officer (CPO) is responsible for the department’s Privacy Program, including but not limited to, daily operations of the program, development, implementation, and maintenance of policies and procedures, monitoring program compliance, investigation and tracking of incidents and breaches, and ensuring the program is in compliance with federal and state laws. The CPO is charged with building a strategic and comprehensive privacy program that defines, develops, maintains and implements policy and processes that enable consistent, effective privacy practices which minimize risk and ensure the confidentiality of protected information, paper or electronic, across all media types. The incumbent is responsible for developing and implementing policies designed to protect data from unauthorized access. Performs difficult and complex analyses related to the Department and prepares comprehensive briefings to various areas within the CDCR. Oversees projects to reduce risk, mediate vulnerabilities, and enhance privacy protection. The CPO is responsible for developing, reviewing and implementing the most complex and critical privacy and business practices to ensure that the department complies with privacy laws and regulations. The CPO serves in a leadership role for privacy compliance as the highest level advisor to the Assistant Secretary, OLA and Executive Leadership on laws, regulations and best practices for departmental privacy-related issues.

Acts as the departmental Privacy subject matter expert and consultant for CDCR projects, its customers, and program areas. Applies proficient knowledge of current and evolving business concepts to set policy that ensures the collection, use, sharing, and storage of CDCR’s personally identifiable information are aligned with privacy best practices and standards. Acts as a privacy expert, provides analyses and policy recommendations to the Director and Executive Staff on federal and state laws, regulations, policies, and procedures related to the privacy of personal, confidential and sensitive information, including personal health information covered by the Health Insurance Portability and Accountability Act (HIPAA). Acts as Lead in the development, implementation, and maintenance of CDCR’s privacy policy, associated policies and procedures in coordination with CDCR management, administration, and legal counsel. The CPO develops and disseminates department privacy policies and procedures, based on an analysis of the laws in this area. Establishes guidelines, priorities, and management systems to ensure an efficient and effective operation. Evaluates the impact of laws, rules and legislation on the privacy and security process. Researches and reviews privacy legislation and new or proposed bills involving privacy and security issues. Provides feedback to the Legislative Office regarding departmental or program-area impact. Determines if new/revised laws or requirements may require changes in departmental policy or procedures.

Establishes and implements policy for the investigation of privacy complaints and the resolution of privacy incidents. Works collaboratively with the Division of Enterprise Information Services in establishing an ongoing process to track, investigate, and report inappropriate access and disclosure of PII or PHI protected information. Monitors patterns of inappropriate access and/or disclosure of protected information. Independently researches and provides expert privacy consultation on incidents of all types, including hard copy and electronic incidents from CDCR, as well as its business partners. Leads various program areas in the implementation of corrective action plans. Acts as Incident Commander on Incident Response Teams and determines the appropriate action plan in investigating, mitigating, and correcting major security incidents. Performs required breach risk assessment, documentation, and mitigation. Coordinates required incident reporting to CDCR Executive Management, State Office of Information Security and other entities. Manages all required breach determination and notification processes under HIPAA and applicable State breach rules and requirements. Independently analyzes incident data and develops statewide reports, performance measures, and trend analysis.

Conducts privacy impact assessments and manages analytical studies on the most complex CDCR systems that collect personally identifiable information in order to identify and mitigate existing and potential privacy risks and vulnerabilities. Researches and stays abreast of emerging technologies and develops new methods and innovative solutions to address related privacy challenges throughout the department. Acts as the expert privacy consultant in the review and development of Budget Change Proposals, Issue Papers and Post Implementation Evaluation Reports to ensure compliance with privacy best standard. Conducts ongoing privacy awareness campaigns for the department’s workforce including creating privacy displays, presentations, handouts, posters, and other training materials to educate the department on proper privacy protection strategies. Works with different program areas to identify any area-specific privacy vulnerabilities, develops appropriate mitigation plans, and oversees the successful implementation and ongoing execution of such mitigation plans.

Prepares written documents to provide information and/or direction on issues related to Departmental programs and services such as amendments for legislation, Department position letters on legislative bills, and other legal correspondence. Analyzes correspondence, researches, and gathers information to draft response memos and letters from the Assistant Secretary’s Office.
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 mission of the California Department of Corrections and Rehabilitation (CDCR) is to facilitate the successful reintegration of the individuals in our care back to their communities equipped with the tools to be drug-free, healthy, and employable members of society by providing education, treatment, rehabilitative, and restorative justice programs, all in a safe and humane environment.

CDCR has a legal obligation to establish and maintain a privacy program that supports the Department's primary mission. State and federal law, as well as industry best practices, require implementation of privacy, information security protocols and safeguards to prevent, manage, and mitigate privacy, information security, and security risks. Failure to comply with these requirements can result in penalties for non-compliance and could jeopardize the safety of employees, the public, victims, contractors, parolees and individuals in our care.

The CPO investigates and processes information security incidents that involve Protected Health Information (PHI) and Personally Identifiable Information (PII). Such oversight involves conducting risk assessments, preparing required notifications to oversight agencies and affected individuals when required by law, and working with Hiring Authorities and enforcement agencies for mitigation and/or remediation of incidents resulting in reportable breaches. The CPO will also provide guidance and training to all CDCR programs on privacy concerns and departmental policy and practice.

The incumbent serves as the Department's point-of-contact/liaison with the Office of Information Security and Privacy Protection, the California Health and Human Services Agency, and all other state and federal agencies, with respect to privacy-related complaints against the Department.
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.

Under the provisions of Government Code Section 11019.9, all departments, including CDCR, are required to implement and maintain a permanent privacy policy. CDCR must also designate a position to be responsible for CDCR's Privacy Policy. State and federal law, as well as industry best practices, require implementation of privacy, information security protocols and safeguards to prevent, manage, and mitigate privacy, information security, and cyber security risks. Failure to comply with these requirements can result in penalties for noncompliance. Additionally, public health and safety could be immediately jeopardized by the failure or disruption of a system. Currently, CDCR does not have a designated position responsible for developing, implementing, and maintaining the departmental Privacy Policy.

As a covered entity under HIPAA, CDCR must protect individual privacy rights and secure staff data by preventing unauthorized access, use, disclosure, transfer, reporting, or destruction. With the increase in teleworking, CDCR also faces new challenges and risks in terms of information security. The increased use of technology to manage Protected Health Information (PHI) and Personally Identifiable Information (PII), as well as increased electronic data sharing, has increased the risk to privacy, information security, and cyber security.

Per the Department of General Services (DGS), State Administrative Manual (SAM) section 5300 et seq. and Statewide Health Information Policy Manual (SHIPM) section 1.2.1 State Agency Responsibility, CDCR is responsible for augmenting the privacy program to comply with and implement statewide privacy policies and procedures. Per SAM, information security refers to the protection of information, information systems, equipment, software, and people from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information, regardless of its form (electronic, optical, oral, print, or other media), is critical to ensure business continuity, and protection of information assets against unauthorized access, use, disclosure, disruption, modification, or destruction. Information security is also the means by which privacy of personal information held by state entities is protected.

The CPO will be responsible for building a strategic and comprehensive privacy program that defines, develops, maintains and implements policy and processes that enable consistent, effective privacy practices which minimize risk and ensure the confidentiality of protected information, whether paper or electronic and across all media types.
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 CPO will be the principle policy maker for the Department over the following areas:

1. Privacy Policy:

The CPO, serving as CDCR's subject matter expert on privacy, will act as lead in the development, implementation and maintenance of the department's Privacy Policy, associated policies and procedures, in coordination with CDCR management, administration, and legal counsel to ensure the department is in compliance with federal and state privacy laws and regulations. The CPO will ensure the Privacy Policy is designed to protect data from unauthorized access. The CPO will provide analyses and policy recommendations to the Director and Executive Staff on federal and state laws, regulations, policies, and procedures related to the privacy of personal, confidential and sensitive information, including personal health information covered by the HIPAA. The CPO develops, implements and disseminates department privacy policies and procedures, based on an analysis of the laws in this area.

2. Policy for the Investigation of Privacy and Security Complaints/Incidents:

The CPO will establish and implement policy for the investigation of privacy and/or security complaints and incidents. The CPO will work collaboratively with the Division of Enterprise Information Services in establishing an ongoing process to track, investigate, and report inappropriate access and disclosure of PII or PHI protected information. Monitors patterns of inappropriate access and/or disclosure of protected information. The CPO researches and provides expert privacy consultation on incidents of all types, including hard copy and electronic incidents from CDCR, as well as its business partners.

3. Policy for Remedial and Corrective Action to Resolve Privacy and Security Incidents:

The CPO will lead various program areas in the implementation of corrective action plans by acting as the 'Incident Commander' and determining the appropriate action plan to mitigate and correct major security incidents. Sets policy for breach risk assessment, documentation, and mitigation. In addition, coordinates required incident reporting to CDCR Executive Management, State Office of Information Security and other entities. Manages all required breach determination and notification processes under HIPPA and applicable State breach rules and requirements.

4. Privacy Awareness Training Policy:

The CPO position oversees and sets policy on privacy awareness training, mandates, and compliance for departmental employees. The CPO develops and has oversight of ongoing privacy awareness campaigns for the department's workforce including creating privacy displays, presentations, handouts, posters, and other training materials to educate the department on proper privacy protection strategies.
C. ROLE IN POLICY INFLUENCE (continued)

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

The Chief Privacy Officer position requires a high level of independent judgment and has full decision-making authority over the Department's privacy program. The CPO will direct the most critical/complex reviews, as the incumbent will lead the Department's efforts in developing and implementing a robust privacy program that is in compliance with state and federal privacy laws. The incumbent will serve as the department's subject matter expert on privacy, and as such, will be required to have expert knowledge of state and federal privacy laws and regulations. The position will provide oversight, governance, and strategic direction regarding departmental privacy issues.

As sensitive privacy issues, proposals, and/or special projects arise through state and/or federal regulations, proposed legislation, and/or court mandates, the CPO will be responsible for assessing them, determining the impact on departmental programs, and collaborating with CDCR program directors and external stakeholders to ensure CDCR privacy policy and business practices comply with state and federal laws.

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

The CPO will be developing, recommending, and implementing new policy as well as modifying and implementing existing policy. New policy will be developed as required to meet the operational need of CDCR, in response to state and federal law/regulation changes impacting privacy, and legislative or court mandates, audit findings and resultant corrective action plans, and/or collective bargaining agreements. Existing policy will be reviewed and updated as required, commensurate with program changes within CDCR, and external changes impacting privacy practices.