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>07/29/2022</td>
<td>Employment Development Department</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Organizational Placement (Division/Branch/Office Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology Branch (ITB)/Cybersecurity Division</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. CEA Position Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief, Cybersecurity Division</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. Summary of proposed position description and how it relates to the program's mission or purpose. (2-3 sentences)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Chief of the Cybersecurity Division is a member of the Employment Development Department’s Executive Staff and the Information Technology Branch (ITB) Executive Team, with responsibility for an annual Cybersecurity Division budget of $15 million. The incumbent provides strategic direction for the initiation, design, development, testing, operation and defense of the EDD’s IT environments, and directs efforts to prevent, restrict and address sources of disruption, ranging from natural disaster to malicious acts. The incumbent works with executive level stakeholders across multiple divisions, functions and programs across the EDD, to ensure cohesive and timely implementation of IT-related strategies and mission-critical projects to meet current and future organizational needs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. Reports to: (Class Title/Level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deputy Director, Information Technology Branch (CEA C)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. Relationship with Department Director (Select one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.</td>
</tr>
<tr>
<td>□ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.</td>
</tr>
<tr>
<td>(Explain):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. Organizational Level (Select one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ 1st  □ 2nd  ✔ 3rd  □ 4th  □ 5th (mega departments only - 17,001+ allocated positions)</td>
</tr>
</tbody>
</table>
9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

The Chief of the Cybersecurity Division provides vision and leadership for developing and supporting EDD’s new Cybersecurity and anti-fraud effort. The incumbent determines and develops enterprise-wide cybersecurity policy and direction, and establishes the Department’s strategic goals and long-range objectives, pertaining to EDD’s Cybersecurity systems. The incumbent plans, organizes, and directs a broad range of Cybersecurity activities, including: Asset Protection, Contingency Planning, Incident Management, Policy and Procedure Development and Training, Privacy, Security Compliance, Security Engineering and Architecture, Security Operations, Security Risk Management and Security Testing and Assessment. The incumbent has a significant breadth and depth of understanding of the EDD’s business process needs, assesses internal and external risks, provides appropriate mitigation strategies, and stays current on relevant laws, regulations and technologies.

The position has extensive decision-making authority and works with senior level stakeholders across multiple functions and programs to ensure cohesive and timely implementation of IT-related strategies and mission-critical projects to meet current and future organizational needs. The incumbent plays a primary role in providing leadership and oversight to broaden and strengthen Departmental operations, including: EDD information technology stored in more than 4000 servers and 12,000 clients, equipment and staffing requirements, systems services, document management systems, database management systems, and storage and retrieval systems.

- Develops, implements, and monitors a strategic, comprehensive enterprise information security, IT risk and fraud management program. Develops and implements strategic security and fraud planning to achieve business goals by prioritizing defense initiatives and coordinating the evaluation, deployment, and management of current and future security technology using a risk-based assessment methodology.

- Acts as a primary advocate for the Department’s security vision through regular communication of security and fraud strategies and plans, to a broad range of stakeholders, including: the executive team, department heads, end users, partners and customers. Accountable for developing, implementing, maintaining, and overseeing the enforcement of policies, procedures, and associated plans for system security administration and user security systems, equipment, software, and other technologies based on industry-standard best practices. Creatively and independently provides resolution to security and fraud problems in a cost-effective manner. Creates education and awareness programs and advises the Department at all levels on security issues, fraud, best practices and vulnerabilities.

- Develops and enhances an information security management framework. Ensures the Cybersecurity Division has appropriate systems in place to monitor requests for release of personal and confidential information and that these are correctly evaluated and authorized, or denied, based on existing laws, regulations, and policies. Collaborates with the IT Divisions on enterprise technology development to fully secure information, computer, network and processing systems. Assesses and communicates all security risks associated with any and all purchases or practices performed by the Department. Promotes and oversees strategic security relationships between internal and external resources, including government entities, vendors, and partner organizations.

- Consults with and advises the CIO, executive staff, program managers, and Division Chiefs, on information security and fraud matters, including existing and emerging threats. Oversees the activities of the Cybersecurity Division with other branches and divisions involved in the security and confidentiality of the Department’s information assets, such as Labor Relations, Legal Office, and the Investigation Division.

- Represents the Department in coordinating information security issues and requirements with California state control agencies, federal agencies, other state and local agencies, and individuals. Keeps abreast of security incidents and acts as the primary lead on any information security incidents. Ensures all information technology and security related audits are kept focused on scope, tracked, and submitted on time. Provides guidance, evaluation, and advocacy on audit responses. Develops strategy for dealing with increasing numbers of audits and compliance checks.

- Oversees subordinate staff who manage risk and fraud assessments to identify potential vulnerabilities that could threaten the security of the Department’s information assets, and determine the probable loss or consequences of identified threats and assesses the likelihood of such occurrences. Keeps abreast of security incidents and acts as a primary lead on any information security incidents. Collaborates with post-incident reviews, oversees the development of action plans to reduce further exposure, and provides direction to subordinate staff who evaluate trends and weaknesses in EDD’s security program. May be involved in highly confidential investigations of employee misuse or policy violations, which may involve forensic investigation and testimony in court. Directs the design and implementation of technology recovery and business continuity plans, procedures, audits and enhancements.
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 Employment Development Department (EDD) enhances California's economic growth and prosperity by collaboratively delivering valuable and innovative services to meet the evolving needs of employers, workers, and job seekers. The EDD provides a variety of services to business, workers, and job-seekers. The department administers several multi-billion dollar benefit programs, including the Unemployment Insurance, Disability Insurance, and Paid Family Leave programs that provide financial stability to workers and their communities. Additionally, the EDD provides critical employment service programs to Californians, collects the state’s labor market information and employment data, and serves as one of the nation’s largest tax agencies through the collection of payroll taxes.

EDD’s ability to deliver services to the public and efficiently adapt to meet changing demand for those services, and the ability of the department to securely administer benefits programs containing the personal, private data of millions of Californians, is predicated on innovative technological solutions and the highest levels of data security.

The Cybersecurity Division Chief will directly support the EDD’s mission by establishing, developing and leading the department’s new Cybersecurity Division to initiate, design, develop, test, operate and defend EDD’s IT environments, and will direct efforts to prevent, restrict and address sources of disruption to EDD’s services to the public. The incumbent will perform a leading role in overseeing cybersecurity enhancements, suspicious activity monitoring tools, and staff training to proactively address cybersecurity vulnerabilities, threats and security findings, implement technology to mitigate benefit fraud, meet the increasing need in cyber risk management, and strengthen the EDD cybersecurity posture.
In addition, EDD is continuously audited by control agencies such as Department of Labor (DOL), Internal Revenue Services (IRS), CA State Auditors, CA Department of Military, CA Department of Technology (CDT), and other internal/external required audits. The creation of the new Cybersecurity Division directly supports the Administration's strategic goal of sustainable and secure business operations by addressing the immediate cybersecurity and fraud challenges EDD faces. This will also build long-term, sustainable, and flexible processes that will allow EDD to serve the people of California securely. This proposal will ensure that EDD addresses issues raised by the California State Auditor, Strike Team, California Cybersecurity Integration Center (Cal-CSIC) and the Legislature regarding cybersecurity.

The state's UI program has drawn significant attention due to the substantial service challenges faced during the pandemic. The new CEA will be responsible for securing EDD’s information systems and safeguarding information assets. The CEA will create, develop and, through subordinate managers, oversee the implementation of policies, procedures and tools to directly address compliance with the following statewide directives, federal laws, and guidelines to safeguard the EDD’s information, data, and technology:

- Executive Order B-34-15 – Increase California’s preparedness to respond to cyber-attacks
- Chapter 518, Statutes of 2015 (AB 670) – IT Security Assessments
- Chapter 508, Statutes of 2016 (AB 1841) – Cyber-security Incident Response Planning
- California Department of Technology Strategic Plan – Vision 2023
- 20 CFR §603.9(b) (1): Requires unauthorized access and disclosure of Unemployment Compensation (UC) data.
- Civil Code §1798.24(e): Requires agencies to keep an accounting of disclosures of personal information.
- SAM §5330: Requires each state entity to ensure compliance with information security requirements, both internally and externally.
- SAM §5335: Requires each state entity to continuously monitor its information systems for signs of suspicious or inappropriate activity.
- SAM §5335.1: Requires each state entity to implement a continuous monitoring program to facilitate ongoing awareness of vulnerabilities and to support risk management decisions.
- SIMM 5300-B: Foundational framework comprised of 30 priority security objectives to assist state entities with prioritization of their information security efforts.

The Cybersecurity Division Chief will report direct to the Information Technology Branch Deputy Director and will be an integral part of the Information Technology Branch Executive leadership team, along with the other Division Chiefs and the Deputy Director.

The scope of responsibility of the Cybersecurity Division Chief extends throughout the Cybersecurity Division but will directly impact all areas of the Information Technology Branch and the EDD’s other Branches, particularly the Unemployment Branch and Disability Insurance Branch, as these mission-critical services rely on the EDD’s technology as the platform.
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 Cybersecurity Division Chief will provide direction and be responsible for formulating and developing policies to strengthen governance and authority relating to Cybersecurity, impacting EDD’s public facing website, web accessibility, social media, mobile applications, internet applications, identity management, internal applications, and intranet. Specific examples of policy areas for which the CEA will be the principle policy maker include the following:

Integrated Risk Management and Governance Risk and Compliance:
The CEA will create and maintain policies to provide a comprehensive risk management and communication framework that includes risk appetite, risk calculation and risk assessment methodologies, risk acceptance criteria, and the identification of risk categories. These policies are needed to track cyber threat and fraud issues from identification through resolution, and to develop a strong IT security risk program to meet current and future IT security assessments and audit requirements. This will be accomplished, in part, through the creation and establishment of Integrated Risk Management (IRM) and Governance Risk and Compliance (GRC), which is necessary to support the EDD cybersecurity program efforts to identify, analyze, evaluate and treat information security risks. The CEA will establish, risk management policies that will address the deficiencies of EDD’s security governance and management cited by the CMD and CDT audits respectively.

Data Discovery and Classification:
The CEA will create and maintain Data Discovery and Classification policies that will allow EDD to be in accordance with SAM and SIMM policies of classifying all information assets (e.g. records, file, and/or databases). Each of these information assets requires categorization and classification for proper security controls to prevent unauthorized access or misuse. Currently, the Department is not in full compliance with the SAM and SIMM policies related to classifying all information assets; however, the CEA will create critical policies and develop the necessary procedures and automated tools, to assist in the classification of information systems and information assets, to allow EDD to be in compliance and to mitigate the risk of not having the appropriate safeguards in place to protect the information. These efforts to implement an enterprise-wide data discovery and classification program, will ensure that the EDD will be able to automatically classify and categorize information, automate remediation of data and applicable security permissions, and automatically prohibit data from being stored or processed on inappropriate assets. Failure to properly classify data will result in the Department being out of compliance with these SAM and SIMM policies as well as the Department not having the proper safeguards in place to prevent unauthorized access or misuse of information.

Security Assessment:
The CEA will create policies to ensure that the EDD meets its mandatory obligations in the area of Security Assessment. State agencies are mandated by SAM 5315.4 (revised in 2014) to develop and implement a system security test and evaluation plan. The EDD is further mandated by the IRS PUBLICATION 1075 to perform monthly vulnerability assessments of EDD’s applications due to their interaction with Federal Taxpayer Information (FTI). However, the EDD does not currently possess the tools and resources necessary to meet the SAM or IRS mandates to perform comprehensive security reviews of application code including third party libraries and publicly sourced code to identify and remediate potential exploitation points and system vulnerabilities. Software vulnerabilities are identified daily, and exploitation of those vulnerabilities are rapidly used by cyber criminals. The CEA will create critical Security Assessment policies in order to implement methodologies, testing tools, and software composition analysis, which will ensure that the EDD meets its mandates and protects the integrity of EDD data.
### C. ROLE IN POLICY INFLUENCE (continued)

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

As a member of EDD’s Executive Staff and the ITB Executive Team, the position has extensive decision-making authority and provides vision and leadership for developing and supporting security and fraud initiatives. The incumbent directs the planning and implementation of enterprise IT systems, business operations and facility defenses, against security breaches, vulnerability and fraud, to prevent, restrict and address sources of disruption ranging from natural disasters to malicious acts. The Cybersecurity Division Chief is designated as the EDD’s Information Security Officer (ISO) and Privacy Officer, and participates in executive-level policy and decision-making regarding the direction and effective application of IT to meet EDD’s business goals and objectives. The incumbent is the primary policy maker for Cybersecurity and works with other ITB divisions and other EDD programs to ensure cohesive and timely project implementation and continually evaluates processes for future policy and procedural revisions. Rapid advancements in technology, threats and risks in the Cybersecurity arena, and legislative changes and projects with strict deadlines; require agility in policy making to ensure EDD’s Cybersecurity policies continue to be compliant, effective and robust.

---

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

The Cybersecurity Division Chief will develop and implement, new enterprise-wide Cybersecurity policy pertaining to:

- Data Discovery and Classification.
- Security Assessment.

Additionally, the CEA will revise, expand upon, and implement existing policies pertaining to:

- Asset Protection.
- Contingency Planning.
- Incident Management.
- Policy and Procedure Development and Training.
- Privacy.
- Security Compliance.
- Security Engineering and Architecture.
- Security Operations.

The Chief will be responsible for implementing all cybersecurity related policies and ensuring they are meeting control agency standards. Failure to properly establish and hold fast to these policies could result in flawed business decisions, inaccuracies in benefit or overpayment collection strategies, damage to the Department’s reputation and overall negative impact to the labor workforce and the State of California as a whole.