Proposed
Department of Health Care Access and
Information Duty Statement

Employee Name Vacant	**Organization** Office of Technology Services Infrastructure and Operations Branch	
Position Number 441-175-1415-XXX	**Location** Sacramento	**Telework Option** Hybrid
Classification Information Technology Specialist III	**Working Title** Chief Enterprise Security Architect	

General Description

Under the broad administrative direction of Infrastructure and Operations Branch Chief, the Information Technology Specialist (ITS) III, Chief Enterprise Security Architect (CESA) is responsible for providing expert advisor level security architecture design and implementation in our programs and across our systems. This position will implement and oversee the maintenance of security solutions throughout the Department and cross-train the Security Operations Group (SecOps) in improving their daily operations. The incumbent will lead Information Security Architecture and performs a wide variety of tasks requiring innovative problem-solving where guidance is not readily available. The incumbent will typically work in the Information Security Engineering and System Engineering domains.

The incumbent serves as a key decision maker in the design and implementation of technology solutions for the Department. The CESA will lead the IT security governance team on the planning, development and implementation of the Department's roadmap to continually enhance security.

The incumbent will also serve as the technical lead for the SecOps team's efforts to monitor the Department's environment for potential threats. The ITS III serves as a Cybersecurity subject matter expert in developing standard procedures and improvements in our monitoring practices. The ITS II will also lead exercises to ensure all systems are logging the right information and that data is being stored based on State requirements.

The incumbent is responsible for overseeing that all security appliances are maintained to best practices, including but not limited to firmware and definition updates. The incumbent will maintain communication with business partners to ensure all security systems take advantage of applicable new features and properly configured security.

Supervision Received	Under broad administrative direction, incumbent reports to the Information Technology Manager II, Infrastructure and Operations Branch Chief.
Physical Demands	Must possess and maintain sufficient strength, agility, endurance, and sensory ability to perform the duties contained in this duty statement with or without reasonable accommodation.
Typical Working Conditions	Requires use of computing devices and phones, frequent faceto-face contact with management, staff, consultants and the public, verbal, written and digital (e-mail) communication, extensive review, analysis and preparation of electronic and written documents,

	assessment of practical demonstrations, mobility to various areas of the Department, occasional travel and overnight stays to training/conferences or the Los Angeles field office may also be required, and work hours may deviate from core business hours based on the service requirements of the Department

Job Duties
E = Essential, M = Marginal

40% E **Technical Security Governance, Monitoring, and Vulnerability Management**
Defines and maintains enterprise security technology roadmaps, ensuring alignment with statewide mandates such as **Cal-Secure** and **Zero Trust Architecture**. Designs and plans implementation strategies for Zero Trust principles across identity, network, and data layers. Oversees governance of security technologies, including architecture standards and lifecycle management. Leads advanced cybersecurity monitoring and vulnerability management activities, including proactive threat hunting, detection tuning, network forensics, and malware analysis to identify and mitigate risks. Establishes and enforces security logging and telemetry standards to meet State requirements. Creates and maintains artifacts supporting incident response, investigations, and compliance reporting. Conducts continuous vulnerability assessments, analyzes results, and advises IT teams on remediation strategies. Provides leadership and mentorship to SecOps staff on monitoring, incident response, and administration best practices. Coordinates security assessment exercises to identify systemic risks and ensure enterprise resilience.

30% E **Information Security Engineering**
Architects and integrates enterprise security tools to create a cohesive, resilient security ecosystem. Designs how disparate security technologies—such as identity management, endpoint protection, SIEM, DLP, and network security—work together to enforce Zero Trust principles and meet Cal-Secure objectives. Leads planning and implementation of new security solutions, ensuring they align with enterprise architecture standards and statewide mandates. Continuously evaluates existing tools, recommending and executing enhancements to improve interoperability, automation, and performance. Oversees lifecycle management of all security technologies, including configuration optimization, patching, firmware updates, and feature enablement to maintain peak operational condition. Collaborates with vendors and internal teams to validate architecture designs, troubleshoot integration issues, and ensure security controls are embedded across platforms. Provides technical leadership for complex deployments and modernization initiatives, ensuring security solutions scale with organizational needs and emerging threats.

20% E **Cybersecurity Incident Response**
Provides strategic guidance and coaching to SecOps and other team members during incident response activities, ensuring best practices and effective coordination. While day-to-day incident handling is led by other team members, the Chief Enterprise Security Architect serves as an escalation point and assumes leadership for the most critical or high-impact security incidents. Advises on

		containment, eradication, and recovery strategies to minimize organizational risk and ensure compliance with statewide and departmental policies. Collaborates with Senior IT leadership and communicates with executive stakeholders during major incidents. Oversees the development of incident response playbooks and ensures lessons learned are integrated into architecture and process improvements. Prepares and reviews detailed reports and artifacts documenting critical incident investigations and response actions.
5%	E	**Knowledge Management and Skill Development** Serves as a security expert and leader collaborating with other departmental experts and team members to develop and implement key strategic IT security initiatives including innovation and optimization opportunities. Researches and determines enterprise system design changes and change requirements needed to drive targeted business outcomes by understanding business drivers and business capabilities (Current State and Future State). Maintains awareness and expertise of current and emerging IT Security trends and technologies keeping abreast of industry standards, applying new and emerging processes and procedures with an emphasis on cloud architecture.
5%	M	Perform other related duties as required.

Other Expectations

- Demonstrate a commitment to performing duties in a service-oriented manner.
- Demonstrate a commitment to maintaining a work environment free from workplace violence, discrimination, and sexual harassment.
- Demonstrate a commitment to following best practices and applying office-wide standards throughout July 2023 Page 3 of 3 the organization.
- Demonstrate the ability to establish and maintain priorities, successfully complete work assignments, and meet deadlines as required.
- Show initiative in making work improvements, identifying, and correcting errors, and initiate work activities.
- Demonstrate the ability to gain and maintain the confidence and cooperation of others.
- Demonstrate a commitment to building an inclusive work environment that promotes HCAI's diversity, equity and belonging where employees are appreciated and comfortable as their authentic selves.
- Demonstrate a commitment to maintaining a work environment free from workplace violence, discrimination, and sexual harassment.
- Demonstrate a commitment to HCAI’s Mission, Vision, and Goals.
- Demonstrate a commitment to HCAI’s Core Values and Guiding Principles.
- Maintain good work habits and adhere to all HCAI policies and procedures.

To Be Signed by the Employee and Immediate Supervisor

I have read and understand the duties and expectations of this position

I have discussed the duties and expectations of this position with the employee.

Employee Signature/Date

Supervisor Signature/Date