

DUTY STATEMENT

BRANCH ENTERPRISE OPERATIONS SERVICES		POSITION NUMBER (Agency – Unit – Class – Serial) 368-406-1415-901			☐ CURRENT ☒ PROPOSED	
SECTION Information Technology		CLASSIFICATION TITLE Information Technology Specialist III				
PROGRAM (If applicable) Information Technology - Security		WORKING TITLE Knowledge Bank Information Security & Privacy Officer				
REGIONAL HUB Sacramento		COI Yes	WWG E	CBID R01	TENURE LT	TIME BASE FT
WORK SCHEDULE M-F 8am-5pm	SUPERVISION EXERCISED Yes	SPECIFIC LOCATION ASSIGNED TO 1400 10th Street, Sacramento, CA 95814				
INCUMBENT (If known)		EFFECTIVE DATE				
PRIMARY DOMAIN (IT positions only)		Information Security Engineering				

AGENCY OVERVIEW

The Governor's Office of Land Use and Climate Innovation (LCI) serves the Governor and his Cabinet as staff for long-range planning and research and constitutes the comprehensive state planning agency. LCI assists the Governor and the Administration in planning, research, policy development, and legislative analysis. LCI formulates long-range state goals and policies to address land use, climate change, population growth and distribution, urban expansion, infrastructure development, groundwater sustainability and drought response, and resource protection. LCI's budget programs include State Planning and Policy Development, Strategic Growth Council, California Volunteers, Racial Equity Commission, and Youth Empowerment Commission. LCI is a fast-paced, creative work environment that requires staff to have strong collaboration skills, the ability to respond quickly to changing policy needs, a positive attitude, and the ability to keep things light under pressure, proven commitment to creating a work environment that celebrates diverse backgrounds, cultures, and personal experiences.

GENERAL STATEMENT

Under administrative direction of the Governor's Office and Land Use and Climate Innovation (LCI) Information Technology Manager II, (Chief of Knowledge Bank and Platform Services), the Information Technology Specialist III (ITS III), Knowledge Bank Information Security and Privacy Officer serves as the lead privacy, data protection, security governance, and compliance analyst supporting the statewide Knowledge Bank initiative and related enterprise technology platforms.

The incumbent is responsible for leading enterprise privacy, data protection, and security governance activities to help ensure Knowledge Bank services, CEQA modernization systems, permitting coordination capabilities, cloud environments, public-facing systems, operational workflows, vendor solutions, and supporting infrastructure comply with State of California privacy laws, security requirements, audit standards, accessibility mandates, records management obligations, and enterprise governance frameworks.

The position supports statewide modernization initiatives by integrating privacy-by-design, security-by-design, accessibility, records management, operational governance, auditability, and compliance requirements into Knowledge Bank operations, application development efforts, procurement activities, enterprise workflows, service design, release planning, vendor oversight, and long-term technology planning while coordinating closely with the department's Information Security Office and enterprise security leadership. This position will also serve as a liaison between LCI program areas, agency partnerships, and third-party providers.

% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. <i>(Use addition sheet if necessary)</i>
-----------------------------	---

DUTY STATEMENT

100%	ESSENTIAL FUNCTIONS
35%	Risk Management, Privacy and Data Protection Oversight - Serves as the lead privacy and data protection officer for the statewide Knowledge Bank initiative, CEQA modernization, permitting coordination capabilities, and related enterprise technology platforms. - Develops, implements, and maintains enterprise governance frameworks, operational privacy controls, data protection standards, confidentiality procedures, and compliance practices supporting Knowledge Bank services, public-facing systems, regulated workflows, and statewide operational requirements. - Ensures Knowledge Bank applications, operational workflows, cloud environments, SaaS solutions, public-facing systems, integrations, and data-sharing activities comply with applicable privacy laws, information security requirements, accessibility mandates, records management requirements, and statewide governance standards. - Leads CEQA risk impact assessments, data classification reviews, confidential information evaluations, records management reviews, and enterprise data protection assessments for Knowledge Bank implementation, CEQA modernization, permitting coordination capabilities, and operational activities. - Reviews enterprise data collection, storage, transmission, retention, sharing, disposal, and access management practices to ensure proper handling and protection of sensitive, confidential, regulated, and operationally controlled information. - Develops and maintains enterprise privacy documentation, including privacy procedures, operational standards, compliance tracking artifacts, governance documentation, data handling guidance, and enterprise privacy policies. - Identifies privacy risks, operational vulnerabilities, governance gaps, unauthorized data exposure risks, and compliance concerns affecting Knowledge Bank services and related enterprise operations and recommends corrective actions and mitigation strategies. - Ensures security-by-design, data minimization, and least-privilege principles are incorporated into enterprise modernization initiatives, operational workflows, public-facing applications, vendor solutions, and business processes. - Coordinates with ITU and security leadership, legal staff, executive leadership, business units, procurement personnel, project teams, vendors, and technical teams regarding security and privacy compliance requirements, data-sharing agreements, records management obligations, confidentiality expectations, and operational governance activities. - Monitors enterprise operational compliance with statewide security standards, confidentiality requirements, accessibility regulations, records responsibilities, and operational governance obligations. - Aligns CEQA knowledge bank risk management engagements using current LCI security policies and procedures.

DUTY STATEMENT

30%	Security Governance, Risk Management, and Compliance - Leads enterprise security governance, risk management, and compliance oversight activities supporting the statewide Knowledge Bank initiative, CEQA modernization, permitting coordination capabilities, and related enterprise operational environments. - Interprets and applies to State of California security and privacy policies, including State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), California Department of Technology (CDT) policies, Zero Trust principles, accessibility requirements, and statewide information security standards. - Conducts enterprise security assessments, operational risk analyses, compliance reviews, control evaluations, and governance assessments associated with Knowledge Bank services, enterprise applications, cloud environments, vendor solutions, and modernization projects. - Reviews and evaluates enterprise operational controls, including identity and access management, logging and monitoring practices, encryption standards, secure data handling practices, role-based access controls, privileged access, and enterprise audit logging requirements. - Coordinates vulnerability management activities, remediation tracking, security review activities, control validation, and operational compliance monitoring associated with Knowledge Bank applications and supporting environments. - Supports implementation and monitoring of LCI's security program's Zero Trust Architecture principles, cloud security governance, secure configuration management, operational risk management, and enterprise security best practices. - Ensures Knowledge Bank modernization initiatives incorporate appropriate operational controls, privacy safeguards, audit capabilities, security monitoring practices, accessibility requirements, records considerations, and compliance validation activities. - Identifies security risks, control gaps, operational vulnerabilities, compliance concerns, and audit readiness issues, and recommends mitigation strategies to project leadership, technical teams, vendors, and enterprise security leadership. - Supports development and maintenance of System Security Plans (SSPs), incident response procedures, disaster recovery documentation, business continuity artifacts, privacy documentation, and enterprise governance materials for Knowledge Bank services and related platforms. - Promotes enterprise privacy awareness, operational compliance practices, security governance standards, confidentiality obligations, and secure data handling expectations through stakeholder guidance, communication, training support, and coordination efforts.
15%	Security and Privacy Architecture Review, Procurement, and Project Support - Reviews enterprise application architectures, cloud solutions, SaaS platforms, APIs, operational workflows, vendor solutions, and system integrations to evaluate privacy, confidentiality, security, accessibility, records, and compliance impacts. - Participates in project planning activities, procurement reviews, architectural discussions, operational readiness reviews, implementation planning sessions, release planning activities, and modernization governance activities to ensure privacy and security requirements are integrated throughout the project lifecycle.

DUTY STATEMENT

15%	- Reviews Statements of Work (SOWs), vendor security documentation, privacy documentation, implementation plans, contract language, data-sharing practices, system diagrams, and architectural diagrams to ensure alignment with statewide security, privacy, accessibility, records management, and compliance requirements. - Coordinates with technical teams, infrastructure staff, application teams, business programs, procurement staff, legal staff, and vendors regarding secure system design, privacy safeguards, operational controls, compliance expectations, and enterprise governance requirements. - Supports development and implementation of enterprise security architecture standards, privacy governance controls, data protection practices, and operational security practices supporting the Knowledge Bank, CEQA modernization, permitting coordination capabilities, and related enterprise platform operations. Interagency Coordination, Payment Security, and Regulatory Compliance - Coordinates closely with State departments, local agencies, control agencies, vendors, business programs, and external stakeholders as additional permitting functions, enterprise workflows, integrations, public-facing services, and operational capabilities are incorporated into the Knowledge Bank and related enterprise platforms. - Provides security and privacy oversight for enterprise business functions involving fee collection, payment processing, financial transactions, revenue tracking, confidential financial information, customer account management, and integration with financial or payment-related systems. - Ensures enterprise solutions supporting payment collection, financial workflows, customer transactions, and related services comply with State security requirements, privacy regulations, audit standards, records management obligations, and applicable financial security controls. - Reviews operational and technical designs associated with financial transactions, payment gateways, data-sharing activities, customer account management, system integrations, and enterprise reporting to ensure secure handling of confidential, financial, and regulated information. - Coordinates with fiscal staff, procurement personnel, legal teams, vendors, security staff, technical teams, and external agencies regarding operational security controls, privacy requirements, data protection standards, and compliance obligations related to financial and payment processing activities. - Supports implementation of secure operational controls involving identity and access management, encryption standards, audit logging, transaction monitoring, data retention, fraud prevention, secure data transmission, and least-privilege access practices associated with enterprise permitting and payment services. - Evaluates operational risks and compliance impacts associated with onboarding new agencies, expanding permitting coordination capabilities, integrating financial services, implementing customer-facing functions, and adding new data-sharing or transactional services. - Provides security and privacy guidance to project teams, business stakeholders, partner agencies, and enterprise leadership regarding interagency operational governance, confidential information handling, financial system security, payment security, data protection,
------------	--

DUTY STATEMENT

	and enterprise compliance requirements. Provides recommended mitigation, transfer, or acceptance strategies to the risk register for tracking key performance indicators (KPIs) to key risk indicators (KRIs) to meet the LCI business risk tolerance and appetite strategies
	MARGINAL FUNCTIONS
5%	Performs other job-related duties as required to support Knowledge Bank security, privacy, operational governance, compliance activities, modernization initiatives, audit coordination efforts, emergency response activities, and organizational priorities.
KNOWLEDGE AND ABILITIES Knowledge of: Development and application of technology in the current and future business environment; emerging technologies and their applications to business processes; policy development; and applications and implementation of information systems to meet organizational requirements. Ability to: Research and identify best practice methods and processes to identify current and emerging trends in technology and recommend appropriate courses of action.	
DESIRABLE QUALIFICATIONS - Experience with risk management processes (e.g., methods for assessing and mitigating risk). - Experience with frameworks, laws, regulations, policies, and ethics related to cybersecurity and privacy. - Applicable business processes and operations of customer organizations. - Business continuity and disaster recovery continuity of operations plans. - Vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). - Information security program management and project management principles and techniques. - Prior CISO/ISO and Privacy Officer experience. - Currently certified in one or more of the following: CISM, CRISC, CDPSE. - Experience with the State Administrative Manual (SAM) resource and compliance requirements. - Experience with Office of Information Security (OIS), State Information Management Manual (SIMM) compliance requirements. - Information Security Assessments and Information Security Program Audit processes. - Managed or led all security program control initiatives across administrative, physical, and technical domains. - Governance, Risk, and Compliance audit preparedness. - Ability to integrate information security requirements into the acquisition process, using applicable baseline security controls as one of the sources for security requirements, ensuring a robust software quality control process. - Ability to identify critical infrastructure systems with information and communication technology that were designed without system security considerations. - Experience writing technical documentation for workflows, plans, guidelines, policies, standards and procedures to meet business requirements for security assurance and compliance.	

DUTY STATEMENT

SPECIAL PERSONAL REQUIREMENTS • Ability to maintain consistent attendance • Ability to demonstrate punctuality, initiative, and dependability • Ability to work independently, while working with others in a small group environment		
SPECIAL PHYSICAL CHARACTERISTICS: Persons appointed to this position must be reasonably expected to lift, carry, push, pull, or otherwise move objects weighing up to 30 lbs. with or without a reasonable accommodation. This position involves sitting most of the time and may involve walking or standing for brief periods of time. This position may be eligible to participate in LCI's hybrid telework schedule. Participation in telework is subject to LCI's guidelines. Occasional extended hours outside of normal working business hours may be required.		
The statements contained in this duty statement reflect general details as necessary to describe the principal functions of this job. It should not be considered an all-inclusive listing of work requirements should not be considered. Individuals may perform other duties as assigned, including work in other functional areas to cover absence of relief, to equalize peak work periods or otherwise balance the workload.		
SUPERVISOR'S STATEMENT: <i>I HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE AND HAVE PROVIDED A COPY OF THE DUTY STATEMENT TO THE EMPLOYEE.</i>		
SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE
EMPLOYEE'S STATEMENT: <i>I HAVE READ AND UNDERSTAND THE DUTIES LISTED ABOVE AND CAN PERFORM THESE DUTIES WITH OR WITHOUT REASONABLE ACCOMMODATION. (IF YOU BELIEVE REASONABLE ACCOMMODATION IS NECESSARY, DISCUSS YOUR CONCERNS WITH YOUR HIRING SUPERVISOR. IF UNSURE OF A NEED FOR REASONABLE ACCOMMODATION, INFORM YOUR HIRING SUPERVISOR, WHO WILL DISCUSS YOUR CONCERNS WITH HUMAN RESOURCES OFFICE).</i>		
EMPLOYEE'S NAME (Print)	EMPLOYEE'S SIGNATURE	DATE