STATE OF CALIFORNIA
GOVERNOR'S OFFICE OF LAND USE & CLIMATE INNOVATION
HRO-19 (REV 06/2026)

DUTY STATEMENT

BRANCH ENTERPRISE OPERATIONS SERVICES		POSITION NUMBER (Agency – Unit – Class – Serial) 368-403-1414-903				☐ CURRENT ☐ PROPOSED
PROGRAM INFORMATION TECHNOLOGY		CLASSIFICATION TITLE Information Technology Specialist II				
SECTION/UNIT (If applicable) INFORMATION SECURITY UNIT		WORKING TITLE Network Security Operations Engineer				
REGIONAL HUB Sacramento		COI Yes	WWG E	CBID R01	TENURE LT	TIME BASE FT
WORK SCHEDULE M-F 8am-5pm	SUPERVISION EXERCISED None	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, and Racial Equity Commission. LCI is a fast-paced, creative work environment that requires staff to have strong collaboration skills, an ability to quickly respond to changing policy needs, and a positive attitude and sense of humor. Proven commitment to creating a work environment that celebrates diverse backgrounds, cultures, and personal experiences.

GENERAL STATEMENT

Under general direction of the Information Technology Manager II (Chief Information Security Officer), the Information Technology Specialist II (Network Security Operations Engineer) performs a variety of complex technical tasks related to identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techniques.

The position serves as the department's subject matter expert for enterprise network and security operations and provides technical expertise supporting the organization's cybersecurity objectives. The IT Specialist II supports and coordinates security controls, security governance initiatives and operational information technology security activities, including the troubleshooting and resolution of complex security-related issues

% 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. *(Use addition sheet if necessary)*
100%	**ESSENTIAL FUNCTIONS**
35%	**Network Security and Operations** Responsible for implementation, maintaining and operation of network infrastructure and its security operations and maintenance. Support the network design for security controls and implement network security best practices. Serve as-a-liaison on to network and firewalls for systems and network operations, vendors and/or third-party providers. Provide on-site and remote security, network and firewalls technical assistance to other IT resources and customers at network support tiers 1, 2, and 3. Troubleshoot network problems and outages, scheduling upgrades, and collaborating with other teams

DUTY STATEMENT

	on network optimization. Diagnose network connectivity problems while improving capacity and performance. Troubleshoot network failures and change network components as required to maintain/restore network operations. Test network infrastructure, including software and hardware devices in a cloud or on premises to meet production systems resilience. Monitor and improve the security of the LAN and WAN traffic and connectivity to maintain acceptable service levels. Analyze enterprise security threats, vulnerabilities, and attack vectors impacting network operations and recommend risk mitigation strategies to management and stakeholders. Analyze bandwidth and requirements of applications including imaging, electronic data interchange, database applications, productivity and workgroup/workflow software. Perform packet captures and analyzes information to determine and resolve connectivity issues. Define and maintain network standards for hardware and software. Plan for and make recommendations to accommodate anticipated access, bandwidth and power requirements for network systems. Advise management on strategic network security planning, future-state architecture, and infrastructure investments necessary to support evolving business and security requirements. Improve the security of and perform configuration and installation of all routers, firewalls, DNS security, wireless access points, DoS/DDoS, Anti-Chatbots, honeypots/honeynets and switching products utilized in the environment including web application firewalls, next generation firewalls, and load balancers. Provision, configure and manage network and firewall devices on-perm and in a cloud environment. Patch network vulnerabilities based on LCI risk tolerance postures.
35%	**Security Operations** Monitor and manage critical LCI security operation technologies including but not limited to cloud infrastructure, intrusion detection and prevention software, anti-ransomware agents, host-based protection technologies, 0-day and APT mitigations (sandboxing, honeypot, behavioral monitoring, etc.), packet capture and metadata analysis, MDR/XDR/EDR, penetration testing, vulnerability management, DLP, secure email, etc. Detect, triage, investigate and conduct root cause analysis of security incidents, active attacks, and/or operational issues. Actively monitor, assess and recommend tactical and strategic initiatives based on new and emerging threats posing risk to on-prem and cloud computing environments. Apply knowledge, skill, and abilities to detect attacks or compromised assets including, but not limited to, threat tactics/techniques/procedures, in-depth knowledge of security network architecture, in-depth knowledge of IT platform operations (e.g. Windows, Linux, Mac, network devices.), vulnerability exploits and management, methods of access and related controls, encryption, etc. Manage external engagement including scheduling, project management, and coordination with technical and security staff across LCI and agency/entity departments for security related tasks. Lead and coordinate security incident response (IR) process to identify, contain, eradicate, and recover from information security incidents. Conduct root cause investigations, develop corrective action recommendations and post incident reporting. Participate in the procurement and engagement of outsourced security resources if/as needed to meet the IR objectives. Analyze security services (infrastructure, application, identity, remote access solutions) of existing and planned cloud infrastructures (Infrastructure as a Service (IaaS), Platform as a Service (PaaS)). Secure business applications and computing environments across on-prem, public, private or hybrid cloud infrastructures. Maintain a consistent, secure environment using configuration management solutions.

DUTY STATEMENT

25%	**Security Compliance** Ensure all technical security controls meet the organization's system security plans and the governance risk and compliance (GRC) platform business objectives. Oversee the security programs technical controls to ensure compliance with various security models and supported frameworks that include Cal Secure, CIS, CRF, NIST, CSF2.0, OWASP, MITRE, State Administrative Manual (SAM) policies and supported Statewide Information Management Manual (SIMM) standards. Provide secure business solutions to improve the risk tolerance for risk mitigation and acceptance measures. Advise management, business units, and stakeholders regarding information security risks, compliance obligations, compensating controls, and risk treatment options to support informed business decisions. Stay apprised of current and proposed security changes impacting regulatory, privacy and security industry best practice guidance. Provided recommended mitigation, transfer or acceptance strategies to the risk register for tracking key performance indicators (KPI)s to key risk indicators (KRI)s to meet the LCI business risk tolerance and appetite strategies. Protect business applications in compliance with privacy, security, business resiliency and compliance frameworks as defined in corporate policies. Apply learned knowledge across key lines of business, including products, practices and procedures to meet the security programs business objectives. Develop, review and recommend modifications to security standards, system security plans, security guidelines and procedures to ensure compliance with statewide requirements, industry best practices, and departmental security objectives.
	MARGINAL FUNCTIONS
5%	Perform other job-related duties as required.

KNOWLEDGE AND ABILITIES

Knowledge of: Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the State of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and state and federal privacy laws, policies, and standards.

Ability to: Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions; foster a team environment through leadership and conflict

DUTY STATEMENT

management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

DESIRABLE QUALIFICATIONS

- Skill and experience in the technical domains of System Engineering,

  Software Engineering, IT Project Management, and Information Security Engineering.
- One or more of the following security certifications: CompTIA: Cloud +, Network+, Security +, SANS: GCIA, GMON, GPEN, GWAPT, GCTD, GCPN, GCFR, GREM. Cisco Certified Network Associate (CCNA), ISC2: CISSP, CCSP: Azure: Azure Security Engineer and or Associate.
- Experience with Microsoft Sentinel, Defender, or other EDR solutions/SIEMs.
- Experience in leading security investigations to lessons learned activities.
- Experience in offensive security testing.
- Experience with application security.
- Strong communication skills to clearly express ideas and concepts, both written and verbally.
- Ability to perform in a lead and supporting role and take responsibility for mission-critical secure infrastructure components.
- High degree of knowledge and experience in the cybersecurity kill chain to mitigate thread adversary techniques, tactics, and procedures.
- Experience with Cisco ISE/DNA, HP Aruba ClearPass Policy Manager, Network Address Translation/Internet Protocol (NAT/IP), Cisco switches, Extreme switches, Juniper and Aruba networks, firewall and demilitarized zone (DMZ) (Perimeter Network) using Palo Alto firewall and Palo Alto web filtering and Prisma SASE.
- Ability to perform in a lead role and take responsibility for mission-critical secure infrastructure components that include security vulnerability and end point protection risk assessments.
- Skill in identifying software communications vulnerabilities. Skill in identifying, capturing, containing and reporting malware.
- Experience writing technical documentation for workflows, system security plans (SSP), standards and procedures to meet business requirements for security assurance and compliance.

SPECIAL PERSONAL REQUIREMENTS

- Ability to maintain consistent attendance
- Ability to demonstrate punctuality, initiative, and dependability

SPECIAL PHYSICAL CHARACTERISTICS

Persons appointed to this position must be reasonably expected to lift, carry, push, pull, or otherwise move objects weighing up to 10 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.

STATE OF CALIFORNIA
GOVERNOR'S OFFICE OF LAND USE & CLIMATE INNOVATION
HRO-19 (REV 06/2026)

DUTY STATEMENT

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. 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 HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE AND HAVE PROVIDED A COPY OF THE DUTY STATEMENT TO THE EMPLOYEE.***		
SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE
EMPLOYEE'S STATEMENT: ***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).***		
EMPLOYEE'S NAME (Print)	EMPLOYEE'S SIGNATURE	DATE