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) 368-403-1415-901				☐ CURRENT ☐ PROPOSED
PROGRAM INFORMATION TECHNOLOGY		CLASSIFICATION TITLE Information Technology Specialist III				
SECTION/UNIT (If applicable) INFORMATION SECURITY UNIT		WORKING TITLE Cloud Network Security Operations Engineer				
REGIONAL HUB Sacramento		COI Yes	WWG E	CBID M01	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 administrative direction of the Information Technology Manager II (Chief Information Security Officer) , the Information Technology Specialist III (Cloud Network Security Operations Engineer) performs a variety of complex level tasks in relation to the responsibility of identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techniques. This position will support and or maintain cloud security, network security and security operational activities to include secure cloud infrastructure, network controls, network firewalls, incident response, end point protection, penetration testing, vulnerability management, anti-phishing, security awareness training and technical security governance risk and compliance initiatives. This position is a senior subject matter expert and will serve as a liaison between LCI and third-party providers. The incumbent will communicate and actively maintain working relationships with customers for various security controls, security governance and operational information technology security troubleshooting purposes.

% 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**
30%	**Cloud Security** Develop and maintain secure, resilient enterprise-grade cloud processes in tandem with LCI's ITU architects and system engineers. Secure business applications and computing environments across public, private or hybrid cloud infrastructures. Protect business applications in compliance with privacy, security, business resiliency and compliance frameworks as defined in LCI's security policies.

DUTY STATEMENT

	Configure Azure and MS365 are based on best security technical standards. Maintain a consistent, secure environment using configuration management solutions. Conduct rigorous oversight of security systems and security configuration administration to reduce risk to enterprise systems and accounts. Deploy strong identity and access management (IDAM) controls across applications and computing environments. Assist with the development, maintenance and utilization of scripts (e.g., PowerShell, Python, Ruby, etc.) to support custom extract transform load (ETL) tools with a security focus for data flow. Actively monitor, assess and recommend tactical and strategic initiatives based on new and emerging threats posing risk to cloud computing environments.
30%	**Network Security** 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 for network and firewalls for systems and network operations, vendors and/or third-party providers. Provide on-site and remote security, network and firewall technical assistance to other IT resources and customers. Maximize network performance by monitoring performance, troubleshooting network problems and outages, scheduling upgrades, and collaborating with other teams on network optimization. Monitor and improve the security of the LAN and WAN traffic and connectivity to maintain acceptable service levels. 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. Troubleshoot network failures and change network components as required to maintain/restore network operations. 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. 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-premise and in a cloud environment. Troubleshoot network failures and change network components as required to maintain/restore network operations.
20%	**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-premise 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.

DUTY STATEMENT

	Manage external engagement including scheduling, project management, and coordination with technical and security staff across LCI and agency/entity departments for security related tasks. Participate and support the security incident response (IR) process to identify, contain, eradicate, and recover, as well as root cause investigations 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, including Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Secure business applications and computing environments across on-premise, public, private or hybrid cloud infrastructures. Maintain a consistent, secure environment using configuration management solutions.
15%	**<u>Security Compliance</u>** 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. 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 (KPIs) to key risk indicators (KRIs) 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 program's business objectives. Participate in and support in creating and modifying written documentation that includes security standards, system security plans, security guidelines and supported procedures.
	MARGINAL FUNCTIONS
5%	Perform other job-related duties as required.

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.

DUTY STATEMENT

DESIRABLE QUALIFICATIONS:

- Experience writing technical documentation that includes system security plans, network flow diagrams, security standards and procedures.
- Demonstrated problem-solving abilities to manage complex state, local and international security requirements.
- Successful track record collaborating with technical and non-technical teams to promote ideas to support business enablement.
- Skill in mentoring and operationally leading security team members.
- Skill in identifying software vulnerabilities.
- Skill in identifying, capturing, containing and reporting malware and ransomware.
- Experience with HP Aruba ClearPass Policy Manager, Network Address Translation/Internet Protocol (NAT/IP), Cloudflare network security solutions, Cisco switches, Extreme switches, Aruba networks, firewall and demilitarized zone (DMZ) (Perimeter Network) using Palo Alto firewall and Palo Alto web filtering, Prisma SASE and or the equivalent.
- Experience with application security.
- Experience with Microsoft Sentinel, Defender, or other EDR solutions/SIEMs.
- Experience in offensive security testing.
- Experience in leading security investigations to lessons learned activities.
- Experience in architecting and engineering MS Azure infrastructure cloud platforms that include M365, access management, Azure, Purview, eDiscovery and zero-trust principles.
- Skill in applying white-box and black-box software testing.
- Skill and experience in the cybersecurity kill chain to mitigate thread adversary techniques, tactics, and procedures.
- Strong communication skills to clearly express ideas and concepts, both written and verbally.
- Ability to perform in a support role and take responsibility for mission-critical secure infrastructure components that include network security, asset vulnerability, security assessment and end point protection risk assessments.
- One or more certifications in cloud, network and security operations of the following: Azure: MS Cybersecurity Architect Expert, Azure Security Engineer Associate, CompTIA: Cloud+, CompTIA Security+, ISC2: CISSP, CCSP, SANS: GCIA, GMON, GPEN, GWAPT, GCTD, GCPN, GCFR, GREM and GCSA.
- Experience writing technical documentation for workflows, plans, guidelines, policies, 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
- Ability to work independently, while working with others in a small group environment

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

DUTY STATEMENT

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.

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