Office of Systems Integration
"SERVING CALIFORNIA"

☐ Current
☒ Proposed

DUTY STATEMENT

1. POSITION INFORMATION

Civil Service Classification Information Technology Specialist III	Working Title Cyber Defense Advisor
Employee Name Vacant	Position Number 791-500-1415-901
Project/Division Name CHHSA, Office of Information Officer (OAIO)	Supervisor's Name Lloyd Indig
Unit Click here to enter text.	Supervisor's Classification Information Technology Manager II
Physical Work Location 10390 Peter A McCuen Boulevard, Mather, CA 95655	Duties Based on: ☒ Full Time ☐ Part Time - Fraction
Effective Date TBD	

2. REQUIREMENTS OF POSITION

Check all that apply:

☒ Conflict of Interest Filing (Form 700) Required
☒ Requires Fingerprinting & Background Check
☒ May be Required to Work in Multiple Locations
☐ Other *(specify below in Description)*

Description of Position Requirements *(e.g., the position may move from project to project upon business need, managing staff at an alternate location, graveyard/swing shift, frequent travel, etc.)*:

The position physically reports to the California Office of Emergency Services (Cal OES) at 10390 Peter A McCuen Boulevard, Mather, CA 95655. Work is conducted in a professional office environment. Business dress, according to current (Cal OES) office policy, is required. This position requires the ability to work excess hours, to effectively work under pressure to meet deadlines, use of a computer to communicate and prepare written materials, and the ability to travel to meetings, training, and conferences at various locations. Additionally:

1. EMERGENCY OPERATIONS – ACTIVATION/ OPERATIONAL ASSIGNMENT UP TO 100% AT VARIOUS TIMES:
    a. When requested to fill an operational assignment and until demobilized, the following duties will be performed, and your regular duties may temporarily cease:
    b. May be required to work in the State Operations Center (SOC), Regional Emergency Operations Center (REOC), Joint Field Office (JFO), Area Field Office (AFO), Local Assistance Center (LAC), or other location to provide assistance in emergency response and recovery activities. All staff are required to complete operational related training and participate in one of three (3) Readiness Teams that rotate activation availability on a monthly basis if not assigned to an Operational Branch (e.g., Fire/ Law/ Region/ PSC Operations (Technicians)/ PSC Engineering (Engineers). May be required to participate in emergency drills, training and exercises.
    c. Staff need to work effectively under stressful conditions; work effectively & cooperatively under the pressure of short leave time; work weekends, holidays, extended and rotating shifts (day/night). Statewide travel may also be required for extended periods of time and on short notice.
    d. While fulfilling an operational assignment it is important to understand that you are filling a specific "position" and that position reports to a specific Incident Command System (ICS) hierarchy. This is the chain of command that you report to while on this interim assignment.
    e. On Call/Standby/Duty Officer (if applicable)
    f. If assigned on-call, standby or as a Duty Officer, you are required to be ready and able to respond immediately to any contact by Governor's Office of Emergency Services (Cal OES) Management (including contact from the State of California Warning Center) and report to work in a fit and able condition if necessary as requested.
2. AFTER HOURS: Employee may occasionally be contacted for after-hours emergency support.
3. TRAVEL: Employee is required to operate a State vehicle during the course of deployment as part of employment. Employee may be required to travel to respond to IR incidents at various sites within California.
4. TRAINING: Employee is required to successfully complete all training related to the functions of the job.
5. CERTIFICATION: Employee shall obtain a CompTIA Security +, GIAC Security Essentials, or equivalent certification within six (6) months of hire date as a condition of employment.

6. SECURITY CLEARANCE: Employee must pass a "CHHS" or other required entity background check. In addition, employee shall obtain a SECRET Homeland level security clearance within six (6) months of hire date and maintain the clearance to work in secured areas.

3. DUTIES AND RESPONSIBILITIES OF POSITION

IT Domains used:

☐ Business Technology Management	☐ Information Technology Project Management
☐ Client Services	☐ Software Engineering
☒ Information Security Engineering	☐ System Engineering

Summary Statement:

Under the administrative direction of the California Health and Human Services (CHHS) Agency Information Security Officer (AISO), Information Technology Manager II (ITM II), the Information Technology Specialist III (ITS III) serves as a specialized technical advisor on Cybersecurity threats to the CHHS Agency and government and non-government entities. The ITS III will report directly to and receive most assignments from the California Cybersecurity Integration Center (Cal-CSIC) Cyber Operations Branch Chief, ITM II; however, direction and assignments may also come from a designated Team Lead. The ITS III will represent the CHHS as a Cyber Defense Advisor on the California Cybersecurity Integration Center (Cal-CSIC) team as part of the Homeland Security partnership.

The Cal-CSIC serves as the central organizing hub of the state government's cybersecurity activities. Additionally, the Cal-CSIC's mission is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, including public and private sector computer networks in the state. The Cyber Operations Branch provides the following services to the Cal-CSIC: Incident Response, Compromise Assessment, Incident Response Planning and Training, and Digital Forensics Lab.

The Cyber Defense Advisor will provide guidance and advice to the CHHS Agency on methods to investigate, document, and report on cybersecurity issues and emerging trends, and will provide actionable technical and tactical cyber information and intelligence to federal, state, local, tribal, and territorial (SLTT) governmental and private sector partners through ad hoc reports, briefings, and presentations. The incumbent will work with the Cal-CSIC and OES teams using cutting-edge security technology to create relevant and timely cyber threat products including advisories, recommended actions, and bulletins to assist California and partner entities to include Multi-State Information Sharing and Analysis Center (MS-ISAC), federal and SLTT personnel, and assist in applying prescribed analytical standards.

Percentage of Duties	Essential Functions
40%	As a subject matter expert in cybersecurity, the ITS III will: • Research, identify, evaluate, and monitor cybersecurity threats and the impact of those threats to the state's health and human services sector (government and non-government entities). • Research, document, and develop reusable cybersecurity defense procedures/playbooks in identifying and analyzing cybersecurity threats for the state's health and human service sector. • Provide cybersecurity recommendations and advice to senior executive leadership based on the identified threats and vulnerabilities. • Provide advice and input for Incident Response, Disaster Recovery, Contingency, and Continuity of Operations Plans to senior executive leadership to proactively prepare for and prevent future security incidents. • Research, identify, evaluate, and monitor compliance requirements including: The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, etc. as it relates to industry requirements and impact to cybersecurity.
25%	As a specialized advisor with master-level knowledge in security technology the ITS III will: • Assess and recommend the appropriate security controls to senior executive management and describe how the controls are employed within the CHHS entities information systems and its environments of operation to the health and human services sector. • Analyze cybersecurity threat intelligence collected from a variety of the most cutting-edge resources to determine patterns and trends within the State. • As required, support and assist State (Cal-CSIC; CDT-SOC; CHP-CCIU) Federal (MS-SAC; DHS; FBI), Regional: (RFCs), Local (STAS), Private Sector: (3rd party cybersecurity resources), and others. Facilitates the building of situational threat awareness and sharing of related intelligence to: o Create an integrated analysis of threat trends and events. o Identify and assist with the mitigation of knowledge gaps.

	○ Suggest methods to degrade or mitigate adversary threat. ○ Proactively prepare for and prevent future incidents
15%	As an expert in cybersecurity threats, the ITS III will perform incident handling tasks to act against cyber-security threats using cutting-edge cyber-security tools and analysis. **Incident Response:** • Assist the impacted state or non-state sector with security incidents or urgent situations to mitigate immediate and potential threats using playbook and security techniques. • Assist law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and agencies responsible for advancing information security within state government. • Perform incident handling tasks (e.g., triage, forensic collections, intrusion correlation and tracking, threat analysis, and remediation) on a tactical incident response team deployable to various locations within the state of California in direct support of incident response efforts as outlined by Government Code 8586.5. • Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. • Formulate strategies and provide advice to the health and human services sector on how best to utilize state and local resources and capabilities in a timely, effective manner to speed recovery. **Threat Response:** • As required, support and assist Local (Local law enforcement), State (Cal-CSIC; CHP-CCIU; CMD-CMF), Federal (FBI Cyber Division; DHS NCCIC) and others. Activities include supporting the appropriate law enforcement investigative activities for: ○ Collecting evidence and gathering intelligence to provide attribution. ○ Linking related incidents and identifying additional possible affected entities. ○ Identifying threat pursuit and disruption opportunities. ○ Developing and executing courses of action to mitigate the immediate threat and facilitating information sharing and coordination with Asset Response efforts. ○ Use data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze cybersecurity events that occur within their environments for the purposes of mitigating threats. **Asset Response:** • As required, support and assist State (CDT-SOC; Cal-CSIC; CMD-CMF), Private Sector (3rd party cybersecurity resources) and others. Activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents by: ○ Identifying other entities possibly at risk and assessing their risk to the same or similar vulnerabilities. ○ Assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks. ○ Facilitating information sharing and operational coordination with Threat Response for the affected Entity Response. ○ As required, support and assist Entity (ISO; IT staff; Management teams; Cybersecurity staff), Private Sector (3rd party cybersecurity resources) and others. Activities include: Sharing information surrounding the event with other cybersecurity advisors to assist with the investigative, analysis, response, and recovery phases of cyber incident response in order for the affected entity as the data owner to retain responsibilities to ensure appropriate actions and safeguards are in place to remediate threats and secure their information.
15%	As a specialized advisor with master-level knowledge in security technology, the ITS III will facilitate and collaborate with the Cal-CSIC and OES team to develop a statewide cybersecurity strategy on Cybersecurity and in accordance with state and federal requirement, standards, and best practices. This includes: • Developing and conducting presentations or briefings on aspects of the project(s) to executive team. • Negotiating with project stakeholders or suppliers to obtain resources or materials. • Attending various entity and other task force meeting as entity representative.
Percentage of Duties	Marginal Functions
5%	The incumbent will perform other related duties as required to fulfill the mission, goals, and objectives.

%	Additional duties may include, but not be limited to: • Assisting where needed within the program, which may include special assignments • Complying with general State and CHHS administrative reporting requirements (i.e. completion of time sheets, project time reporting, travel requests, travel expense claims work plans, training requests, individual development plans, etc.); and • Attendance at staff meetings.

4. WORK ENVIRONMENT *(Choose all that apply from the drop-down menus)*

Standing:	Occasional (13-25%)	Sitting:	Frequent (51-75%)
Walking:	Occasional (13-25%)	Temperature:	Temperature Controlled Office Environment
Lighting:	Artificial Lighting	Pushing/Pulling:	Not Applicable
Lifting:	Not Applicable	Bending/Stooping:	Not Applicable

Other: *Click here to enter text.*

Type of Environment: a. Cubicle b. N/A

Interaction with Public: a. Required to assist customers on the phone and in person. b. Select c. Select.

5. SUPERVISION

Supervision Exercised *(e.g., Directly – 1 Information Technology Supervisor II; Indirectly – 5 Information Technology Associates)*

N/A

6. SIGNATURES

Employee's Statement:
I have reviewed and discussed the duties and responsibilities of this position with my supervisor and have received a copy of the Duty Statement and can perform the duties outlined above without a Reasonable Accommodation.

Employee's Name (Print)

Employee's Signature Date

Supervisor's Statement:
I have reviewed the duties and responsibilities of this position and have provided a copy of the Duty Statement to the Employee.

Supervisor's Name (Print)

Supervisor's Signature Date

7. HRD USE ONLY

Human Resources Division Approval

☒ Duties meet class specification and allocation guidelines. ☐ Exceptional allocation, 625 on file.	HR Analyst initials	Date approved
	NM	7/26/2021

Reasonable Accommodation Unit use ONLY *(completed after appointment, if needed)*

* If a Reasonable Accommodation is necessary, please complete a Request for Reasonable Accommodation form and submit to Human Resource Division (HRD), Reasonable Accommodation Coordinator.

List any Reasonable Accommodations Made:
Click here to enter text.

**** AFTER SIGNATURES ARE OBTAINED:**

- **SEND THE ORIGINAL DUTY STATEMENT TO HRD TO FILE IN THE EMPLOYEE'S OFFICIAL PERSONNEL FILE (OPF)**
- **PROVIDE A COPY TO THE EMPLOYEE**
- **FILE A COPY IN THE SUPERVISOR'S DROP FILE**