State of California
Department of Industrial Relations

DUTY STATEMENT

☒ **CURRENT**

☐ **PROPOSED**

CIVIL SERVICE CLASSIFICATION Information Technology Specialist I		**WORKING TITLE** IT/Cyber Security Specialist		
PROGRAM NAME Office of Information Services			**UNIT NAME** OIS	
ASSIGNED SPECIFIC LOCATION 1515 Clay Street, Suite 401, Oakland, CA 94612			**POSITION NUMBER** 400 – 176-1402-020	
BARGAINING UNIT 01	**WORK WEEK GROUP** E	**BILINGUAL POSITION** No	**CONFLICT OF INTEREST FILER** Yes	**BACKGROUND CHECK** No

General Statement

Under general direction of the Information Technology Manager I with the Department of Industrial Relations (DIR), Information Security Office (ISO), the Information Technology Specialist I (ITS I) is responsible for assessing and managing vulnerabilities on DIR IT assets and Pen Testing applications before and after applications are in production. Incumbent uses their skills and knowledge with Application Security by using an Appsec tool to analyze and report application vulnerabilities to DIR IT developers and the severity of these vulnerabilities. Incumbent is responsible for the management, coordination, and mitigation of all types of IT security risks found through IT audits and the security risk analysis process.

Candidates must be able to perform the following essential functions with or without reasonable accommodations.

Percentage of Time Spent	Duties Essential Job Functions
20%	Manage, assess, and assist with mitigation of vulnerabilities found on all DIR IT assets on the DIR network. Responsible for creating and distributing various kinds of vulnerability reports in various formats to assist the IT helpdesk, Network group and IT operations team to resolve and/or mitigate IT vulnerabilities. Research and extrapolate resolution of vulnerabilities through various sources including Rapid 7 support team. Use Rapid 7 Insight Virtual Machine (VM) tool to create sites, asset groups, reports and schedule scans or manually run scans on assets. Report false/positives and exclude vulnerabilities as stipulated by IT teams in the organization. Oversee several simultaneous mitigations or resolutions with various IT groups with or without coordination of Rapid 7 support team. Use Service Now to submit tickets and follow through with resolution with the proper IT personnel.
20%	Responsible for application security of all DIR applications hosted by DIR. Use the App Sec tool to create accounts, app profiles, security policies, and interpret scans results to assist DIR software developers and application administrators. Interpret results of scans and vulnerabilities found in scans and third-party software. Assist IT developers in training and vendor technical support for interpretation of results, mitigations and application design and alternatives.
15%	Responsible for the penetration test of web-facing applications. Create application and scan profiles, schedule or run manual scans using both the Standard and Enterprise version of pen test tool. Create various types of reports based on the need and interpret results for application developers and administrators. Work with

	vendor support when necessary to decipher and interpret vulnerabilities and reports. Responsible for entering IT risks on the Risk Register (POAM) and providing status updates to CDT on a quarterly basis. Interpreting risks and identifying the proper teams/personnel to fulfill a resolution/mitigation for the risk. Identify reports and resolutions and provide those to IT personnel for mitigation on behalf of the ISO. Responsible for follow up and follow through until the risk (testing, retesting, obtaining, reviewing, and filing artifacts) is fully resolved.
15%	Performs Security Risk Assessments (SRAs) for all DIR IT applications hosted internally or externally. SRAs are required to be submitted before a new system goes to production and thereafter updated periodically when modified. SRAs are reviewed for completeness and accuracy by this position according to SAM & SIMM requirements and NIST standards. Related to this review, corrective action plans are recommended by the ISO if a system does not meet the SRA requirements. Corrective action plans are monitored and reviewed until SAM, SIMM and NIST requirements are met.
15%	Manage Security Information and Event Management (SIEM) technologies. Responsible for the oversight when SIEM interprets event logs from hundreds of servers, firewalls, and web applications throughout the enterprise and generates reports on an as needed basis. SIEM support includes customization of the SIEM and log management appliances and generates alerts based upon the automated analysis of thousands of potential events per second. Effective use of this appliance is critical to the execution of DIR information security and compliance.
10%	Performs IT Contract Administration duties in support of researching, purchasing and renewing software purchases that are used by the ISO office. Provides Quality Assurance and Security Risk Management duties in accordance with the Department's policies and procedures as required to fulfill DIR-OIS mission critical, goals and objectives including possible technical support of other databases.

Percentage of Time Spent	Marginal Job Functions
5%	Perform other duties as assigned by the IT Manager I which may include other miscellaneous activities, including but not limited to, providing support for other IT management and staff within IT Operations unit, OIS Network and OIS Development teams to accomplish security tasks and responsibilities. Participates in other projects as needed. Research and stay abreast Information Technology (IT) policies to comply with California Statewide Information Management Manual (SIMM). Reviewing IT policies to provide advice and guidance to plan for IT policy project.

Conduct, Attendance, and Performance Expectations

ITS I must maintain a high level of integrity, professionalism, and confidentiality; uses sound professional judgment, exercise initiative, and objective action. Consistently behaves in an honest, fair, and ethical manner. Communicates clearly, simply, and effectively. Works cooperatively with all levels of OIS management and staff, other government agencies, and stakeholders to provide the highest level of service possible in person, by phone or email. Develops and maintains knowledge and skill related to specific tasks, methodologies, materials, tools and equipment; completes assignments in a timely and efficient manner; and adheres to department/division, directives, policies and procedures, , including attendance, leave, and conduct. Maintains regular and acceptable attendance at such level as is determined at the Department's sole discretion. Performs all work in accordance with DIR-ISO Compliance Policy and Procedure Directives and Memoranda. The ITS I must have the ability to maintain a collaborative working relationship with IT managers, supervisors and staff, business, vendors, other state entities to ensure DIR ISO system needs are fully met. Have a solid technical, networking and software basics understanding of the cloud, databases, and applications. Possess a wide range of technical skills that are shared in a leadership capacity to train and mentor ITA (Information Technology Associate) staff.

Supervision Received

The Information Technology Specialist I reports directly to and receives the majority of assignments from the Information Technology Manager I. However, direction and assignments may also come from the Chief Information Officer depending on the scope and complexity of the work performed.

Supervision Exercised

N/A

Work Environment, Special Requirements/Other Information, Physical Abilities, Additional Requirements/Expectations, and Personal Contacts

Work Environment

The incumbent will be assigned a space located on the 4th floor of the Elihu Harris State Building located in Oakland. The location has elevator access and is fully air conditioned with natural and artificial lighting. Hybrid telework options will be considered as job duties dictate. The majority of the time incumbent will be working in front of a computer. A laptop will be provided that can be brought home by the incumbent as necessary. Minimal travel may be required. Must be able to discuss mitigation techniques and where and how the vulnerabilities violate DIR application security policies. The ITS I create the annual Technical Recovery plan (TRP) and coordinates all input to it. The TRP is reviewed by this position annually before review and approval by Executive staff and DIR director. It is the duty and responsibility of this position along with the ISO to organize and coordinate a tabletop exercise every 2 years. May require some travel to Sacramento to attend training, attend meeting at California Dept. of Technology and Department of General Services as needed.

Special Requirements/Other Information

Ability to maintain a collaborative working relationship with IT managers, supervisors and staff, business, vendors, other state entities and with the California Department of Technology (CDT) to ensure DIR OIS system needs are fully met. Have a solid understanding of the cloud, databases, and the applications and programs used by those databases. Possess a wide range of technical skills. Also have a foundation in System Development Life Cycle and an understanding of data modeling, including conceptualization and database optimization.

Physical Abilities

Being in a stationary position for long periods of time. Move and transport office items in a safe manner.

Additional Requirements/Expectations

Work with the DIR Information Security Office (ISO) team to continuously develop, maintain and stay up to date on asset management security controls, appsec security, cyber & IT system security risks and disaster recovery. Incumbent shall be able to organize assignments, work under pressure, have attention to detail and possess effective oral and written communication skills. Ability to work professionally and ethically.

Personal Contacts

The incumbent will need to interact with the IT Supervisors, IT Managers, IT Business Analysts, subject matter experts in all DIR business and OIS units as well as legal and privacy offices. Must also work with external stakeholders and vendors.

Employee Acknowledgment

I have read and understand the duties listed above and certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and ability to work cooperatively with others; and a state of health consistent with the ability to perform these assigned duties as described above with or without reasonable accommodation. If you believe a reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for a reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Medical Management Unit in the Human Resources Office.

Employee Name

Employee Signature

Employee Sign Date

Supervisor Acknowledgment

I certify this duty statement represents a current and accurate description of the essential functions of this position. I have discussed the duties of this position with the employee and provided the employee with a copy of this duty statement.

Supervisor Name

Supervisor Signature

Supervisor Sign Date

HUMAN RESOURCES OFFICE APPROVAL

J.W.
C&S Analyst Initials

1/17/25
Approval Date