DUTY STATEMENT

EMPLOYEE NAME:	Vacant	CURRENT DATE:	03/03/2020
CLASSIFICATION:	Information Technology Specialist I	POSITION #:	673-860-1402-039
DIVISION/OFFICE:	Office of Information Services	CBID:	R01
SECTION:	Security Operation Center		
SUPERVISOR'S NAME:	Westley Warren		
SUPERVISOR'S CLASS:	Information Technology Supervisor II		

I certify that this duty statement represents an accurate description of the essential functions of this position.

I have read this duty statement and agree that it represents the duties I am assigned.

Supervisor's Signature ***Date*** ***Employee's Signature*** ***Date***

SPECIAL REQUIREMENTS OF POSITION (IF ANY):

- ☒ Designated under Conflict of Interest Code.
- ☐ Duties performed may require annual physical.
- ☐ Duties performed may require drug testing.
- ☐ Duties require participation in the DMV Pull Notice Program.
- ☐ Requires the utilization of a 32-pound self-contained breathing apparatus.
- ☐ Operates heavy motorized vehicles.
- ☐ Requires repetitive movement of heavy objects.
- ☐ Works at elevated heights or near fast moving machinery or traffic.
- ☒ Performs other duties requiring high physical demand. (Explain below)

  May require lifting and/or moving equipment up to 50 lbs

SUPERVISION EXERCISED (check one):

- ☒ None
- ☐ Supervisor
- ☐ Lead Person
- ☐ Team Leader

FOR SUPERVISORY POSITIONS ONLY: Indicate the number of positions by classification that this position DIRECTLY supervises:

0

Total number of positions in Section/Branch/Office for which this position is responsible:

0

FOR LEADPERSONS OR TEAM LEADERS ONLY: Indicate the number of positions by classification that this position LEADS:

MISSION OF SECTION:

The mission of the California Air Resources Board's (CARB) information technology (IT) program is to leverage the most effective IT available to achieve its program goals. This mission includes ensuring that such technologies are professionally managed, properly maintained and secured, and efficiently utilized.

The Security Operation Center (SOC) has the responsibility for managing and reporting security incidents; developing and maintaining information security and privacy plans, policies, processes, procedures and standards; developing CARB's technology recovery plan (TRP); risk management; security training and awareness; information security operations; and providing information security consulting services for implementing new IT products, projects, and systems.

CONCEPT OF POSITION:

Under general supervision, the Information Technology Specialist I (IT Spec I) acts as a team leader on the more complex systems software projects, and/or works independently as a high-level technical specialist on the more complex systems assignments. This is the expert specialist level. This class is used to analyze, design, code, implement, maintain, and evaluate computer software; this includes, but is not limited to, operating systems, control systems, proprietary software packages, telecommunications software, and database management software. This class is also used as a high-level technical advisor to act as consultants to other information technology personnel in solving system problems and achieving the best use of available hardware and software resources; to act as lead person over other personnel; to coordinate and ensure effective operations of complex multiple hardware and software configurations; and to do other related work.

The IT Spec I. conducts business activities in a professional manner that leads to superior customer satisfaction and delivers services that meet or exceed the customer's expectations. The IT Spec I is responsible for individual decisions and actions while working on systems using best practices and innovative technologies. When handling confidential personnel and/or business data, the IT Spec I must maintain confidentiality.

INFORMATION TECHNOLOGY DOMAINS:

☐ Business Technology Management

☒ Information Security Engineering

☐ IT Project Management

☒ Software Engineering

☐ Client Services

☐ System Engineering

% Of Time	RESPONSIBILITIES OF POSITION
30% E	Serves as the Technical lead, works closely with the Information Security Officer (ISO) and Chief Information Officer (CIO), to provide information security administration and support for CARB end users, applications, databases, systems, and networks on a daily basis. Advises OIS staff on a variety of complex systems assignments. Independently conducts security reviews to monitor and audit all major information systems and data processing activities. Regularly reviews complex system and network log files. Reviews sources of new threats and vulnerabilities, such as federal, state, and vendor web sites. Immediately responds to security incidents and audit findings to determine root cause or implement defensive or preventing strategies. Provides required notifications and reports to stakeholders and control agencies. Plans and guides the technical teams to run vulnerability/security scans within the enterprise. Analyzes, translates and reports scan findings to OIS management, and to Executives as directed. Develops a remediation plan and follows the remediation progress; presents reports to OIS management. Independently monitors, reports, and educates OIS staff on security findings and remediation options. Independently researches and presents new security threats and mitigation strategies to OIS management. Manages, implements, and coordinates security orientation and annual security awareness training programs for all CARB staff. Maintains cybersecurity threat intelligence and develops defensive strategies to combat the latest known threats. Develops plans and oversees projects to implement defensive measures and to remediate security vulnerabilities in legacy systems. Collaborates with development and project teams to ensure best practices are implemented in new and evolving information systems. Creates, tracks, and submits any required documentation to control agencies such as the State's Information Security Office or the CA Department of Technology (CDT).
30% E	Provides technical expertise on complex IT security-related issues and maintains technical expertise on emerging IT trends and strategic IT direction and their implications for information security. Independently researches, identifies, and verifies new security threats and vulnerabilities, and corresponding leading edge, innovative best practices and technologies for defensive and preventive measures. Responds to written and verbal inquiries from CARB executives, managers, and internal or external parties on management issues pertaining to security, privacy, disclosure or resolution. Works closely with the ISO and CIO to create, track, and submit required regulatory documents to the State's Information Security Office, CDT, and any other control agencies. Independently creates and maintains documentation for any system administration activities performed or changes implemented, such as change logs, installation procedures, security risk mitigation plans, commented script code documents, deployment plans, status reports, etc. Develops and diagrams standard operating practices and procedures to provide consistent and competent customer service to end users. Automates security process and incident handling by developing the appropriate level of scripting automation. Troubleshoots complex network security issues in partnership with the networking team.
15% E	Independently acts as a technical lead on complex software projects and assignments, including: research, review, recommend, and implement hardware and software requests for approval by OIS Management and ISO; ensures CIO approves all Administrative Privileges requested by CARB end users. Ensures hardware and software is compatible with, and interfaces well with ARB's existing and/or proposed enterprise infrastructure, and does not create security risks to CARB's technical

	environment and sensitive, confidential, or mission-critical data. Responsible for managing, tracking, and reporting licensure compliance with software licenses to ensure CARB sustains any internal and/or external audits. Supports custom software development projects and maintenance teams by reviewing and providing input to new project concepts, change requests, feasibility studies, etc. Assists OIS IT Procurements by recommending and/or providing alternative solutions for commercial software, system software, and infrastructure hardware and software upgrades or replacements that promotes a secured IT environment and supports development of related documentation. Supports development and implementation of technology recovery plans, procedures, tests, and execution in compliance with State Information Management Manual and CARB business needs. Coordinates prioritization and recovery objectives with CARB programs and technical teams. Technical leads technology recovery planning and testing. The SSS II must also maintain confidentiality while handling and processing any confidential personnel/business data. May be required to travel.
15% E	Serves as a technical lead for IT special projects involving complex systems software and commercial software application integration. Meets with OIS managers, developers, and with program management and staff to gather, explore, and evaluate IT problems, system needs and technical requirements. Consults with technical experts from other state entities, product vendors, and service providers to research alternatives and determine advantages and disadvantages, costs and benefits. Proposes solutions for the most highly complex IT systems needs and advises technical and business managers on the advantages and disadvantages of alternatives. Leads a team of OIS staff and program staff to develop data classifications for all data held at the Board. Independently creates, assigns, documents, and implements priority statuses to all data, including data that is considered highly confidential and mission critical to CARB.
5% E	Serves as a SME to a variety of complex enterprise-wide systems such as but not limited to, enterprise applications, O365, Windows and Linux operating systems and various security related tools. Designs, develops, configures, and tests system configuration changes needed to provide required system functionality, tailored for CARB use. Independently researches and recommends commercial software products and system components to be procured, developed, tested, implemented, and deployed to CARB end users enterprise-wide, or tailored to specific user groups. Serves as a backup to developing, implementing, enhancing, and providing daily administration, maintenance and operations as needed.
5% M	Attends IT training, and provides knowledge transfer to other OIS staff informally or formally via "Train the Trainer", "on-the-job training", one-on-one mentoring, brown-bag sessions, etc. Documents system configuration and technology details in the IT knowledge base. May require lifting and/or moving equipment up to 50 pounds.