State of California – California Natural Resources Agency
California Natural Resources Agency
Human Resources

Duty Statement

UNIT	CLASSIFICATION	POSITION NUMBER (Agency-Unit-Class-Serial)
Information Technology	Information Technology Specialist II	534-001-1414-001
DEPARTMENT	**WORKING TITLE**	**CBID**
California Natural Resources Agency	Information Security Engineer	R01
HEADQUARTERS	**REPORTING LOCATION**	**EMPLOYEE**
Sacramento, CA	715 P street, Sacramento, CA 95814	TBD
SUPERVISOR CLASSIFICATION		**EFFECTIVE DATE**
Information Technology Manager I		TBD

POSITION DESCRIPTION

Under general direction of the California Natural Resources Agency's (CNRA) Security Operations Center Manager, the position serves as an Information Security Engineer. The position is a senior member of the CNRA Security Operations Center (SOC) working independently as a recognized technical security expert. The incumbent is responsible for performing the most complex information security activities and tasks as needed as part of the security detection, analysis, remediation, security controls operations, and incident response team to provide critical protection of the California Natural Resources Agency organizations information technology assets. The position will utilize and assist in the development of state-of-the-art technologies and processes through which those defined information security controls and protections are achieved.

The incumbent develops and maintains a mastery working level knowledge of relevant information technology assets under the protection of the CNRA SOC, of applicable State/Federal and industry regulations and best practices with respect to information security, of department and information security policies and procedures, and of information technology security technologies and practices. The position will develop and maintain knowledge of the information technology threat landscape, security risk management methodologies, defined security controls, network architecture and protocols, and operating systems, as well as interoperability and interdependency of these components/elements.

ESSENTIAL FUNCTIONS:

The position requires the incumbent to balance concurrent assignments and complete assigned projects and tasks on time at a level commensurate with the classification. Satisfactory job performance is required to maintain a teleworking agreement. In all job functions, employees are responsible for creating an inclusive, safe, and secure work environment that values diverse cultures, perspectives, and experiences, and is free from discrimination. Employees are expected to provide all members of the public with equitable services and treatment, collaborate with underserved communities and tribal governments, and work toward improving outcomes for all Californians.

%	TASK/DUTIES
40%	Investigates and responds to security threats. Responsible for providing specialized cybersecurity technical expertise to CNRA information technology and executive stakeholders. Performs advanced technology security problem solving and counter-measure activities for on-premises, cloud, and user endpoint technologies. Perform cyber forensics activities in response to a cybersecurity incident. Monitor and manage critical SOC technologies including but not limited to intrusion detection and protection devices, host-based protection technologies, 0-day and APT technologies (sandboxing, behavioral monitoring, etc.), packet capture and metadata analytic systems, data loss protection, email hygiene systems, etc. Apply knowledge of indicators of compromise and threats to detect attacks or compromised assets including, but not limited to, threat tactics/techniques/procedures, in-depth knowledge of security network architecture, knowledge of IT platform operations (e.g. Windows, Linux, network devices), vulnerability exploits and management, methods of access and related controls, encryption technologies, etc. Coordination with technical staff across CNRA organizations to assess any indicators of

Duty Statement

	compromise. Coordination with the CNRA Information Security Office to provide security solutions that adhere to industry standards and best practices.
35%	Responsible for the implementations, operations, and maintenance of security control tools. Perform audits of security controls and software to ensure proper functionality. Maintain the highest level of expertise in security operations technologies, techniques, and processes as well as threat actor techniques and operations. Participate in systems evaluations, audits, and reviews that affect the SOC, security monitoring, and threat intelligence. Define and maintain enterprise-wide information security methodologies, frameworks, reference models, and documentation standards. Participate in the development and maintenance of SOC policies, procedures, and other artifacts as needed to operate a successful security operations function. Create comprehensive documentation of all work performed which includes the writing of reports and applicable technical documentation of systems, as well as quality assurance review of incident reports and documentation prepared by other SOC cybersecurity personnel.
15%	Serve as a senior resource to CNRA organizations in the investigation, tracking, resolution, and reporting of defined information security events. Develop and execute playbook scripts (for tiers 1 and 2) that detail the steps to be taken for indicated security events. Participate in Information Security Incident Response Teams. Participate in post-incident reviews and develop action plans to reduce exposure to similar incidents. Provide direction, oversight, and assist CNRA organizations for defined security remediation activities. Represent security monitoring and threat intelligence as required in both internal and external meetings and engagements. Provide oversight for the planning and implementation of information security projects, monitor compliance with established plans, schedules, directives. Coordinate with Agency stakeholders to conduct incident response exercises.
5%	**Support Diversity, Equity, and Inclusion** Participate in professional development training, as well as tasks, trainings and activities that support programmatic and workplace diversity, equity, and inclusion. Embed equity and environmental justice considerations into policies and administrative practices.
MARGINAL FUNCTIONS:	
%	**TASK/DUTIES**
5%	Other job-related duties as assigned and necessary for operational continuity. Attend staff meetings and training and prepare administrative paperwork to meet operational needs.
TYPICAL WORKING CONDITIONS	
Office Environment	
POSITION CATEGORY:	
This position is categorized as **Office-Centered**.	
SPECIAL REQUIREMENTS:	
The statements contained in this job description 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. The incumbent of this position may perform other duties (commensurate with the classification) as assigned, including work in other functional areas to cover during absences, to equalize peak work periods, or to otherwise balance the workload.	
SUPERVISOR STATEMENT:	

Duty Statement

I CERTIFY THIS DUTY STATEMENT REPRESENTS AN ACCURATE DESCRIPTION OF THE ESSENTIAL FUCNTIONS 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 (PRINT)	**SUPERVISOR SIGNATURE**	**DATE**
EMPLOYEE STATEMENT: I CERTIFY I HAVE READ, UNDERSTAND, AND CAN PERFORM THE DUTIES OF THIS POSITION EITHER WITH OR WITHOUT REASONABLE ACCOMMODATION. I HAVE DISCUSSED THESE DUTIES WITH MY SUPERVISOR AND HAVE BEEN PROVIDED A COPY OF THIS DUTY STATEMENT.		
EMPLOYEE NAME (PRINT OR TYPE)	**EMPLOYEE SIGNATURE**	**DATE**

State of California – California Natural Resources Agency
California Natural Resources Agency
Human Resources

Duty Statement

UNIT	CLASSIFICATION	POSITION NUMBER (Agency-Unit-Class-Serial)
Information Technology	Information Technology Specialist I	534-001-1402-XXX
DEPARTMENT	**WORKING TITLE**	**CBID**
California Natural Resources Agency	Information Security Specialist	R01
HEADQUARTERS	**REPORTING LOCATION**	**EMPLOYEE**
Sacramento, CA	715 P street, Sacramento, CA 95814	TBD
SUPERVISOR CLASSIFICATION		**EFFECTIVE DATE**
Information Technology Manager I		TBD

POSITION DESCRIPTION

Under the direction of the California Natural Resources Agency's (CNRA) Security Operations Center (SOC) Information Technology Manager I, the Information Technology Specialist I (ITS I) serves as an Information Security Specialist. The ITS I is a member of the CNRA SOC working independently and/or in conjunction with other CNRA SOC staff. The ITS I is responsible for performing complex information security activities and tasks as needed as part of the security detection, analysis, remediation, security controls operations, and incident response team to provide critical protection of CNRA's information technology assets. The incumbent will utilize and assist in the development of state-of-the-art technologies and processes through which those defined information security controls and protections are achieved.

The ITS I develops and maintains an advanced working level knowledge of relevant information technology assets under the protection of the CNRA SOC, of applicable State/Federal and industry regulations and best practices with respect to information security, of department and information security policies and procedures, and of information technology security technologies and practices. The incumbent will develop and maintain knowledge of the information technology threat landscape, security risk management methodologies, defined security controls, network architecture and protocols, and operating systems, as well as interoperability and interdependency of these components/elements.

The ITS I works primarily in Information Security Engineering, Software Engineering, and System Engineering domains.

ESSENTIAL FUNCTIONS:

The position requires the incumbent to balance concurrent assignments and complete assigned projects and tasks on time at a level commensurate with the classification. Satisfactory job performance is required to maintain a teleworking agreement. In all job functions, employees are responsible for creating an inclusive, safe, and secure work environment that values diverse cultures, perspectives, and experiences, and is free from discrimination. Employees are expected to provide all members of the public with equitable services and treatment, collaborate with underserved communities and tribal governments, and work toward improving outcomes for all Californians.

%	TASK/DUTIES
40%	Investigates and responds to security threats utilizing various security platforms and technologies. Responsible for providing specialized cybersecurity technical expertise to CNRA information technology and executive stakeholders. Performs advanced technology security problem solving and counter-measure activities for on-premises, cloud, and user endpoint technologies. Monitor and manage critical SOC technologies including but not limited to: intrusion detection and protection devices, host-based protection technologies, 0-day and APT technologies (sandboxing, behavioral monitoring, etc.), packet capture and metadata analytic systems, data loss protection, email hygiene systems, etc. Apply knowledge of indicators of compromise and threats to detect attacks or compromised assets including, but not limited to, threat tactics/techniques/procedures, in-depth knowledge of security network architecture, knowledge of IT platform operations (e.g. Windows, Linux, network devices), vulnerability exploits and management, methods of access and related controls, encryption technologies, etc. Assist

Duty Statement

	senior SOC staff with technical project coordination across CNRA organizations to assess any indicators of compromise. Assist senior SOC staff with technical project coordination with the CNRA Information Security Office to provide security solutions that adhere to industry standards and best practices.
30%	Assists with implementations, operations, and maintenance of security control tools. Perform audits of security controls and software to ensure proper functionality. Maintain an advanced level of expertise in security operations technologies, techniques, and processes as well as threat actor techniques and operations. Participate in systems evaluations, audits, and reviews that affect the SOC, security monitoring, and threat intelligence. Define and maintain enterprise-wide information security methodologies, frameworks, reference models, and documentation standards. Participate in the development and maintenance of SOC policies, procedures, and other artifacts as needed to operate a successful security operations function. Create comprehensive documentation of all work performed which includes the writing of reports and applicable technical documentation of systems, as well as quality assurance review of incident reports and documentation prepared by other SOC cybersecurity personnel.
20%	Serve as a technical resource to CNRA organizations in the investigation, tracking, resolution, and reporting of defined information security events (incident response). Develop and execute playbook scripts (for tiers 1 and 2) that detail the steps to be taken for indicated security events. Participate in Information Security Incident Response Teams. Participate in post-incident reviews and develop action plans to reduce exposure to similar incidents. Provide direction, oversight, and assist CNRA organizations for defined security remediation activities. Represent security monitoring and threat intelligence as required in both internal and external meetings and engagements. Provide oversight for the planning and implementation of information security projects, monitor compliance with established plans, schedules, directives. Coordinate with Agency stakeholders to conduct incident response exercises.
5%	**Support Diversity, Equity, and Inclusion** Participate in professional development training, as well as tasks, trainings and activities that support programmatic and workplace diversity, equity, and inclusion. Embed equity and environmental justice considerations into policies and administrative practices.
MARGINAL FUNCTIONS:	
%	**TASK/DUTIES**
5%	Other job-related duties as assigned and necessary for operational continuity. Attend staff meetings and training and prepare administrative paperwork to meet operational needs.
TYPICAL WORKING CONDITIONS	
Office Environment	
POSITION CATEGORY:	
This position is categorized as **Office-Centered**.	
SPECIAL REQUIREMENTS:	
The statements contained in this job description 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. The incumbent of this position may perform other duties (commensurate with the classification) as assigned, including work in other functional areas to cover during absences, to equalize peak work periods, or to otherwise balance the workload.	
SUPERVISOR STATEMENT:	

Duty Statement

I CERTIFY THIS DUTY STATEMENT REPRESENTS AN ACCURATE DESCRIPTION OF THE ESSENTIAL FUCNTIONS 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 (PRINT)	**SUPERVISOR SIGNATURE**	**DATE**
EMPLOYEE STATEMENT: I CERTIFY I HAVE READ, UNDERSTAND, AND CAN PERFORM THE DUTIES OF THIS POSITION EITHER WITH OR WITHOUT REASONABLE ACCOMMODATION. I HAVE DISCUSSED THESE DUTIES WITH MY SUPERVISOR AND HAVE BEEN PROVIDED A COPY OF THIS DUTY STATEMENT.		
EMPLOYEE NAME (PRINT OR TYPE)	**EMPLOYEE SIGNATURE**	**DATE**