CALIFORNIA NATURAL RESOURCE AGENCY

JOB DUTY STATEMENT

CLASSIFICATION	POSITION #	ORGANIZATION
Information Technology Specialist II	534-001-1414-003	CNRA- Information Security Operations
APPOINTEE		

COLLECTIVE BARGAINING IDENTIFIER

☐ Management Related ☐ Supervisory Related ☐ Confidential Related ☒ Rank and File BU: 01

SUPERVISOR NAME and CLASSIFICATION
Richard Harmonson - Information Technology Manager II

APPROVED BY	DATE
Tim Garza	7/1/2018

Percent of Time	*Activity*
	POSITON SUMMARY Under the administrative direction of the California Natural Resources Agency's (CNRA) Security Operations Officer, the position serves as an Enterprise 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.

Employee Signature Date

Supervisor/Manager Signature Date

	Essential Functions
45%	The SOC Security Engineer uses technical knowledge related to various security technologies to analyze and respond to security threats from various security platforms and technologies. Responsible for providing specialized technical expertise in the area of cybersecurity. Performs advanced technology security problem solving and counter-measure activities. 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 compromise.
35%	Security Engineer is responsible for the implementation, operations, and maintaining of defined security control tools. Perform audits of defined 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 are conducted affecting the SOC and Security Monitoring and Intelligence. Participate in the development and maintenance of SOC policies, procedures, and other artifacts as needed to operate a successful security operations function. Define and maintain an enterprise-wide information security methodology, framework, reference model, and documentation standards.
20%	Serve as a lead 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 specific, indicated security events. Participate/Lead Information Security Incident Response Teams. Participate in post-incident reviews and develop action plans to reduce exposure to similar incidents. Provide direction, oversight, and assists to CNRA organizations for defined security remediation activities. Represent Security Monitoring and 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.
	Special Requirements
	Incumbent must maintain confidentiality regarding all information security items and the participating in any forensics and/or security activities, or any other situations related to IT security issues where discretion is required. Occasional after-hours work scheduled and travel to various offices and locations throughout the State of California may be required. Under the provisions of the North American Electric Reliability Corporation Critical Infrastructure Protection Standard CIP-004 as part of the Energy Policy of 2005, this position has authorized cyber access to or unescorted physical access around critical cyber assets and is subject to a satisfactory background check prior to appointment and every seven years thereafter.

Knowledge, Skills, and Abilities

It is desired that incumbent possess one of the following Security Certification(s):
* CompTIA Advanced Security Practitioner
* GIAC Information Security Professional
* GIAC Certified Incident Handler
* ISACA Certified Information Systems Auditor
* (ISC)^2 Certified Information Systems Security Professional
* (ISC)^2 Certified Cloud Security Professional

Possess experience and knowledge in the practices, principles, and techniques of information security. Knowledge and understanding of NIST 800-53. Ability to analyze and formulate security policies and procedures.

Incumbent must have extensive knowledge and abilities in the following disciplines:
* Practices, principles, and techniques of information security
* Security architecture
* Security vulnerabilities
* Cyber hacking
* Operational security
* Access controls
* Messaging and network protocols
* Cryptography
* Security assessments
* Penetration testing
* Documentation skills
* Experience with Linux, Windows and Network Operating Systems and Protocols
* Strong working knowledge of Routing and Access Control Devices
* Strong critical thinking and problem-solving skills