

SHADED AREA TO REFLECT RECLASS POSITION NUMBER ONLY**DUTY STATEMENT**

EFFECTIVE DATE: December 2014

CDCR INSTITUTION OR DEPARTMENT Enterprise Information Systems (EIS)		POSITION NUMBER (Agency – Unit – Class – Serial) 065-620-1337-035
UNIT NAME AND CITY LOCATED Executive/AISO, Rancho Cordova		CLASS TITLE Senior Information Systems Analyst (Specialist)
WORKING DAYS AND WORKING HOURS 8:00 a.m. to 5:00 p.m. (Approximate only for FLSA exempt classifications)		SPECIFIC LOCATION ASSIGNED TO Information Security Office
PROPOSED INCUMBENT (If known)		CURRENT POSITION NUMBER (Agency – Unit – Class – Serial)
YOU ARE A VALUED MEMBER OF THE DEPARTMENT'S TEAM. YOU ARE EXPECTED TO WORK COOPERATIVELY WITH TEAM MEMBERS AND OTHERS TO ENABLE THE DEPARTMENT TO PROVIDE THE HIGHEST LEVEL OF SERVICE POSSIBLE. YOUR CREATIVITY AND INGENUITY ARE ENCOURAGED. YOUR EFFORTS TO TREAT OTHERS FAIRLY, HONESTLY AND WITH RESPECT ARE CRITICAL TO THE SUCCESS OF THE DEPARTMENT'S MISSION.		
Under the general direction of the Agency Information Security Officer, the Senior Information Systems Analyst (Specialist) works as a lead for information security risk management and network security tasks for the Information Security Office. The CDCR must comply with federal and state security regulations including NIST Security requirements, HIPAA Security Rule, and SAM Information Security Sections. The Senior Information Systems Analyst (Specialist) will be committed to adopting the best practices of information security industry as promulgated by the private, state, and federal entities in order to secure confidential and sensitive information, to counteract hacker attacks, and to protect against virus infection throughout the organization. The mission is to ensure a secure computing environment that will provide availability, confidentiality, and integrity of information. The Senior Information Systems Analyst (Specialist) works within the ISO Office, which is comprised of security analysts and technologists performing a wide array of complex security related tasks. The Senior Information Systems Analyst (Specialist) position will provide advanced technical advice and train staff in performing the complex technical security functions for the protection of CDCR's and other technical and operational areas. This position will provide technical security expertise and collaborate with other units in security related areas within EIS.		
% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. (Use addition sheet if necessary)	
ESSENTIAL FUNCTIONS		
25%	Oversee policy administration for the information security appliance suite used to manage the CDCR network assets. This includes network and host intrusion prevention systems, anti-malware suite, host data loss prevention and device control appliance, encrypted USB device central management appliance, and the security event manager. The Senior Information Systems Analyst (Specialist) is responsible for the managing, tuning, calibrating, and deployment of the security appliances and associated software. In addition, the incumbent is responsible for engineering security policies that mitigate and minimize the risk to CDCR information assets while ensuring that business process functionality is not hindered.	
25%	Perform complex technical vulnerability and risk assessments of the CDCR network managed assets including the network hardware components, network schematics for enterprise applications, network endpoints (workstations and servers), distributed locations remote access, and data center operations and facilities by using vulnerability tools. Develop and implement a network risk assessment methodology that includes the selection and application of vulnerability and countermeasure tools, identification of threats to the network, assessment of risks associated with threats, and recommendations for corrective actions by applying security industry standards such as NIST, SANS, and COBIT. The position will assess threats associated with all areas of technologies that communicate over the CDCR network resources. This would include such technologies as wireless (WiFi), laptops and mobile workstations, smart phones, email communications, VPN/Remote access, storage capacity, backup processes, internal and external system interfaces, third party applications, web proxy, and external contractor activities.	
20%	Analyze network security events through event correlation. This would include studying network incident reports, reviewing network change requests, communicating with the various units, and monitoring the security appliances for potential anomalies. Utilize network software and hardware security tools to identify potential threats and, if needed, modify appliance settings to enhance network security. Participate as an active member of the Computer Security Incident Response Team (CSIRT) by providing technical analysis and identifying potential remediation procedures.	

DUTY STATEMENT

EFFECTIVE DATE: December 2014

10%	Perform complex risk assessments on IT projects that are being proposed that will involve the CDCR network. Also identify the impact of the project on the overall CDCR infrastructure by interpreting business requirement and detailed design documents. Apply the advanced knowledge of network security to identify risks relevant to the project and CDCR enterprise network. Ensure IT projects comply with the applicable state and federal regulatory information security requirements.
5%	Develop the CDCR Enterprise Information Security Architecture by understanding the applications, technology, and infrastructure in the department, and by including the organizational structure(s); all applicable legal, regulatory, and statutory information security requirements; business risk tolerance level; business goals and objectives; operational goals and objectives; technical security catalogue or portfolio, system and interface diagrams; data flows; and network topologies. Ensure that the Information Security Architecture is aligned with the business strategy and the IT infrastructure by understanding the current and future technology and the business functions and programs in the department.
5%	Participate in the development of information security policies and procedures for the ISO by applying security industry best practices, state and federal mandates, health and medical related security standards, and other authoritative sources. Write/review information security policies and procedures in order to ensure compliance with the appropriate state and federal security regulations. Knowledge of security industry references such as NIST, SANS, ISO.
5%	Participate in the contingency planning for the CDCR by assisting the ISO in developing the Emergency Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. Ensure that the contingency planning documents will adhere to the state guidelines and regulations by being knowledgeable of these regulations.
5%	Perform network related tasks as required. Other duties as assigned.

KNOWLEDGE AND ABILITIES

Knowledge of: Principles of public administration, organization, and management; information technology systems equipment, software, and practices; analytical techniques; technical report writing and principles of personnel management, supervision, and training; the department's Equal Employment Opportunity objectives; a manager's role in the Equal Employment Opportunity and the processes available to meet equal employment objectives.

Ability to: Analyze information and situations, identify and solve problems, reason logically, and draw valid conclusions; develop effective solutions; apply creative thinking in the design of methods of processing information with information technology systems; monitor and resolve problems with information technology systems hardware, software, and processes; establish and maintain effective working relationships with others; communicate effectively and supervise technical personnel; effectively contribute to the department's equal employment objectives.

DESIRABLE QUALIFICATIONS

Special Personal Characteristics: Effective communication skills, both written and verbal.

Interpersonal Skills: Ability to influence and motivate individuals and teams working toward mutual goals which have basic cooperative attitudes.

- Additional Desirable Qualifications:* Experience, including but not limited to: Identifying network based vulnerabilities, designing network based threat countermeasures, participating in network related incident management activities, and managing network related risk; Experience working on large and complex network security or network related IT projects; Experience working with Cisco related network security solutions; Experience working on network security compliance activities in a regulated industry; Experience performing network security related activities in the healthcare industry; Experience providing network security or network related IT related consulting services to clients in the public and/or private sector(s); Knowledge of state IT policy and governance processes; Knowledge of state IT policy and governance processes; Experience performing network risk assessments; Experience performing network

DUTY STATEMENT

EFFECTIVE DATE:	December 2014
-----------------	---------------

vulnerability assessments; Experience designing, implementing, and managing network based technical controls including but not limited to Cisco Adaptive Security Appliance (ASA) firewalls, Cisco Firewall Software Module (FWSM), Cisco network based Intrusion Prevention Systems (IPS), and Cisco based secure remote access solutions; Experience working in an environment where network security services are provided by an external service provider; Experience participating in enterprise network design and implementation efforts with a focus on integrating security into the enterprise design; Certified in Cisco Security (CCSP, CCNP Security, or CCIE Security); Certified in information security (CISSP, CISM, or CISA); SANS Certified; Understanding of State governance process; Experience with projects supporting correctional environments and processes. Knowledge of the OSI model; Knowledge of State Information Security policies and structure. Ability to interpret various software code written in language including, but not limited to binary, machine, assembly, various programming languages and object based programming. Experience or knowledge of information security incident response process including, but not limited to forensic analysis and preservation of evidence.

SPECIAL PHYSICAL CHARACTERISTICS

Incumbent occasionally moves equipment either solely (40 lbs. max.) or with another person (100 lbs. max.), may be required to open equipment and replace parts as directed, and is expected to exert up to 40lbs of force occasionally and/or a negligible amount of force frequently or constantly to lift, carry, push, pull, or otherwise move objects. Involves frequent walking, standing and sitting. Persons appointed to this position must be able to travel to assigned locations.

SUPERVISOR'S STATEMENT: *I HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE*

SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE
---------------------------	------------------------	------

EMPLOYEE'S STATEMENT: *I HAVE DISCUSSED WITH MY SUPERVISOR THE DUTIES OF THE POSITION AND HAVE RECEIVED A COPY OF THE DUTY STATEMENT*

The statements contained in this duty statement 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. Individuals may perform other duties as assigned, including work in other functional areas to cover absence of relief, to equalize peak work periods or otherwise balance the workload.

EMPLOYEE'S NAME (Print)	EMPLOYEE'S SIGNATURE	DATE
-------------------------	----------------------	------