CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION

POSITION DUTY STATEMENT – INFORMATION TECHNOLOGY

☐ PROPOSED

☒ CURRENT

CDCR INSTITUTION OR HEADQUARTERS PROGRAM	POSITION NUMBER (Agency-Unit-Class-Serial)			
Enterprise Information Services	065-621-1414-003			
DIVISION / UNIT	CLASSIFICATION TITLE			
	Information Technology Specialist II			
	WORKING TITLE			
	Security Architect - Endpoints			
Office of the Information Security Officer	TIME BASE / TENURE	CBID	WWG	COI
	Full-Time/ Permanent	R01	E	Yes ☒ No ☐
LOCATION	INCUMBENT		EFFECTIVE DATE	
Birkmont Drive, Rancho Cordova			07/13/2026	

CDCR'S MISSION and VISION

Mission

To facilitate the successful reintegration of the individuals in our care back to their communities equipped with the tools to be drug-free, healthy, and employable members of society by providing education, treatment, rehabilitative, and restorative justice programs, all in a safe and humane environment.

Vision

We enhance public safety and promote successful community reintegration through education, treatment, and active participation in rehabilitative and restorative justice programs.

Commitment

CDCR and CCHCS are committed to transforming the correctional landscape to create safer, more professional, and more fulfilling environments for our employees, the incarcerated population, and those supervised in our communities. Through systemwide improvements grounded in proven and emerging practices, we aim to strengthen rehabilitation, enhance workplace satisfaction, and support successful reentry into the community through our institutions, parole, and community partnerships. Our shared mission is to promote safety, wellness, and human dignity while fostering positive change for all those who live and work within our institutions and communities.

CDCR and CCHCS are committed to building an inclusive respectful workplace. We are determined to attract and hire candidates from all communities and empower employees from a variety of backgrounds, perspectives, and personal experiences. We are proud to foster inclusion and drive collaborative efforts at all levels of the Department.

DIVISION OVERVIEW

Enterprise Information Services (EIS) is the catalyst that drives transformation. We enhance safety, enable rehabilitation, and drive operation efficiency. EIS provides a full range of information technology (IT) services for the Department that includes Information Security, IT Procurement, Infrastructure, software development, implementation and support.

GENERAL STATEMENT

Under general direction of the Information Technology Manager I (ITM I). The Information Technology Specialist II (ITS II) works as a technical senior security specialist to enhance and drive the Department's security program. The CDCR Office of the Information Security Officer (OISO) must ensure compliance with federal and state security regulations such as NIST requirements, HIPPA Security Rule, and SAM Information Security Sections. The ITS II sets and implements best practices of information security for one of the largest correctional and public safety organizations in the nation. The incumbent will coordinate with Department, private, State and Federal entities to secure and protect confidential and sensitive information. This position will counteract information security threats, perform ongoing red-team engagements, proactive threat hunting, incident response, cyber threat intelligence collection and analysis, and defense countermeasure implementation. The ITS II works in the OISO which is comprised of security analysts, engineers, and technologists performing a wide array of complex security related tasks. The ITS II will be concerned with department security at the endpoint level, working with the CDCR Endpoint Management and Monitoring (EMM) team. Additionally, as one of the OISO's security architects, the ITS II position will work closely with the Enterprise Architects to provide advanced technical leadership to the EIS, while empowering peers to perform the most complex technical security functions for the protection of technical and operational areas in a law enforcement environment.

INFORMATION TECHNOLOGY DOMAINS – PLACE AN "X" ON ALL APPLICABLE DOMAINS

	Business Technology Management		Client Services	X	Information Security Engineering
X	Information Technology Project Management	X	Software Engineering	X	System Engineering

% 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.
30%	**Security Architecture and Design** Acts as an expert technical security architect providing technical guidance for IT initiatives taking into consideration information security, law enforcement, and technology policies, standards, best practices, and regulatory requirements. Provide expert level input and feedback on cyber security strategies, designs, and implementation/integration efforts for EIS initiatives. This will include, but not be limited to, on premise solutions, cloud solutions, managed solutions, and hybrid designs. Provide expert level input and feedback on secure application development strategies, designs, and implementation/integration efforts for EIS initiatives. This will include, but not be limited to, software development standards, application architecture, application scanning, identification, and authentication controls. Provide expert level input and feedback on endpoint security strategies, designs, and implementation/integration efforts for EIS initiatives. This will include, but not be limited to, anti-malware, data loss prevention, OS hardening, and other host-based security initiatives. Engage with Agency-wide functional teams to implement security initiatives according to agency roadmaps and strategic plans. Ensure security initiatives are implemented according to defined policies and standards for information security. Provide a forward-looking view of the threat, predicting shifts in adversarial intent, goals, and strategic objectives agency executive leadership. Provide expert analysis of log management, scanning and security monitoring tools, including but not limited to the detection of criminal, fraudulent, illicit access, outside penetration activities on the CDCR network.
20%	**Security Platform Administration- Operations** Act as a lead in the architecting, deployment, and administration of onsite and remote access end points access to CDCR systems and resources from internal staff, interagency, inmate and public users. Administer and manage network security platforms and appliances. Responsible for the life cycle management of security solutions, from its initial implementation to decommission (installation, setup and initial configuration, installation of patches, corrective changes, etc.). Ensure implementation of organizationally defined standards on security systems. Protect security systems by defining and managing access privileges and controls structures. Work with various EIS operational units to coordinate overall security implementation. Work with the Cyber Security Intelligence and Operations Center (SIOC) to continuously improve day-to-day operations of cyber security functions while defining work practices and relevant metrics for security and operational management. Identify and manage security event log sources to ensure Cyber SIOC operations have access to the necessary intelligence for monitoring and response purposes. Identify, implement strategies, and manage Security orchestration, automation and remediation opportunities that align with Cyber SIOC operational processes.
20%	**Incident Response** Participate in the creation, enhancement, and management of the Incident Response Plan (IRP) which include communications strategy, operational procedures, and incident playbooks for the SIOC and OISO. Act in a lead role for response and remediation activities during a cybersecurity incident including documentation of activities within case reports. Provide recommendations and implement approved countermeasures, mitigating controls, and remediation efforts to mitigate cyber security risks. Communicate effectively with the appropriate stakeholders within technical units and business leadership on remediation.
20%	**Security Intelligence** Guide and support high-tech law enforcement investigations to ensure the protection of staff, public, facilities and assets through the evaluation of insider threat intelligence and incorporate new threat hunting practices or other mitigations, as needed. Take a lead role in developing and deploying sound and well-documented digital forensics-related (host, network, cloud, and open source) products and services, provide ongoing support, and implement improvements that advance the effectiveness and efficiency of our digital forensic efforts. Develop user and

	administrative guides to standardize mitigation practices across the organization aiming to increase security, consistency, and efficiency.
10%	**Risk Management** Assist the OISO in developing security strategies to incorporate into the Statewide vision and solve business problems while taking safety, pro-active intelligence-based cybersecurity, cost, complexity, supportability and client experience into consideration. Participate in the security operations planning for the CDCR by assisting the OISO and the CDCR Governance, Risk and Compliance (GRC) unit in developing and testing incident response, communications, emergency operations, business continuity, and technology recovery plans. Coordinates department OISO, IT, and critical infrastructure teams to continuously perform complex risk assessments and security mitigation efforts on all projects that are being proposed within the CDCR and cloud architectures. Identify and report back the risk impact of projects on the overall CDCR infrastructure by interpreting business requirements and detailed design documents. Apply advanced knowledge of network security to identify risks relevant to the project and CDCR enterprise network. Ensure IT projects employ practices within applicable state and federal regulatory information security requirements. Participate in the development of information security policies and procedures for the OISO by ensuring compliance with the appropriate security regulations, standards, or best practices (e.g. NIST, FIPS, FedRAMP, etc.).

SPECIAL PERSONAL CHARACTERISTICS

- Influence, change, and strengthen the community. Set an example each day through positive and pro-social role modeling, utilizing dynamic security concepts through observation and building rapport.
- Willingness to play a significant role in the collaborative efforts toward rehabilitation and public safety enhancement.
- Ability to facilitate conversations as a coach and mentor, engaging in a respectful and understanding manner.
- Ability to build trust, improve communication, and assist with the transformation of correctional culture.

SPECIAL REQUIREMENTS

- CDCR does not recognize hostages for bargaining purposes. CDCR has a "NO HOSTAGE" policy, and all incarcerated individuals, visitors, nonemployees and employees shall be made aware of this.

CONSEQUENCE OF ERROR

The consequence of error at the Specialist I level may result in loss of data, user dissatisfaction, and impact to the organization, project, or work unit, and related support units. Consequences include operational down time, loss of business continuity, and poor customer service and performance.

To be reviewed and signed by the supervisor and employee:

EMPLOYEE'S STATEMENT:

- *I HAVE DISCUSSED THE DUTIES AND RESPONSIBILITIES OF THE POSITION WITH MY SUPERVISOR AND RECEIVED A COPY OF THIS DUTY STATEMENT.*

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

SUPERVISOR'S STATEMENT:

- *I CERTIFY THIS DUTY STATEMENT REFLECTS CURRENT AND AN ACCURATE DESCRIPTION OF THE ESSENTIAL FUNCTIONS OF THIS POSITION*
- *I HAVE DISCUSSED THE DUTIES AND RESPONSIBILITIES OF THE POSITION WITH THE EMPLOYEE AND PROVIDED THE EMPLOYEE A COPY OF THIS DUTY STATEMENT.*

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