Form **DS R-1** State of California Secretary of State	# Duty Statement **Rank & File**	☐**Proposed** (Submit to HR for Review) ☒**Final**

Print or type.
See Specific Instructions on page 2.

A. Current Position Number 785-100-1406-002	B. Probationary Period /JEP Period 12 months	
C. Incumbent Name Vacant	D. Classification/Job Title Information Technology Manager II / Chief Risk Officer (CRO)	E. Date of Hire
F. Unit, Section, Division Information Technology Division		G. Location ☒ Sacramento ☐ Los Angeles
H. Name of Immediate Supervisor/Manager Reggie Fair	I. Classification/Title of Immediate Supervisor/Manager CEA C – Chief Operating Officer	
J. Bargaining Unit (CBID) ☒ BU 1	K. Time Base ☒ Full Time ☐ Part Time ☐ Other	L. Tenure ☒ Permanent ☐ Permanent Intermittent ☐ Limited Term ☐ Intermittent ☐ Other
M. Work Schedule Monday – Friday	N. Work Hours 8:00 AM- 5:00 PM	Occasional off-hours and weekends may be required
O. Background Check Required ☐ Yes ☒ No	P. Job Requires Driving Automobile ☐ Yes ☒ No	Q. Certification Required ☐ Yes Click here to enter text. ☒ No

Section II JOB DESCRIPTION

Under the administrative direction of the Chief Operating Officer, the Information Technology Manager II serves as the Secretary of State (SOS) Chief Risk Officer (CRO) with full management responsibility for establishing and managing the most complex operation of the SOS Risk Management Office. The CRO performs at the mastery level of this career series, directing the most complex initiatives and initiating key actions on a wide variety of complex risk and security related tasks. The CRO will assist the CIO in ensuring information assets and associated technology, applications, systems, infrastructure, and processes are adequately protected in the digital ecosystem in which it operates. The scope of this role will include extensive risk and information security oversight, reporting, governance, communications, education, and consulting. The CRO is a member of the SOS Cybersecurity Program.

ESSENTIAL FUNCTIONS

40% **Risk Management Office Administration**

Domains: Information Security Engineering, Business Technology Management, IT Project Management

Manage the Risk Management Office comprising of the SOS information security officer(s) and risk administrator(s) supporting the most complex systems including the Department of Homeland Security (DHS) designated mission critical infrastructure. Responsibilities involve the hiring, managing, mentoring and developing a high performing staff of information security professionals, performance management, and annual performance reviews. Lead the office to provide a cohesive and collaborative risk, compliance and information security team to ensure effective and efficient risk, compliance, and security oversight. Responsible for identifying, evaluating, and reporting on legal and regulatory, IT, and cybersecurity risk to information assets, while supporting and advancing business objectives. Administer the risk management and information security function across the SOS to ensure consistent and high-quality risk and information security management in support of the business goals. Coordinate with the CIO and executive team in the development, implementation, and maintenance of the security, risk, compliance management and audit framework program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy, and recovery of information assets owned, controlled and/or processed by the organization. Proactively work with the business programs and ecosystem partners to implement practices that meet agreed-on policies and standards for risk management and information security.

35% **Information Security Oversight and Consulting**

Domains: IT Project Management; Information Security Engineering, Systems Engineering, Software Engineering, Business Technology Management

Direct the development, periodic review and update of information security and risk management policies, procedures, standards and guidelines, and oversee their approval and dissemination, and maintenance. Ensure data privacy requirements are included where applicable. Review and approve the criteria and processes by which the risks associated with new services, new ventures and major changes to services, are assessed and managed. Identify key current and future operational and business risks which include the maintenance of both operational and business risk events. Develop business metrics to measure the effectiveness of the security management program and increase the maturity of the program overtime. Conduct assessments to evaluate the design and effectiveness of risk mitigation and management strategies. Responsible for the development of effective reporting of risk that will be used to convey effective understanding and management of critical and principal risks to SOS stakeholders.

Oversee the evaluation, selection and implementation of information security solutions that are innovative, cost effective, and minimally disruptive. Partner with Information Technology (IT) operations, infrastructure, and applications teams to ensure that technologies are developed and maintained according to security policies and guidelines. Ensure security is embedded in the project delivery process by providing appropriate information security policies, practices and guidelines. Act as a champion for the agency information security program and promote a secure and risk-aware culture by defining and executing a security and risk communication and training strategy to develop resources with requisite skillsets, awareness and capabilities to manage and embed risk management and security practices throughout the business programs. Ensure sufficient support to risk owners is available to assist in defining and rating risks and assist owners understand their compliance obligations and controls. Enhance the agency understanding of security beyond a compliance-view only.

20%

Risk and Compliance Management

Domains: : Information Security Engineering, Systems Engineering, Software Engineering, Business Technology Management, Client Services

Manage and direct the office operation to ensure the risk and compliance software is operating effectively to support monitoring of risk registers and potential changes in the agency environment affecting risk. Coordinate with IT and business programs to ensure that all information owned, collected or controlled by or on behalf of the agency is processed and stored in accordance with applicable laws and other regulatory requirements, such as data privacy. Monitor the industry and external environment of emerging threats and advise relevant stakeholders on appropriate course of action.

Coordinate the development and implementation of incident response plans to ensure business-critical services are recovered and the investigation of security breaches, and assist with any associated disciplinary, public relations and legal matters. Manage and contain information security incidents and events to protect the agency assets and reputation. Leverage available tools and technologies to automate risk management activities, including risk assessments, risk reporting, issue management, monitoring/testing and policy administration. Ensure risks assessment on business incidents and errors are being conducted and there is an effective compliance testing program.

MARGINAL FUNCTIONS

5%

Business Relationship Management

Domain: : IT Project Management; Information Security Engineering, Systems Engineering, Software Engineering, Business Technology Management, Client Services

Build and nurture external networks consisting of industry peers, ecosystem partners, vendors and other relevant parties to address common trends, findings, incidents, and cybersecurity risks. Liaise with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organization maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies. Liaise with the enterprise architecture team to build alignment between the security and enterprise (reference) architectures, thus ensuring that information security requirements are implicit in these architectures and security is built in by design.

Section III EMPLOYEE/SUPERVISOR STATEMENT

You are a valued member of the Secretary of State’s office. You are expected to conduct yourself professionally and work cooperatively with team members and others during the course of your duties to enable the department to provide the highest level of service possible. You are to adhere to all applicable state and federal laws, rules and department policies; and exercise good judgment in assisting team members and the public. Your efforts to treat others fairly, honestly and with respect are critical to the organization’s mission and values.

EMPLOYEE’S STATEMENT: I HAVE READ AND UNDERSTAND THE DUTIES, RESPONSIBILITIES, AND PERFORMANCE EXPECTATIONS OF THE POSITION AND DISCUSSED WITH MY SUPERVISOR. I HAVE RECEIVED A COPY OF THE DUTY STATEMENT.

I CAN PERFORM THE ESSENTIAL FUNCTIONS OF THE POSITION WITH OR WITHOUT REASONABLE ACCOMMODATION:

□ YES

□ NO (Notice HR to discuss possible reasonable accommodation)

EMPLOYEE NAME (PRINT FULL NAME)	EMPLOYEE SIGNATURE	DATE SIGNED

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

SUPERVISOR NAME (PRINT FULL NAME)	SUPERVISOR SIGNATURE	DATE SIGNED