Form **DS-RF**
State of California
Secretary of State

Duty Statement
Rank and File

Section I **POSITION INFORMATION**

Print or type.

A. Current Position Number	B. Probationary Period/Job Evaluation Period	C. Form 700 Filer?
785-113-1415-001		Yes

D. Incumbent Name	E. Classification/Job Title	F. Date of Hire
Vacant	Information Technology Specialist III / Information Security Officer (ISO)	

G. Unit, Section, Division	H. Location
Executive Division, Information Security	Sacramento

I. Name of Immediate Supervisor/Manager	J. Classification/Title of Immediate Supervisor/Manager
Ivonne Cedillo	ITMII Chief Information Security Officer

K. CBID (Bargaining Unit)	L. Time Base	M. Tenure
R01	Full Time	Permanent

N. Work Schedule	O. Work Hours	P. Telework
Monday – Friday	8:00AM – 5:00PM, Occasional off-hours and weekends may be required	100% Remote

Q. Background Check Required	R. Job Requires Driving Automobile	S. Certification Required
☐ Yes	☐ Yes	☐ Yes Click here to enter text.
☒ No	☒ No	☒ No

Section II **JOB DESCRIPTION**

Indicate the major functions and associated duties, and the percentage of time spent on each (list higher percentages first). Essential functions assigned less than 5% should be combined with other task statements. The total percentage of all functions, including marginal, must equal 100%.

DESCRIBE THE ORIGINAL SETTING AND MAJOR FUNCTIONS

Under the administrative direction of the Chief Information Security Officer (CISO), the Information Technology Specialist III serves as the Secretary of State (SOS) Information Security Officer (ISO) with full management responsibility for establishing and managing the most complex operation of the SOS Information Security and Cybersecurity domains. The ISO will lead and manage information security and awareness, training, intrusion prevention, incident response, tabletop exercises, risk assessment, and compliance reporting to the California Department of Technology (CDT). The ISO ensures that the organization's information assets are protected from unauthorized access, disclosure, alteration, destruction, or theft. The ISO is also responsible for promoting the organization's awareness of information security issues. The incumbent will collaborate with the Information Technology Division, Risk Management, Audits, and Executives to mature the information security program to develop security policies and standards to ensure confidentiality, integrity, and availability of information assets.

ESSENTIAL FUNCTIONS

Percentage	Description of Duty
40%	**Information Security Officer (ISO)** **Domains: Information Security Engineering, Business Technology Management, IT Project Management** The ISO will help develop and maintain an information security strategy and program that aligns with the organization's goals and objectives. Conduct regular risk assessments to identify potential security threats and vulnerabilities. Develop and maintain policies, procedures, and standards for information security and ensure that they are followed throughout the organization. Provide guidance and support to employees and departments to ensure compliance with information security policies and procedures. Develop and deliver information security awareness and training programs for all employees. Monitor and respond to security incidents, investigate security breaches, and implement corrective actions as necessary. Responsible for identifying, evaluating, and reporting on legal and regulatory, IT, and cybersecurity risks to information assets while supporting and advancing business objectives. Coordinate with the Chief Information Officer (CIO), Audit Office, Chief Risk Officer (CRO), 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.
40%	**Information Security Oversight and Consulting** **Domains: IT Project Management; Information Security Engineering, Systems Engineering, Software Engineering, Business Technology Management** Develop, implement, and maintain a comprehensive information security program to protect the organization's information systems and data. Conduct regular security assessments and vulnerability testing to identify and mitigate potential security risks and threats. Monitor security logs and alerts to identify potential security incidents and respond promptly to mitigate risks and minimize impact. Work closely with all departments to ensure compliance with relevant security policies, procedures, and regulations. Monitor and respond to security incidents, breaches, and violations in a timely and effective manner. Develop and maintain disaster recovery and business continuity plans to ensure the organization can continue to operate in the event of a security incident or outage. Stay up-to-date with the latest security technologies and industry trends to ensure the organization's security program is current and effective. Collaborate with external vendors, partners, and other stakeholders to ensure their compliance with the organization's security policies and procedures. Provide regular reports to senior management on the status of the organization's security program, including any identified risks and vulnerabilities.
15%	**Incident and Threat Response** **Domains: : Information Security Engineering, Systems Engineering, Software Engineering, Business Technology Management, Client Services** The ISO helps develops and educate on the threat model for the Agency in order to properly plan for possible information security incidents. During suspected information security incidents, the ISO provides leadership and guidance around the agency response. This includes being responsible for developing a response plan, leading response actions, and working to ensure containment and recovery. The ISO primarily advises the CIO, Chief Risk Officer, and Chief Deputy Secretary on response activities that may result in press releases, substantial costs, and potential lawsuits and fines. The ISO may be involved in highly confidential investigations of employee misuse or policy violation.

MARGINAL FUNCTIONS

Percentage	Description of Duty
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.

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 that fall within their classification, including work in other functional areas to cover absences or relief, to equalize peak work periods or otherwise balance the workload.

Section III EMPLOYEE/SUPERVISOR STATEMENT

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: (If you believe reasonable accommodation is necessary, please initiate a discussion with either your supervisor or the Secretary of State's Human Resources Bureau).

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
➧	➧	➧