DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY BRANCH
VULNERABILITY MANAGEMENT UNIT

DUTY STATEMENT

JOB TITLE: Information Technology Specialist I **POSITION #:** 472-508-1402-022

WORKING TITLE: Security Operations Specialist (Northern)

EMPLOYEE:

POSITION DESCRIPTION: Under direction of the Vulnerability Management Supervisor (Information Technology Supervisor II), the Information Technology Specialist I (ITS I) supports the Department of Developmental Services (Department) enterprise vulnerability management program with an emphasis on coordination with Northern California Department locations. The incumbent monitors vulnerability scanning coverage, identifies and validates security exposures affecting endpoints, servers, network devices, and managed cloud resources, and works with responsible technical teams to prioritize, track, and verify corrective actions. The position supports statewide asset visibility, system hardening, technical reporting, and compliance with applicable state security requirements. The incumbent does not independently authorize production changes or assume ownership of infrastructure operations.

SUPERVISION EXERCISED: None.

SUPERVISION RECEIVED: Reports to and under direction of the Vulnerability Management Supervisor (Information Technology Supervisor II).

DOMAIN(S):	Client Services	Basic
	Business Technology Management	Basic
	Software Engineering	Basic
	IT Project Management	Basic
	System Engineering	Moderate
	Information Security Engineering	Advanced

EXAMPLES OF DUTIES:

Essential Job Functions:

35% Vulnerability Identification, Scanning, and Asset Coverage. Administer and maintain vulnerability management tools and processes consistent with applicable Department requirements and SIMM 5345-A. Maintain scheduled authenticated and other approved scans across Department headquarters, facilities, endpoints, servers, network devices, and managed cloud environments. Compare scan results with available asset inventories to identify unmanaged assets and gaps in coverage. Validate significant findings, assess exposure and business impact, prepare risk-based corrective action recommendations, and coordinate vulnerability data integration with designated SIEM and service management personnel.

30% Remediation Coordination and Verification. Work with Northern California and enterprise technical support teams, system owners, and infrastructure personnel to communicate vulnerability findings and remediation priorities. Track assigned corrective actions, document risk decisions and approved exceptions, verify patching or configuration changes through rescanning and other evidence, and monitor for recurring findings or regressions. Produce operational reports on remediation progress, outstanding exposures, scanning coverage, and process improvement opportunities. Infrastructure teams retain responsibility for implementing production changes.

15% Security Standards, Risk Reviews, and Change Validation. Participate in risk and technical standards reviews of Department systems and IT projects. Assess security configuration and hardening against approved baselines; identify deviations and recommend corrective actions. Review evidence of change management approvals and post-change security validation to help identify unintended exposure or operational impacts. Coordinate findings with responsible system owners and the VMU Supervisor.

15% Security Advisory Analysis and Supervisor Reporting. Monitor, analyze, and categorize Common Vulnerabilities and Exposures (CVEs), security advisories, and informational alerts from external agencies. Assess potential impacts to Department assets and provide regular technical findings, status reports, and recommended corrective actions to the VMU Supervisor. Coordinate with Northern California and enterprise IT staff regarding required patches, remediation priorities, and verification. Support the supervisor in preparing management briefings and escalating significant security risks to ISO leadership as directed.

Marginal Job Functions:

5% Other duties as assigned within the scope of the classification, including training, exercises, and temporary support during significant cybersecurity events.

WORKING CONDITIONS: Work is performed primarily in an office or approved telework environment, with the position headquartered at Allenby. Duties require prolonged computer use, detailed technical analysis, and coordination during time-sensitive security events. After-hours, weekends, or on-call support may be required. Occasional travel may be required including day trips or overnight assignments to other Department locations. This position is a hybrid, in-office/telework position, and may be subject to change. Incumbent can be required to report to the office, or any designated location at any time. Telework agreements can be modified and/or cancelled at any time.

DESIRABLE QUALIFICATIONS:

Knowledge of: Administering vulnerability scanning and exposure management tools such as Tenable or comparable platforms; validating scan coverage against asset inventories; assessing Windows desktop and server configurations, network infrastructure, and managed cloud assets; and coordinating patching and remediation verification; CVE and security advisory analysis, SIMM 5345-A, security baselines, change management, SIEM and service management integrations, Microsoft Sentinel, ServiceNow, and cloud monitoring in Microsoft Azure, Microsoft 365, or AWS; PowerShell, SQL, regular expressions, scripting, GitHub/DevOps, and responsible generative AI use for security analysis;

Ability to: Demonstrate sound technical judgment, risk-based prioritization, clear written reporting, and effective collaboration with local and enterprise IT teams.

CERTIFICATION OR LICENSE: None.

Employee Name (Print)	Employee Signature	Date

Supervisor Name (Print)	Supervisor Signature	Date

Employee and Supervisor acknowledge that by signing this Duty Statement that they have discussed and agree to the expectations of the position.