

**DUTY STATEMENT
OFFICE OF LEGISLATIVE COUNSEL
LEGISLATIVE DATA CENTER
LEGISLATIVE TECHNOLOGY BRANCH
INFRASTRUCTURE SERVICES DIVISION**

CLASSIFICATION TITLE: Information Technology Specialist II
Infrastructure Services Division (ISD)

WORKING TITLE: Senior Infrastructure Security Specialist
POSITION NUMBER: 154-1414-011

EFFECTIVE DATE: XX/XX/2023

ORGANIZATION SETTING AND MAJOR FUNCTIONS

Under the direction of the Deputy Director of the Infrastructure Services Division, the Information Technology Specialist II (ITS II) acts as a senior infrastructure security consultant, subject matter expert and technical/project lead in the successful delivery of secure infrastructure solutions and services both on-premises and in the cloud. The ITS II works with a highly specialized team of IT professionals and communicates and collaborates directly with cross-divisional technical teams at Legislative Data Center (LDC). The ITS II is responsible for the successful and secure delivery of critical infrastructure technology services and programs in a matrix-managed environment. The ITS II is responsible for developing, implementing, and maintaining robust security measures to protect data and ensure compliance with industry standards and regulations.

The ITS II has a strong understanding of infrastructure security best practices and industry standards required to meet the evolving business needs of the legislature. The ITS II partners with the Cybersecurity, Network and Environmental (CNE) Division to identify and mitigate security issues/vulnerabilities, implement effective security controls, and to integrate security best practices into project workflows, including the software development lifecycle (SDLC), to ensure the delivery of secure products and services to our customers, and to develop and implement comprehensive security strategies and measures across our technology infrastructure. The ITS II plays a critical role in ensuring the security and scalability of our on-premises/cloud-based/hybrid solutions and services and for maintaining a secure and reliable technology environment.

The ITS II acts as an infrastructure security liaison forming a bridge between other divisions and technical teams, and is responsible for ensuring the security, integrity, and availability of both on premise and cloud-based infrastructure services. The ITS II plans, implements, and manages infrastructure security measures to protect critical systems, data, and applications from potential threats and vulnerabilities and works closely with cross-functional teams to identify risks, implement security solutions, and continuously monitor and improve the security posture of the organization. The ITS II collaborates with the CNE Division and data stakeholders to configure security controls and ensure that data protection measures align with data governance policies and compliance requirements. The ITS II works as a key member of legislative

project teams in the delivery of IT solutions designing, implementing and maintaining security measures across infrastructure tiers. The ITS II implements measures needed to ensure that physical and virtual infrastructure, including servers, networks, and storage, is protected and secure. The ITS II works with the project teams to implement security best practices such as encryption, access controls, data segregation, data loss prevention, and data retention policies, all tailored to the unique requirements and risk profiles of each tier.

The area of responsibility managed by the ITS II is critical to the business success of the LDC, the Office of Legislative Counsel (OLC), and the Assembly and Senate Legislative Members where the consequence of error is high. Duties include, but are not limited to:

50% Infrastructure Security Lead

- Provides technical leadership and IT support in the delivery of secure technology services and solutions for the Senate, Assembly, and legislative support office customers throughout California. Leads, analyzes, and resolves the most complex customer requests.
- Designs and implements the infrastructure security measures needed to protect data stored on premise and in cloud environments against unauthorized access, including secure authentication methods, encryption, access control lists, intrusion detection systems, firewalls, and other measures. Partners with security specialists in the CNE Division to design and implement new security protocols as needed. Continuously monitors LDC's infrastructure and cloud presence, analyzing threats to the organization's security, and designing/implementation solutions to mitigate those threats. Collaborates with incident response teams to develop incident response plans and conduct regular incident response exercises.
- Leads the planning of the overall organizational IT cloud security strategy. Communicates with stakeholders to determine organizational needs. Evaluates proposed new cloud-based technologies and services for meeting business requirements of the California Legislature. Works with internal technical teams to ensure that new cloud architecture meets the strategic plan of the agency. Reviews and/or participates in the evaluation of new cloud technologies and services that potentially improve staff productivity or provide a means to better meet the needs of the legislative offices. Evaluates request proposals for new/enhanced information technology services requested by the Legislature and make appropriate recommendations and/or decisions.
- Conducts comprehensive risk assessments to identify potential security vulnerabilities and threats, evaluating security controls, assessing data flows, and determining the potential impact of a security breach. Implements/manages continuous monitoring and alerting systems to detect and respond to security incidents. Reviews configurations to ensure systems are hardened appropriately to reduce the security weaknesses and vulnerabilities that threat actors can exploit. Regularly performs vulnerability scans to identify and remediate security weaknesses.
- Stays up-to-date with emerging trends and technologies in the cybersecurity field to provide innovative and cutting-edge solutions. Stays up-to-date with relevant data security standards and compliance regulations and ensure that infrastructure security controls align with these standards and assists in compliance assessments.

40% Consultant/Advisory

- Demonstrates expert knowledge across multiple technical areas to support complex application security architecture solutions. Identifies, establishes, and maintains relationships with key information technology stakeholders to assure effective communication takes place on business requirements, operational and project objectives and issues related to the most complex legislative information technology products and services.
- Serves as the primary liaison between ISD and the CNE division, and coordinates with system owners, common control providers, and the technical teams on the allocation of security controls as system-specific, hybrid, or common controls. Works with the CNE division to partner with other divisions within LDC to provide security services including application security reviews/assessments.
- Provides recommendations on infrastructure architecture, hardware, software, and network configurations to optimize application performance, scalability, security and reliability.
- Provides technical security guidance and mentoring to engineers, designers, and developers.
- Creates a high-performance environment at the LDC and within service and project teams to ensure the highest quality information technology solutions are developed that meet the business objectives of LDC's customers.
- Provides technical and project leadership on major service developments and project assignments; monitors project progress and development to ensure milestones are met and deliverables meet service and project objectives and requirements. Provides status to LDC management and Information Technology stakeholders.
- Assists in the definition and development of policies, missions, goals, plans, and objectives of ISD as well as provides consultative support to other units within the agency and the Legislature.
- Works closely with vendors to assess new technologies and to provide oversight, negotiate contract modifications, and analyze compliance with contract specifications.
- Serves in a consultative capacity to agency executives and the Senate and Assembly Rules Committees.

10% Mentorship/Training

- Provides mentorship, training, and knowledge transfer to staff on information and skills related to secure infrastructure/application/cloud architectures, technical administration, services and solutions.
- Provides training, assistance and prepares documentation to support specialized work processes, acting as a liaison to OLC staff, LDC staff and legislative staff.
- Works as a partner to the CNE division in helping keep LDC teams abreast on latest security standards and guidelines.
- Mentors LDC staff, providing procedural guidance on matters related to the development, implementation, support, and maintenance of mission-critical IT applications.
- Assists IT project managers, sponsors, management, and executive management in identifying and managing delivery opportunities and providing support and guidance on projects/efforts that are experiencing problems.

Information Technology Domains:

Legislative Technology Consultants:
Applications Services:

Critical skills
Critical skills

Information Security:	Critical skills
Systems Infrastructure:	Critical skills
Network Infrastructure:	Critical skills
Business Technology Management:	Moderate skills
Client Services:	Moderate skills
Project Management:	Critical skills

WORK ENVIRONMENT REQUIREMENTS

- Core business hours are 8:00 a.m. – 5:00 p.m. Schedule may be adjusted and is contingent upon business needs.
- The ITS II must carry a mobile device during core business hours and off-shift hours, evenings, weekends, and State Holidays for the ability to respond to calls after hours and lead multi-disciplinary IT professional teams in organizing, analyzing, troubleshooting, and resolving IT problems.
- The ITS II uses secured LDC virtual private network technologies from off-site locations to access LDC’s applications/systems to perform job duties outside of standard business hours. Occasional travel may be required.
- Frequent sitting, keyboarding, and use of mouse.

ALLOCATION FACTORS

Supervision Received:

- The ITS II reports to the Deputy Director of ISD. Assignments are made by the Deputy Director and are general in nature, accompanied by any special constraints and/or requirements. The ITS II is responsible for analysis, planning, researching, and implementation of these assignments.

Actions and Consequences:

- The ITS II is responsible for applying IT policies, standards, processes, procedures. Works with executive management, legislative customers and internal IT teams to identify business problems, opportunities and solutions to advance business programs and services.
- The consequence of poor decisions, judgment or advice, or inadequate research may have a negative and serious impact on the reputation of the LDC and upon customer confidence levels. The quality of the services is critical; risks to California’s legislators and LDC are extreme due to the political nature of customer environment.

Personal Contacts:

- The ITS II works closely with OLC executive staff, Senate and Assembly Rules executive staff, all LDC management, business, technical, operations, and administrative personnel, with the vendor community, and other public agencies.
- The ITS II must develop and maintain strong working relationships with executives,

management, peers, staff, and vendors.

Administrative Responsibilities:

- The ITS II is responsible for planning, budgeting, and tracking of the projects, tasks, and activities within the ITS II's purview.

Supervision Exercised:

- The ITS II may lead or direct work and/or assignments but does not supervise staff or provide day-to-day operational management or supervision.
- The ITS II has defined responsibility and authority for highly complex decision-making related to technology projects under ITS II's purview.

Knowledge, Skills, and Abilities Required:

Knowledge of:

- The principles and methods to identify, analyze, specify, design and manage highly complex functional business and infrastructure requirements.
- Security architecture concepts and enterprise architecture reference models.
- Engineering concepts and practices as applied to systems security and systems architecture.
- Security assessment and authorization processes.
- Authentication, authorization, and access control methods.
- System testing and evaluation methodologies and processes.
- Application security system concepts and functions.
- System life cycle management principles, including software security and usability.
- Industry standards and organizationally accepted analysis principles and methods.
- Web based attacks and the OWASP top ten.
- NIST Cybersecurity Framework and CIS Critical Security Controls.
- Configuring and using software-based computer protection tools.
- Application firewall concepts and functions (e.g., single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).
- Network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML)
- System hardening standards and best practices required to ensure the organization's resources are protected, and the tools, methods, and best practices used to reduce the attack surface in technology infrastructure.
- Analysis methods to obtain and translate legislative customers' business and information needs into automated legislative process solutions, and to resolve data processing issues and computer systems errors.
- On-premise and cloud-based IT architectures and cloud providers.

- Project management practices to ensure projects stay on schedule and appropriate action is taken when problems occur and apply risk management practices to mitigate risk of failure of projects.
- Current teaching and training methods and techniques to instruct customers on the use of the business applications and technologies.
- Customer service and support practices to provide the levels and types of services required to meet customers' business needs.
- Hardware and software supported by LDC to assist in determining the hardware and software requirements for new customer requests.
- Human behavior and motivation techniques to create a high-performance work environment and encouraging positive working relationships with all levels of the organization and cross-functional teams.
- Information technology concepts, best practices, methods and principles that support legislative business solutions and decision-making.
- Legislative environment and legislative process, including the legislative calendar and deadlines, to provide effective information technology services and solutions.
- OLC Vision, Mission, Values, organizational structure, policies, processes, procedures, rules and regulations.
- Public administration and organizational principles to coordinate and prioritize all incoming legislative requests to effectively meet deadlines.
- Testing methods and procedures to oversee test plans that validate the functional and performance criteria required to meet the customers' information system requirements and the information technology environment for projects.

Skills and Ability to:

- Apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management.
- Perform security reviews and identify gaps or determine the capability of security architectures and designs (e.g. firewall, virtual private networks, routers, servers, etc.), and develop a security risk management plan.
- Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Serve as the primary liaison between ISD and the CNE division, and coordinates with system owners, common control providers, and the technical teams on the allocation of security controls as system-specific, hybrid, or common controls.
- Design multi-level security/cross domain solutions.
- Apply the methods, standards, and approaches for describing, analyzing, and documenting enterprise information technology architecture.
- Create a high-performance work environment and perform effectively with cross-functional teams to meet goals and objectives.
- Motivate, guide, coach, and mentor others by conveying a commitment to the work assignment that ties to the support of the OLC vision, mission, and values.
- Analyze critical data and politically sensitive situations, reason logically, prudently, and creatively. Draw valid conclusions, develop effective solutions, and use a variety of analytical techniques to resolve highly complex problems and make mission critical recommendations.

- Coordinate and conduct demonstrations of the LDC's information technology solutions that support California's legislative processes to legislators, high-ranking legislative staff and OLC executives.
- Act as an advisor to executive management, managers, supervisors, colleagues, team members in applying information technology to legislative processes.
- Advise management on formulating IT strategy, policy, and governance throughout the organization and enterprise wide.
- Address detailed examination from legislative leaders, members, and high-ranking legislative staff without deferral or delegation in a discreet and nonpartisan manner on technology initiatives.
- Design, develop and present visual presentations to inform legislative leaders, members, high-ranking legislative staff, executive management, managers, supervisors, colleagues and team members of program or project issues, status, system features, and proposals.
- Effectively communicate both orally and in writing with legislative leaders, members, high-ranking legislative staff, executive management, managers, supervisors, colleagues, team members, contractors, and vendors.
- Efficiently and effectively, manage time and resources allocated to complete program, project and operational assignments.
- Establish and maintain strong cooperative and collaborative working relationships with others including executive management, managers, supervisors, colleagues and team members.
- Exercise discretion when confronted with strong pressures for and exposure to disclose confidential information because of the partisan nature of the Legislature.
- Exercise sound fiscal responsibility to adhere to fiscal guidelines, regulations, principles, and standards of the OLC when committing resources for program, project, or operational support.
- Listen, discern, and constructively summarize subtle and sensitive communications from legislative staff in a partisan political environment.
- Provide quality and timely ad hoc assignment information to executives, team members, and stakeholders.
- Provide vendor management and oversee planning and control of assignments, including management of communications, risks, issues, change requests, and incident tracking for the legislative applications and services assigned to the section.
- Maintain an arm's length and nonpartisan relationship with partisan legislative leaders, members, and legislative staff.
- Quickly adapt to changes in program, project, and operational priorities by being flexible in shifting schedules, milestone, resources or competing priorities.
- Research advanced knowledge of new and emerging legislative business, information technology and/or industry trends related to the functional areas of the Legislature.
- Write clear and concise problem analyses, operations procedures, and training manuals to fully document customers' business requirements and needs.

I have discussed with my supervisor the duties of the position and have received a copy of the duty statement. I certify that I am able to perform the duties of this position with or without reasonable accommodation.

Employee's Signature

Date