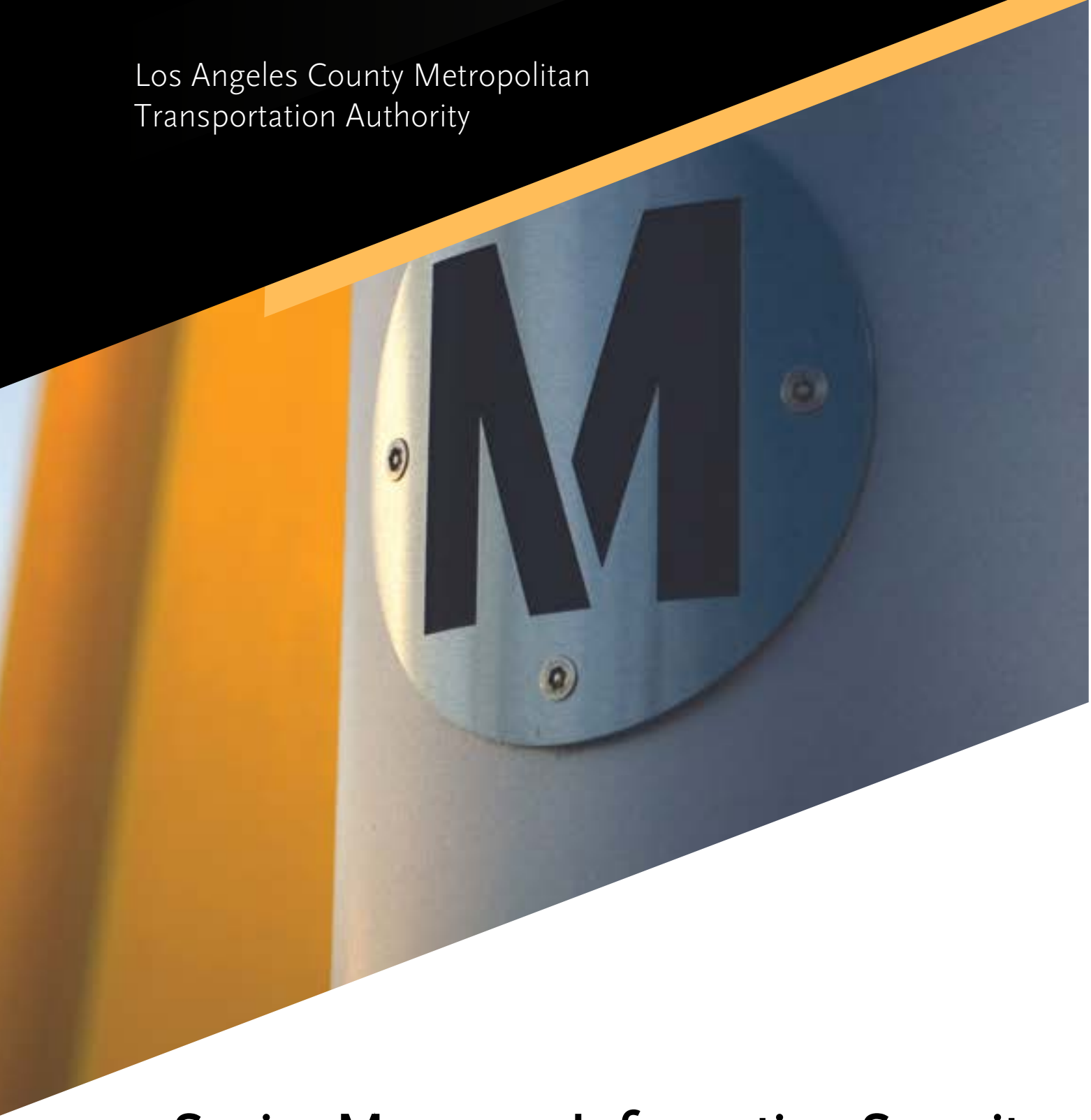
Los Angeles County Metropolitan
Transportation Authority



# Senior Manager, Information Security

Metro

Trusted Hiring Partner

GOMEZ PARTNERS

# ABOUT


**The Los Angeles County Metropolitan Transportation Authority**, also known as *Metro*, is the county agency that plans, operates, and coordinates funding for most of the public transportation system in Los Angeles County, California, the most populated county in the United States.

Metro is unique among the nation's transportation agencies. Metro serves as transportation planner and coordinator, designer, builder, and operator for the country's largest, most populous county. More than 10 million people – nearly one-fourth of California's residents – live, work and play within Metro's 1,433-square-mile service area.

The agency directly operates a large transit system that includes bus, light rail, heavy rail (subway), and bus rapid transit services; and provides funding for transit it does not operate, including Metrolink commuter rail, municipal bus operators and paratransit services.

Metro


## MISSION

**Metro** safeguards the transit community by taking a holistic, equitable, and welcoming approach to public safety. Metro recognizes that each individual is entitled to a safe, dignified, and human experience.

## VALUES

- Implementing a **Human-Centered Approach**
- Emphasizing **Compassion** and a **Culture of Care**
- Recognizing **Diversity**
- Acknowledging **Context**
- Committing to **Openness** and **Accountability**

Metro

# THE COMMUNITY




A place for bold dreams, creative expression and limitless possibilities, Los Angeles is a city defined by its people. One of the most culturally diverse destinations in the world with Angelenos from 140 countries who speak 224 different languages, LA inspires visitors to immerse themselves in unique perspectives, unexpected moments and open-hearted community. There's always something new to discover in the City of Angels whether you're a frequent visitor or a first timer, with an abundance of multi-faceted neighborhoods and hidden gems to explore. From world-class museums and championship sports teams to beautiful beaches and one-of-a-kind culinary experiences, Los Angeles invites you to join our vibrant, bustling community of dreamers and doers.

Metro

Senior Manager,
Information Security

# THE BENEFITS

*Providing Outstanding Employee Benefits*

- **Medical & Dental Coverage**: Metro will cover a significant portion of your health care premiums.
- **Retirement & Pension**: Save for your future with 401K and 457 retirement plans PLUS a generous pension plan.
- **Career Paths:** Metro provides educational reimbursement, professional development, certifications, and training programs to advance your career.
- **Work-Life Balance**: Metro offers employees flexible work schedules available, paid time off and paid holidays, family leave, and a child care center.
- **Wellness**: Metro provides employees a FREE onsite fitness center, wellness fairs, and agency-wide fitness challenges and events.
- **Employee Perks**: Ride on the Metro system for FREE with a Metro TAP Card, employee discounts, recreational activities, and resources in improve your life.

Metro

# THE ROLE


The **Senior Manager, Information Security** leads the alignment and integration of the organization's information security and risk management programs with Cybersecurity standards and frameworks, focusing on identifying, protecting, detecting, responding, and recovering from cybersecurity threats, while ensuring compliance and promoting a culture of security awareness and resilience across the organization.

## Duties & Responsibilities

- Plans, develops, implements, and manages a strategic enterprise information security and risk management program to ensure the integrity, confidentiality, and availability of information owned, controlled, or processed by the organization.
- Identifies and supports security initiatives and establishes governance programs.
- Plans, develops, and manages data, systems, and network security policies, standards, procedures, processes, and guidelines throughout Metro related to information access, security, privacy, compliance and disaster recovery, inclusive of all media formats.
- Assists appropriate teams in ongoing management, review, audit, and enforcement, including firewall configuration audits, log analysis, and gap remediation.
- Ensures compliance with statutory and regulatory requirements pertaining to information access, security, and privacy for Metro, and its affiliate organizations as requested or necessary.
- Supervises, measures, and monitors potential information security exposures, violations of information security policies and procedures, and breaches of information security measures, and reports all significant discoveries to the Deputy Executive Officer, Enterprise Information Management in a timely fashion.
- Partners with business and IT leaders on risk and control areas, such as regulatory, external audit and risk management processing, including conducting periodic risk assessments.
- Collaborates with the business area management to identify primary risk exposures and ensure the existing security architecture appropriately addresses and mitigates the exposure.
- Advises the IT Leadership Team on risks related to information security and recommends actions in support of the Metro's wider risk management and security program.
- Coordinates with all other IT functional areas to provide guidance and direction for the inclusion of appropriate security and access controls in hardware and software systems, including teams responsible for applications, infrastructure, privacy, architecture, development, deployment, and operations to establish and implement a secure environment.
- Manages contract relationships with third-party security resources, including Qualified Security Assessors, forensic auditors, and providers of security scans.
- Supervises and directs information security staff and manages contract staff as required.
- Performs security audits of custom written applications and make recommendations to improve security with enterprise custom applications.

## Duties & Responsibilities

- Assists in criminal and other investigations of incidents related to information security or privacy as directed by executive management.
- Partners with internal teams (i.e., IT, Legal, Engineering, Talent) and relevant external resources (i.e., Law Enforcement) and ensures that all incident response processes and tools are in place to manage incidents and meet business goals and regulatory requirements.
- Develops and delivers awareness campaigns, metrics, and programs to educate and train Metro employees on information security, privacy issues, and compliance to Metro's information security policies, standards, and procedures.
- Supervises the design, testing, and implementation of computer systems, providing information security guidelines and/or specifications for all operating and applications systems in use at Metro.
- Closely monitors emerging information security threats, assesses the organization's risk exposure, implements mitigating measures, and communicates this information to key stakeholders on a timely basis.
- Leads evaluations and provides recommendations to leadership regarding new technologies related to information security.
- Reviews and interprets new sources of information on current and emerging laws, rules, regulations, and industry practices relating to information technology security.
- Prepares and presents Metro-wide information security and privacy policies and procedures for senior management consideration and adoption.
- Oversees emergency management and participates in the department's information security, disaster recovery, and safety programs.
- Balances information security needs with the organization's strategic business plan, identifies risk factors, and determines solutions.
- Develops an annual work plan; sets and monitors goals and assignments; manages, assesses, and evaluates staff.
- Works in collaboration with IT leadership to develop and execute department mission, vision, and goals.
- Communicates and implements safety rules, policies, and procedures in support of the agency's safety vision and goals; and maintains accountability for the safety performance of all assigned employees.
- Contributes to ensuring that the Equal Employment Opportunity (EEO) policies and programs of Metro are carried out.
- May be required to perform other related job duties.

# ABILITY

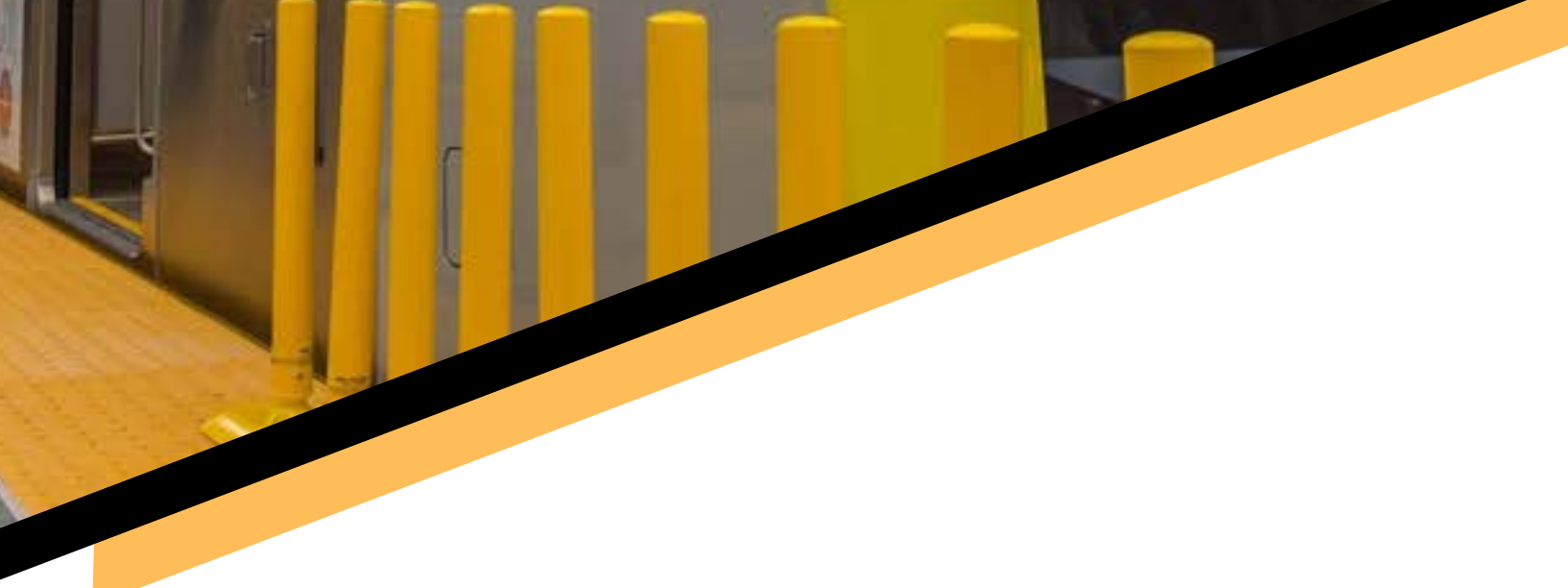
Posses the ***Ability*** to (*defined as a present competence to perform an observable behavior or produce an observable result*):

- Learn an ever-changing field of knowledge.
- Interact effectively with all technical and non-technical groups.
- Promote adoption of change across a range of business and/or IT related initiatives.
- Recognize, analyze, respond quickly, and deal effectively with problems, issues, and incidents.
- Demonstrate strategic and proactive approach to solving problems.
- Perform security risk and compliance assessments in complex and multiple department and technology environments.
- Build teams and create an environment where asking questions or assistance is encouraged.
- Develop long- and short-range plans.
- Work well under pressure of multiple priorities and short deadlines.
- Keep up to date on latest security and privacy legislation, regulations, advisories, alerts, and vulnerabilities pertaining to information security and privacy as it relates to Metro.
- Understand, interpret, and apply laws, rules, regulations, policies, procedures, contracts, and budgets.
- Utilize a wide variety of computers, operating systems, networks, and telecommunications systems.
- Enter and retrieve information using computers.
- Comprehend technical written material.
- Compile, analyze, and interpret complex data.
- Prepare reports and write clearly, concisely, and convincingly.
- Tailor and deliver messages to different audiences, including leadership, peers, customers, and stakeholders.
- Speak clearly, concisely, and effectively.
- Maintain confidentiality.
- Travel to offsite locations.
- Read, write, speak, and understand English.

# KNOWLEDGE

Has ***Knowledge*** of (*defined as a learned body of information that is required for and applied in the performance of job tasks*):

- Theories, principles, and practices of information security, data protection, digital security, data communications technology, application controls, and IT architecture.
- Statutory and regulatory requirements, standards, and ethics pertaining to information access, audit, investigation, security, and privacy, such as PCI, NERC, and HIPAA.
- Information security domains, networks, systems, operating systems, hardware, software applications, databases, internet, intranet, and client server operation.
- Information security tasks, issues, vulnerability, scanning, reporting, and compliance.
- Processing capabilities and functioning of Metro's digital infrastructure, applications, and controls.
- Digital security and data protection products, tools, benchmarks, and techniques.
- Firewall technology, remote access security, and voice, data, and advanced local-area and wide-area networking technologies.
- Encryption technologies, software, and applications.
- Methods of project and process control, budgeting, and cost analysis and prediction.
- Cloud security concepts and tools.
- All phases of disaster recovery.
- Modern management theory.



# SKILLS

Has ***Skills*** in *(defined as the proficient manual, verbal, or mental utilization of data, people, or things)*:

- Planning, organizing, and constructing the design and implementation of a comprehensive information access, security, and privacy programs.
- Performing cryptology and network engineering on multiple software and hardware platforms.
- Determining strategies to achieve goals.
- Developing various IT areas, including application development for multiple operating systems and platforms, account management, etc.
- Developing and managing reporting of security and risk performance metrics and reporting dashboards for security risk register, business, and technical audiences.
- Working in a complex environment with rapidly changing technology needs.
- Reviewing contracts, Statements of Work (SOW), the procurement process, and vendor selection.
- Analyzing situations, identifying problems, recommending solutions, and evaluating outcomes.
- Exercising sound judgment.
- Communicating effectively orally and in writing.
- Interacting professionally and working effectively with Metro employees, customers, vendors, partners, and business managers across various levels of the organization, and outside representatives and the public.
- Exercising leadership.
- Managing, hiring, training, supporting, and motivating assigned staff to utilize the full range of their skills and reach higher levels of performance.
- Managing through direct reporting supervisory personnel.

# MINIMUM QUALIFICATIONS

## *Education*

Bachelor's Degree in Computer Science or a related field; Master's Degree in a related field *preferred*.

## *Experience*

Six years of relevant experience or three years of relevant supervisory-level experience performing information security work in Windows, UNIX, Wide Area Network/ Local-Area Network (WAN/LAN) environment, and in various areas of IT, including development, design, implementation, technical support, programming, database, and operating systems; experience in a highly regulated environment *preferred*.

## *Certifications, Licenses, & Special Requirements*

A valid California Class C Driver License or the ability to utilize an alternative method of transportation when needed to carry out job- related essential functions.
Certification in one or more areas of cyber security specialization Certified. Information Systems Security Professional (CISSP), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), OSCP (Offensive Security Certified Professional), ITIL (Information Technology Infrastructure Library), CISA (Certified Information Systems Auditor), and/or GIAC (Global Information Assurance Certification) certifications, such as GSEC (GIAC Security Essentials Certification) and/ or GCIH (GIAC Certified Incident Handler).
Exposure to various environmental factors when at offsite locations.
On call 24 hours a day for emergencies.

# PREFERRED QUALIFICATIONS

- Experience implementing information security in a complex organizational structure providing strategic planning, operational support, and team leadership.
- Experience operating security technologies and practices, including but not limited to Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM), firewall administration, endpoint protection, and Security Operations Center (SOC) management.
- Experience designing, implementing, and managing security measures to protect systems, networks, and data.
- Experience leading, motivating, and developing a team of information security professionals, fostering a culture of continuous improvement and adaptation to evolving security threats and technological advancements.
- Experience identifying, assessing, and mitigating information security risks, along with the ability to develop and execute comprehensive incident response plans.
- Experience in handling security breaches, conducting investigations, and liaising with law enforcement and other external agencies, as necessary.
- Possession of recognized certifications such as CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), or similar credentials to demonstrate expertise in information security practices and principles.

# APPLY NOW

## Senior Manager, Information Security


This is an opportunity to join one of the nation's largest and most innovative transportation systems. To apply for the **Senior Manager, Information Security** position with Metro, please visit **www.davidgomezpartners.com** or send your resume to Recruiting@DavidGomezPartners.com .

The deadline to apply is ***Monday, April 1, 2024*** to be considered.

** Salary Range For This Position: $109,346 - $136,698 - $164,029*

Metro

Trusted Hiring Partner

GOMEZ PARTNERS