

Deputy Director, Physical and Cyber Security

San Jose, California

Job Description

The Deputy Director, Physical and Cyber Security plays a critical role in safeguarding our public agency's operations and ensuring the safety and security of our facilities, employees, and the public. If you are a dedicated security professional with a passion for public service and a proven track record in security management, we encourage you to apply for this challenging and rewarding position.

The Deputy Director, Physical and Cyber Security will serve as a pivotal leader within our public agency, responsible for the comprehensive management of physical security and cybersecurity operations. This role entails developing and implementing robust security strategies to protect agency assets, ensure public safety, and maintaining the integrity of sensitive information. The Deputy Director will work closely with senior leadership to ensure that security measures are aligned with the agency's mission and regulatory requirements.

Key Responsibilities:

Leadership and Strategy:

- Collaborate with senior agency officials to develop and enforce security policies, protocols, and procedures.
- Provide strategic direction and leadership to the security team, ensuring that security initiatives align with agency goals and compliance standards.
- Develop and implement risk management strategies to identify, assess, and mitigate security threats and vulnerabilities.

Physical Security:

- Oversee the planning, design, and implementation of physical security measures, including access control systems, surveillance, and emergency response protocols.
- Ensure the security and safety of agency facilities, employees, and the public by maintaining and enhancing physical security infrastructure.
- Experience in managing sworn police staff at a management level is desired
- Experience in responding to and leading initiatives to address workplace violence incidents and prevention strategies
- Coordinate with local law enforcement and emergency services to enhance physical security preparedness and response.

Cybersecurity:

- Lead the development and execution of cybersecurity policies and initiatives to protect agency information systems from cyber threats.
- Oversee the implementation of cybersecurity measures, including firewalls, intrusion detection systems, and incident response plans.

- Ensure compliance with federal, state, and local cybersecurity regulations and standards.
- Conduct regular security audits and assessments to identify and address potential vulnerabilities.

Training and Awareness:

- Develop and implement comprehensive security training programs for agency staff to promote security awareness and best practices.
- Conduct regular drills and exercises to ensure staff preparedness for security incidents and emergencies.

Collaboration and Communication:

- Foster strong relationships with internal and external stakeholders, including government agencies, law enforcement, and cybersecurity organizations.
- Serve as the primary point of contact for security related issues and incidents, providing timely and effective communication to senior leadership and relevant stakeholders.
- Budget and Resource Management:
 - Develop and manage the security budget, ensuring the efficient allocation of resources to support security initiatives.
 - Oversee the procurement and maintenance of security equipment and technologies.

Qualifications – Highly Preferred:

- Bachelor's degree in security management, Information Technology, Criminal Justice, or a related field; advanced degree preferred.
- Minimum of 7 - 10 years of experience in physical security and cybersecurity, with at least 3 - 5 years in a leadership or management role.
- Comprehensive knowledge of security principles, practices, and technologies.
- Strong understanding of federal, state, and local security regulations and standards.
- Experience working with Security Contract Agencies, Sheriff's department, Transit Security, Local City Police Departments.
- Experience with public safety advisory committees or community-oriented policing organizations
- Excellent leadership, communication, and interpersonal skills.
- Proven ability to develop and implement effective security strategies and programs.
- Certifications such as CISSP, CISM, CPP, or PSP is highly desired.
- ASIS CPP Certification highly desired.

Personal Attributes:

- High ethical standards and integrity.
- Strong analytical and problem-solving skills.
- Ability to work effectively under pressure and handle multiple priorities.
- Commitment to public service and the mission of the agency.

Definition

Under general direction, the Deputy Director, Physical & Cyber Security plans, organizes, directs and oversees agency-wide security and cyber security programs and initiatives.

Distinguishing Characteristics

This is an At-Will Executive Management position which serves at the discretion of the General Manager. This position has executive oversight accountability for transit security, including physical and cyber security functions, and contracted security and sworn law enforcement personnel. Additionally, this position has overall responsibility for the identification, evaluation, and mitigation of physical and cyber security risks associated with all VTA operations.

About VTA

The Santa Clara Valley Transportation Authority employs more than 2,000 people dedicated to providing solutions that move Silicon Valley. Unique among transportation organizations in the San Francisco Bay Area, VTA is Santa Clara County's authority for transit development and operations (light rail and bus), congestion management, transportation-related funding, highway design and construction, real estate and transit-oriented development, and bicycle and pedestrian planning. With local, state, and federal partners, VTA works to innovate the way Silicon Valley moves and provide mobility solutions for all. Santa Clara Valley Transportation Authority (VTA) is an independent special district that provides sustainable, accessible, community-focused, innovative, and environmentally responsible transportation options promoting the region's vitality. VTA provides bus, light rail, and paratransit services and participates as a funding partner in regional rail services, including Caltrain, Capital Corridor, and the Altamont Corridor Express.

To learn more, go to: vta.org.

Our Community:

Santa Clara County, sometimes referred to as "Silicon Valley", is unique for its innovation, natural attractions, and social diversity. With numerous amenities and perfect weather, it has long been considered one of the best places in the United States to live and work. calendar of festivals and celebrations supports the community spirit. Nearby open space provides easy access to mountain parks, trails, lakes, streams, and beautiful coastal beaches. San José has received accolades for its vibrant neighborhoods, healthy lifestyle, and diverse attractions from national media, including Business Week and Money magazines.

The county's population of 1.9 million is the largest in Northern California and is rich in ethnic culture and diversity. Enjoy access and the option to explore our closely neighboring counties of San Francisco and Alameda.

Classification Bargaining Unit: Non-Rep

Application Deadline: *Please be aware that this position will close promptly on Tuesday, July 23, 2024, at 11:59 pm. We encourage interested applicants to apply early to ensure consideration.*

Essential Job Functions:

Typical Tasks

- Plans, manages, organizes, and directs activities of assigned physical and cyber security staff, contracts, and programs.
- Selects, supervises, trains, motivates, assigns, evaluates, counsels, and disciplines staff.
- Develops and oversees strategies, goals, policies, standards, procedures, staffing, compliance, and daily operations for the Protective Services Department.
- Serves as the Cyber & Physical Security Executive Coordinator, facilitates liaising with regulatory agencies, Cybersecurity and Infrastructure Security Agency (CISA), Transportation Security Administration (TSA), Federal Transit Administration (FTA), Department of Homeland Security (DHS), Federal Aviation Administration (FAA) and Federal Emergency Management Agency (FEMA), contract law enforcement and contract security.
- Oversees agency security compliance and identifies opportunities for improvements and/or efficiencies; develops and implements change initiatives.
- Oversees the AB1735 (VTA transit prohibition orders) program.
- Oversees the SB553 (Workplace Violence Protection) programs.
- Manages VTA's Security Certification program for all capital initiatives and implements VTA's agency-wide Security Design Criteria and CPTED implementation.
- Serves as program manager of VTA's Sensitive Security Information (SSI) function and the agency archivist for SSI material.
- Oversees security and law enforcement audits and directs the implementation of corrective actions.
- Partners and collaborates with bargaining group partners to improve VTA's relationship with the bargaining and community for security awareness.
- Manages the VTA Chief Information Security Officer (CISO), Cyber Managed Services and Cyber Security Network Operations Center
- Oversees the design and implementation of VTA's cyber security infrastructure including the development of custom commercial off-the-shelf (COTS) software systems.
- Oversees cyber security requirements, including the application structure design ensuring compatibility with existing internal systems and industry standards.
- Develops and implements VTA's Cyber Security Risk Management program to ensure appropriate levels of confidentiality, availability, and integrity.
- Interacts with appropriate parties to ensure safe and secure connectivity of internal VTA domains (IT, SCADA, CCTV, and IoT Access Control);
- Directs security crisis management, investigates root causes, and implements appropriate solutions.
- Oversees vulnerability audits, penetration tests, and IT investigations.
- Works with law enforcement and other advisory bodies, as necessary, to ensure the organization maintains a strong cyber security posture.
- Monitors the external threat environment for emerging threats; advises relevant stakeholders on appropriate courses of action.
- Provides advice and counsel to the General Manager, Board of Directors, and other officials, executives, managers, and employee organizations regarding security issues.
- Provides periodic updates on system security programs, initiatives, and conditions.
- Ensures continuation of grant funding for critical security and law enforcement programs.
- Develops and controls assigned budget.

- Ensures compliance with VTA policies and procedures regarding equal employment opportunity and discrimination and harassment prevention.
- Leads, attends, and/or participates in various professional groups, boards, and committees and stays abreast of new trends and innovations in assigned functional areas.
- Serves as a member of the management team in meetings with collective bargaining groups.
- Performs related duties as required.

Minimum Qualifications

Employment Standards

Sufficient education and increasingly responsible experience to demonstrate possession of the required knowledge, skills, and abilities.

Development of the required knowledge, skills, and abilities is typically obtained through a combination of training and experience equivalent to graduation from an accredited college or university with a four-year degree in criminal justice or a related field and extensive, increasingly responsible experience developing and managing security programs for a public or private sector organization, including experience in physical security, cyber security, and demonstrated managerial experience.

Possession of a valid California driver's license is required.

Possession of active Transit Safety and Security Program (TSSP) certification, Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certification is required.

A certification in ASIS Certified Protection Professional (CPPC) is preferred.

Supplemental Information

Knowledge Of:

- Regulations governing transportation security and reporting procedures.
- Principles and practices of physical security, crime prevention through environmental design (CPTED), critical infrastructure protection, homeland security strategy, and emergency management.
- Principles and practices of security methods, blueprint developments, and access control technology.
- Principles and practices of threat and vulnerability assessment methodologies and hazard analyses.
- Closed-circuit television technologies, including security intrusion systems and access control technology.
- Principles and practices of security technologies related to video surveillance, video analytics, facial recognition, weapons, and explosives screening.
- State and federal laws and policies governing security and reporting procedures.
- Principles and practices of budgetary planning, preparation, administration, and control.

- Principles and practices of administration, organization, management analysis, supervision, fiscal management, and program development.
- Principles, practices, and procedures pertaining to the operation of a large and complex multi-modal transportation system.
- Identification, evaluation, and mitigation of public and industrial security risks in a transportation environment.

Ability To:

- Select, supervise, train, evaluate, motivate, counsel, and discipline subordinate staff.
- Effectively plan, organize, implement, and evaluate physical and cyber security measures.
- Analyze data pertaining to division functions, interpret management information, maintain records and reports, and develop short- and long-range budget plans.
- Define problem areas, evaluate, recommend, and implement solutions to complex issues and problems.
- Effectively manage the AB1735 and SB553 plans.
- Analyze situations, identify problems, recommend solutions, and evaluate outcomes.
- Interpret and apply applicable federal, state, and local policies, laws, and regulations.
- Monitor developments and legislation related to assigned area of responsibility; evaluate impact on VTA's operations and recommend and implement policy and procedure improvements.
- Actively lead or participate in various professional groups, boards, and committees; effectively advocate for VTA's interests.
- Coordinate with executives in other divisions in the preparation and submittal of reports and other documents to regulatory agencies and other audiences.
- Communicate clearly and effectively, both orally and in writing.
- Effectively represent VTA in dealings with government agencies and other entities.
- Establish and maintain effective working relationships with those contacted in the course of work.

What's in it for You?

Work/Life Balance: 40-hour work weeks, and a option of a flexible/hybrid remote schedule.

Health: VTA participates in a CalPERS-sponsored medical plan with VTA contribution to employee and dependent premium health insurance premiums. Employees pay a monthly contribution of any amount in excess of the Kaiser Bay Area Family rate.

Flex Spending Account: \$300 employer-funded Health FSA for eligible employees

Vision: VSP full premium for employees and eligible dependents

Dental: Delta Dental full premium for employees and eligible dependents

Leave: 17 days of vacation (accrued), 80 Hours of sick time (accrued), 12 paid holidays per year, and 1 floating holiday per year.

Retirement:

- Participation in CalPERS
 - Classic Members: 2% @55
 - PEPRAs Members: 2% @62
 - 457 Deferred Compensation Plan (voluntary)
- 457 pre-tax

- 457 Roth
- Self-directed brokerage account option for qualifying employees
 - Retiree medical coverage for eligible employees with VTA contributions to the retiree's medical premium

Additional perks:

- All active full-time employees and their eligible dependents are eligible for transit passes for use over VTA lines, including VTA Paratransit services.
- Employee Assistance Program (EAP) is available to each employee, eligible dependent, and household member, 24 hours a day, seven days a week.
- Tuition Reimbursement
- Professional Development Fund
- Wellness Programs

As we continue to implement our [VTA Forward Plan](#), we aim to strengthen and increase our workforce to take on future opportunities and challenges by elevating our people and our services.

For more information about our VTA Forward Plan, visit: <https://www.vta.org/VTAForward>

General Instructions

Please read this entire job announcement before applying for the position. Print and keep a copy of this announcement so that you can refer to it. Questions not answered within this job announcement may be sent to personnel@vta.org.

To ensure consideration, completed applications must be submitted online to the Human Resources department by the stated closing time and date posted. When the stated closing date is "continuous," apply immediately; the position may close without notice. You will receive an immediate email confirming receipt of your submitted application. If you do not receive this email, contact NEOGOV's Applicant Assistance Line at (855) 524-5627 between 8:00AM to 5:00PM (PST) Monday through Friday, excluding holidays.

Only on-line applications will be accepted for this recruitment (paper applications or resumes will not be accepted). Job Interest Notification Cards, or copies of previous, partial, or un-submitted applications, are not an acceptable substitute to a completed application.

ALL APPLICATION AND TESTING NOTIFICATIONS WILL BE SENT BY E-MAIL.

Applicants should select e-mail as the preferred method of notification. Candidates must maintain an up-to-date, valid and reliable e-mail address. Candidates are also responsible for maintaining up-to-date phone numbers and addresses on their on-line account. Due to the number of applications received, candidates must check their application status through their on-line account. Contact NeoGov for assistance if needed.

Information on how to apply for jobs at the VTA is available on the VTA Employment website and from the NEOGOV's Applicant Assistance Line (855) 524-5627. NeoGov Applicant support is available from 8:00AM to 5:00PM (PST) Monday through Friday, excluding holidays.

Americans with Disabilities Act Accommodations

The Human Resources Department will make reasonable efforts in the recruitment/examination process to accommodate applicants with disabilities. If you wish to request an accommodation, call the Human Resources Department at (408) 321-5575 or email at Personnel@vta.org.

Application Processing Information

All related current and past work experience (including VTA experience) must be listed and fully described in the Work Experience section of the application ("See Resume" is not acceptable). Incomplete or improperly completed online applications may be rejected even if you are qualified for the position for which you are applying. It is your responsibility to ensure that the online application reflects the work experience and education needed to meet the requirements for the position you are applying for. Although your resume may have all your experience and education details, please make sure to complete each section of the online application to ensure that your information is accurately captured during our screening process.

All applications are subject to review as to meeting minimum qualifications at any point in the recruitment process. Passing any step is no guarantee of continuation if it is determined that the applicant does not meet the minimum qualifications as stated in the class specification.

Candidates found to have exaggerated/falsified their qualifications, experience, training, and/or education may be disqualified at any point in the recruitment process and may be denied future employment with the VTA.

If selected for the position, candidates will be required to complete a criminal conviction disclosure form. Candidates who successfully become VTA employees and fail to disclose any of the criminal background information as required may be subject to discipline up to and including discharge.

Eligible Lists typically remain in effect for six (6) months. However, Human Resources may abolish Eligible Lists at any time during the six (6) month period. Human Resources may extend eligible Lists for up to two (2) years. Eligible Lists may be used for more than one recruitment. If you have questions related to an Eligible List you might be on or were on, you should contact Human Resources.

If you have questions regarding your status as an applicant for this position, please call the Human Resources Department at (408) 321-5575 or email at Personnel@vta.org.

VTA is committed to providing reasonable accommodations to applicants and employees with disabilities or religious needs, absent undue hardship.

VTA is an equal employment opportunity employer. VTA does not and will not tolerate discrimination against applicants or employees on the basis of age, ancestry, color, marital status, mental or physical disability, genetic information, national, origin, immigration status, political affiliation, race, religion, creed, sex, gender identity, gender expression, sexual orientation, pregnancy, medical condition, disabled veteran or veteran status, etc.

Apply at: [Deputy Director, Physical and Cyber Security | Apply tab | Career Pages \(governmentjobs.com\)](#)