POSITION: **INFORMATION SYSTEMS SECURITY ENGINEER**
Position located at the Golden Gate Bridge
San Francisco, CA

SALARY RANGE: **$107,744.00 - $130,228.80 annually, plus excellent benefits**
40.00 hour work week
Employee pays up to 7% of salary/wage toward CalPERS retirement plan

DATE POSTED: **Monday, August 1, 2016**

CLOSING DATE: **Open Until Filled**

OPEN TO: **All Qualified Applicants**

OPENINGS: **One (1) Vacancy and to Create an Eligibility List**

POSITION DESCRIPTION:
Under general direction of the Chief Technology Director, performs the highest level of professional information technology duties related to administration of the District's information security program; assumes responsibility for developing, directing and ensuring the security of the Districts' most complex and strategic operations including VoIP, networked and database systems; performs comprehensive and complex programmatic design, analysis and development duties within the Information Systems Department.

Incumbent will perform work of a professional nature, utilizing skills that require an understanding of the most complex analytical procedures and processes in the District while working with a very high level of independent authority and judgment. Position also assumes responsibility for directing and coordinating various operational and technical security-related activities that impact the District's most complex and strategic systems, network and database operations.

EDUCATION/EXPERIENCE REQUIREMENTS:
College level training and experience equivalent to:

- Bachelor's degree in Computer Science, Information Systems, Software Engineering, Computer Engineering or other related technology major. Applicants who do not possess a degree should attach a statement supporting qualifying experience.
- A minimum of four years industry/ IT experience and two years of project management experience leading large scale enterprise projects that requires fundamental change in business practice and automation to deliver significant value to business. One year of which must have been administering an IT-related security and/or privacy program on a full time basis.
- **PMI Certification is highly desirable.** Applicants who do not possess a certification should attach a statement supporting recent qualifying experience.

ESSENTIAL RESPONSIBILITIES:

- Assumes responsibility for developing, directing, establishing and maintaining the District's information security program and ensuring the security of the District's most complex and strategic operations related to mainframe/server, networked and database systems.
- Develops, coordinates, establishes and maintains policies to provide guidance to District departments and staff regarding Local Area Network (LAN), Wide Area Network (WAN), mainframe, server and desktop security issues; researches and recommends centralized written manuals and procedures regarding security controls.
- Plans, organizes and coordinates committees, task forces and meetings to identify, resolve and administer security-related issues and activities; assists District departments with disaster recovery planning and testing.
- Researches, identifies and analyzes existing and potential security threats that could harm or destroy District information assets; interacts and communicates with other government agencies and external organizations to stay aware of security issues; as appropriate, issues District wide virus and threat warnings as well as information regarding the identification, avoidance and mitigation of such threats.
- Leads and directs complex projects designed to provide for the protection of District information assets; recommends solutions and appropriate technology to meet District needs; designs project and resource plans and schedules; develops proposals using cost/benefit analyses; evaluates proposed system hardware and software to ensure compatibility with existing systems; coordinates with vendors and contractors; writes and evaluates proposals; negotiates contracts for security-related equipment and services; oversees the installation and evaluation of software and hardware; controls and reports budget expenditures; directs members of the project team; provides written reports and presentations on project status.
- Performs District wide information security audits to identify weaknesses that could be used to gain access to confidential District information.
- Serves as the central point of contact for the District regarding information technology-related incidents or violations; assists department information technology staff and others (e.g., law enforcement, auditors) in investigating security violations; performs formal investigations of District employees for misuse of District assets; collects evidence using forensics techniques and specialized software; communicates with department heads, District Counsel, Labor Relations, Human Resources and others regarding sensitive and confidential situations; reports violations to law enforcement agents as required.
- Serves as technical resource to District staff regarding information security matters; provides training to new employees through the District's new employee orientation program, as well as special departmental training sessions.
- Creates, implements, maintains and tests emergency and disaster recovery measures that ensure continual operational readiness of high-profile District systems.
- Attends and participates in professional group meetings; stays abreast of new trends and innovations in the field of information technology in general and information security in particular.
- Other duties as assigned

REQUIRED KNOWLEDGE, ABILITIES, and SKILLS:

- Ongoing identification of needs, design upgrades and implementation of new technology
- Hardware, software and networking protocols utilized in LAN, WAN and related data communication systems, including fiber optics and peripheral equipment.
- Thorough knowledge of Microsoft Operating Systems up to and including Windows Server 2012R2 and Windows 7 Enterprise

REQUIRED KNOWLEDGE, ABILITIES, and SKILLS (Continued):

- Knowledge of Cisco UCS compute
- Thorough knowledge of LAN switch and router management via telnet and web interfaces
- Knowledge of router protocols and setup thereof
- Thorough knowledge of TCP/IP communication
- Knowledge of VLAN and 802.1x technology
- Experience with Cisco IOS software and ISE
- Experience with firewalls and VPN servers
- Experience with syslogs, syslog servers, and SEIM
- The use and care of tools and equipment related to the installation, troubleshooting, maintenance and upgrading of a variety of voice/data networks and communication hardware and software
- Ability to prioritize competing requests for service
- Ability to prioritize multiple tasks and organize schedules to meet District requirements
- Ability to explain technical information to non-technical users
- Record keeping practices and procedures
- Demonstrated ability to prepare clear, concise reports, documentation and correspondence.
- Maintains current knowledge of the field including learning new and existing software, applications, databases and hardware through formal, informal and on the job training and self study
- Ability to communicate professionally and effectively, both orally and in writing
- Ability to work professionally and productively with all encountered in the course of work, including personnel in governmental agencies, local authorities, consultants, the general public, and District staff
- Knows and follows the safety and health rules and safe working practices applicable to the position

SPECIALTY REQUIREMENTS:

Specialized examinations may include one or more of the following:

- ***Application Security management (ASM):*** Experience in application development using standard IT systems development methodology and techniques for resolving business problems. Includes systems design, database management, development of online data entry and data inquiry capabilities, and defining techniques; communications, network analysis, design, planning and performance tuning.

- ***Identity and Access Management (IAM):*** Experience assisting with defining, testing, and implementing IT user provisioning and identity management technologies. Includes developing IAM policies, standards, and procedures; identifying appropriate access control techniques; analyzing and selecting IAM solutions; and familiarity with security and System Development Life Cycles (SDLC) processes.

- ***Incident Response Management (IRM):*** Experience in an IT organization providing technical assistance in computer incident response for potential or actual information-security breaches or attacks. Includes detecting, analyzing, responding to, and reporting information security incidents; and familiarity with the chain-of-custody process.

- ***Network Security Management (NSM):*** Experience in IT network planning, design, and analysis. Includes assisting in implementing security tools and controls such as intrusion detection/prevention systems, sniffers, and firewalls.

- ***Physical / Environmental Security (PES):*** Experience assisting with managing physical and environmental IT security methodologies to prohibit unauthorized physical access and prevent damage to IT resources. Includes physical and environmental security planning, design, and analysis.

- ***Policy and Compliance Management (PCM):*** Experience assisting with developing and implementing IT security policies and standards. Includes assisting in monitoring for compliance.

- ***Risk Assessment Management (RAM):*** Experience performing IT security risk assessments. Includes assisting in developing and implementing business continuity and disaster recovery plans and in developing risk assessment reports of findings and recommendations for remediation.

- ***Security Awareness Training (SAT):*** Experience assisting in developing, implementing, and evaluating IT security awareness training programs and related materials. Includes assisting in reporting of training compliance.

- ***Server Security Management (SSM):*** Experience in IT server, e.g. e-mail, web, application, and database, security management comprised of implementing upgrades, patches, and updates to operating systems, software applications, and security protection software. Includes configuring server environment to protect the integrity of the system, for example by limiting user rights, disabling unnecessary services, and establishing group policies where applicable.

- ***Workstation Security Management (WSM):*** Experience managing the security of workstation, e.g. desktops, laptops and tablets, and portable devices, e.g. thumb drives and personal digital assistants. Includes implementing upgrades, patches, and updates to operating systems, software applications, and security protection software; establishing group policies and user rights; and disabling unnecessary services where applicable.

REQUIRED LICENSE:

- Must possess and maintain a current, valid California driver's license and satisfactory driving record
  - No DUIs and reckless driving infractions within the last 7 years
  - No more than 2 moving violations within the last 3 years
  - Operates District vehicles on a regular basis

APPLICATION PROCEDURE:

FAILURE TO MEET ANY OF THE REQUIREMENTS STATED MAY RESULT IN REJECTION OF YOUR APPLICATION

TO APPLY: www.goldengate.org/jobs

Applicants must apply online by the deadline date. Applications received after the deadline will not be considered.

The District's Human Resources Kiosk is available for filling out and submitting your online application and employment documents. The HR kiosk is located at the San Rafael Office. For directions and general information, visit our website www.goldengate.org.

THE FOLLOWING DOCUMENT(S) MUST BE SUBMITTED AT TIME OF APPLICATION:

DOCUMENTS
1. GGBHT Online Employment Application
2. Cover Letter *(Scan and attach as PDF to your online application)*
3. Resume *(Scan and attach as PDF to your online application)*
4. Written statement supporting additional experience must be submitted with the application. *(Scan and attach as PDF to your online application)*

THE SELECTION PROCESS FOR THIS POSITION may include:

- Assessment of education, training, and experience
- Oral Panel Interview
- Department interview for final candidates
- Background, Employment and Security Investigation

** The District will invite only those candidates whose qualifications **MOST CLOSELY MATCH** the position requirements to continue in the selection process.*

AN EQUAL OPPORTUNITY EMPLOYER

It is the policy of the Golden Gate Bridge Highway and Transportation District to take all personnel actions on the basis of merit and other job-related factors, without regard to race, color, national origin, religion, sex (including pregnancy, childbirth, and related medical conditions), disability: physical or mental, age (40 and older), genetic information, marital status, sexual orientation and identity, medical condition, political affiliation or military status.

Applicants with Disabilities: The Human Resources Department will make reasonable efforts to accommodate applicants with disabilities to complete the Employment Application and in any job-related examination process. If you have special needs, please call (415) 257-4521 (Human Resources). The District's telecommunications device (TDD) for Persons with Hearing Disabilities is (415) 257-4554.

Revised 03/17/2014 SS

Revised 07/27/2016 AD

HR Administration
Human Resources Department
1011 Andersen Drive
San Rafael, CA 94901-5318