September 1, 2011 U1117

The City of San Diego is currently accepting resumes for the unclassified position of

INFORMATION SECURITY, COMPLIANCE, & RISK PROFESSIONAL

Salary Range: Dependent on qualifications and experience

Recruitment: Open to all Qualified Candidates

Filing Deadline: Open Until Filled

The City

With more than 1.3 million people, the City of San Diego is the eighth largest city in the United States and the second largest in California. The City of San Diego's strong economy, diverse population, great educational institutions, unsurpassed quality of life, and world-renowned location make it the ideal place to work, live, and play. With its great weather, miles of sandy beaches and major attractions, San Diego is known worldwide as "America's Finest City."

As one of the region's largest employers, the City of San Diego has a combined Fiscal Year 2011 operating budget of $2.76 billion and employs approximately 10,000 highly dedicated employees. Additional information about the City of San Diego can be obtained on the City's website at www.sandiego.gov.

The Department

The Department of Information Technology, reporting under the Chief Financial Officer, is responsible for City-wide oversight of the City's annual IT budget of approximately $90 million, including management of contracts for outsourced IT services (data center, help desk and desktop support, data and voice networks, and application development and maintenance services); providing enterprise-wide IT strategic direction; creating and implementing IT standards, operational policies, and procedures; coordinating major City-wide IT initiatives; and managing the City's public and internal web sites.

The Position

The **Information Security, Compliance, & Risk Professional** reports to the Information Security, Compliance, & Risk Officer. In general, this position is responsible for assisting with the development and implementation of information security strategies; monitoring and enforcement of the City's information security policies, standards, procedures, and internal controls; coordination and management of a security awareness program, business continuity and disaster recovery plans; overseeing, evaluating, and supporting information compliance issues, which may include managing and monitoring security standards or internal controls compliance, leading or conducting internal investigations, security and risk assessments, and helping

employees understand and comply with applicable information security regulations, policies, and procedures; and may also include providing guidance and autonomous evaluations of the City's information security compliance to management. This position will help manage contractual external information security services provided to the City.

The position will work with other professional Information Security staff who conduct electronic discovery (eDiscovery) related to California Public Records Act (CPRA) requests, litigation or internal investigations, and who administer various security systems and oversee security compliance of IT service providers. This position works with local, regional, state, and federal agencies on a regular basis, including the Law Enforcement Coordination Center (LECC, aka Fusion Center), Regional Terrorism Threat Assessment Center (RTTAC), Computer And Technology Crime High-tech (CATCH) Response Team, California Office of Information Security, San Diego field office of the FBI, and representatives from the federal Department of Homeland Security (DHS) on issues related to cybersecurity and protection of local government critical infrastructure. This position may actively participate in the San Diego Chapter of the FBI-sponsored InfraGard Members Alliance (InfraGard), a public-private partnership dedicated to Critical Infrastructure Protection, especially related to cybersecurity. In addition, this position may be expected to act as a representative of the City of San Diego, working in conjunction with Police Department representatives, in the Securing Our eCity (SOeC) regional public-private partnership dedicated to increasing and enhancing cybersecurity awareness and education for employees, local businesses, citizens, schools, and community groups.

Primary Qualifications:

The ideal candidate will possess the following minimum qualifications:

- Comprehensive working knowledge and experience in information security technologies, tactics, products, and industry best practices;
- Current working knowledge of and experience in general information technology systems and IT industry trends;
- Demonstrated knowledge of and experience in information systems risk and compliance management for ensuring the safety, integrity, and availability of protected data;
- Self-motivated and capable of making and implementing decisions which may have a significant impact on the security and integrity of the organization's data;
- Superior planning and organizational skills to develop and implement information security, risk, and compliance strategies, policies and procedures;
- Demonstrated business and political acumen to work effectively with the public, other agencies, businesses, and elected officials;
- Ability to balance between competing priorities with externally imposed deadlines;
- Strong interpersonal and leadership skills, with the demonstrated ability to successfully interact with a wide variety of stakeholders (e.g., subordinates, co-workers/peers, managers, and executives) and work cooperatively toward commonly supported solutions;
- Excellent written and verbal communications skills;
- A commitment to public service, fiscal responsibility, and innovation in government; and
- Extensive knowledge of and experience with user authentication mechanisms, TCP/IP protocols and standards, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Data Loss Prevention (DLP) systems, and other security tools.

Any combination of education and experience that demonstrates these qualifications may be qualifying. Possession of a Bachelor's Degree in information systems/technology, computer science, information security, business administration, public administration or a related field **and** a minimum of three (3) years of professional level experience in information technology, information security, information systems administration or operations is required. Experience in working with complex systems and projects, requiring motivation and interaction with a wide variety of team/group members, is required. At least three years of public sector experience is highly desirable. Information security certification, such as CISSP, CISSP-M, CISP or CISM is highly desirable. A Master's Degree or advanced education in information technology or information security is desirable. Knowledge, education, or experience in physical security measures and tactics is desirable.

Because this position will have regular access to confidential and potentially "law enforcement sensitive" (unclassified) information as part of the duties, the positions require completion of a thorough, pre-employment police background investigation (see below).

Management Benefits:

The successful candidate will be eligible for participation in the City's Flexible Benefits Plan that offers several optional benefit plans or a taxable cash option; $50,000 in City-paid life insurance; paid annual leave accruing at 22 days per year for the 1st through the 15th year of service; defined benefit City retirement with CalPERS reciprocity for those with eligible service; and a mandatory 1% contribution to the 401(a) plan and .25% contribution to a retiree medical trust with a City match to each; and optional deferred compensation (457) and 401(k) programs.

Retirement benefits for current City employees may differ from this Unclassified position. For further information, contact Risk Management at (619) 236-6600. The benefits currently offered to employees may be subject to future modifications.

Selection Process:

To be considered for this position, please submit the following: your current resume, a letter of interest highlighting your relevant work experience and a list of three work-related references – sending via Email to the Human Resources Department at HumanResources@sandiego.gov, or two copies of the requested materials when using City inter-office mail to MS 56 in an envelope marked ***"CONFIDENTIAL: Unclassified Recruitment* – Information Security, Compliance, & Risk Professional"** or sending by US Mail to:

City of San Diego
Human Resources Department
1200 Third Avenue, Suite 1316
San Diego, CA 92101

Following the closing date, resumes will be screened according to the qualifications outlined above. The most qualified candidates will be invited to a screening interview. Finalist interviews will be held with a City of San Diego selection committee.

Prior to a final selection, **qualified finalist candidates for this position must successfully complete a thorough police background investigation, which includes a polygraph examination. Failure of the background investigation will disqualify a candidate from being hired for this position.** The background investigation package must be picked up from the Police Department, Background Investigations Unit, 1401 Broadway, San Diego, CA 92101. The package must be filled out completely and accurately, and submitted in person at the Police Background Investigations Unit, and the candidate must bring a valid California Identification (e.g., Driver's License), as well as other documents required by the Police Department as part of the background package.

If you have any questions, please contact the City's Human Resources Department at (619) 236-6313.

The City of San Diego has an active Equal Opportunity/ADA Program for employment and vigorously supports diversity in the workplace.

SCOTT CHADWICK
Human Resources Director

Rev. 2/JC/Sept. 16, 2011/2270