SFO

San Francisco International Airport

is accepting applications for the position of

Chief Information Security Officer

Recruitment Services Provided by Ralph Andersen & Associates

Cyber Security Career Opportunity of a Lifetime!

This is truly a rare opportunity to join an award winning and progressive organization. This position focuses on cyber security, information technology, and telecommunications in an extraordinary organization serving the traveling public to all corners of the world. This career capstone awaits interest from only the best-of-the-best professionals in the field of cyber security on a national or global basis. We invite you to present your qualifications and career history for consideration.

San Francisco International Airport

SFO is a world-class, award-winning airport that served more than 57 million guests in fiscal year 17/18. SFO offers non-stop flights to 50 international cities on 44 international carriers. The Bay Area's largest airport also connects non-stop with 85 U.S. cities on 12 domestic airlines. The Airport, an enterprise department of the City & County of San Francisco, accounted for $8.4 billion in business activity and supported nearly 43,000 direct jobs.

SFO's mission is to provide an exceptional airport in service to our communities and is committed to redefining air travel. SFO is renovating Terminal 1: The Harvey B. Milk Terminal, the largest capital project in the Airport's $7.3 billion Ascent Program. For more information, visit www.flysfo.com. View a Youtube video about careers at SFO.

SFO is governed by the Airport Commission, a five-person body appointed to four-year renewable terms by the Mayor of San Francisco. The Commission appoints the Airport Director. SFO operates under the rules, regulations, and authority of the Federal Aviation Administration (FAA), a branch of the Federal Department of Transportation. The Airport maintains full compliance with these regulations as well as those of the Transportation Security Administration (TSA) and the Federal Aviation Administration. The Airport, as part of the San Francisco City and County government, is subject to all relevant provisions of the Charter of the City and County of San Francisco and other related codes and ordinances.

Originally part of the San Francisco Public Utilities Commission, the Airport Commission was established by City Charter in 1970. In accordance with the Charter, the Airport Commission is primarily a policy-making body, establishing the policies by which the Airport operates. The Commission is prohibited by Charter from involving itself in the day-to-day operation of the Airport. This executive level oversight is vested in the Airport Director, Ivar C. Satero.

The Position

The Chief Information Security Officer (CISO) is a position of vital importance to the overall cyber security and safety of the Airport. This position reports to the Airport's Chief Information Officer (CIO). This position requires significant interactions with other top managers and supporting staff in leadership positions throughout the Airport and the wider technology community.

The role of the CISO is to further strengthen and aid in the development of an enterprise information security program to protect the integrity, availability, and confidentiality of information communications technology (ICT), industrial control systems (ICS), and electronic data resources in accordance with accepted industry practices and stakeholders' tolerance for risk.

To safeguard these information assets properly, the CISO will be responsible for supporting each of the Airports eight divisions, identify and implement security policies, standards, guidelines, processes, procedures, and operational practices while ensuring its goals and objectives are properly aligned with their respective mission, goals, and objectives.

Key responsibilities of this position are to:

- Develop, in conjunction with a wide-range of Airport stakeholders, an effective and implementable Airport cyber security strategy;
- Demonstrate a keen understanding of the organization culture as well as the overall business needs relative to the Airport, airlines and tenants for cyber security;
- Manage, coordinate, and develop an effective team that will provide a comprehensive tracking system of issues, resolution, response and implementation of information security policies, standards, guidelines, processes, procedures, and operational practices efforts across the Airport;

- Monitor the Airport's ability to manage its information resources in a manner consistent with existing cyber-related policies and procedures;
- Coordinate and be the liaison with local and federal law enforcement representatives with respect to cyber-based criminal, counter-espionage, and counter-terrorism concerns that have the potential to adversely impact Airport security and operations;
- Assess the effectiveness of existing processes, procedures, controls, and safeguards to prevent cyber-security breaches across SFO's infrastructure;
- Assess the Airport's ability to identify and remediate exploitable cyber-related vulnerabilities present within the SFO's expansive and diverse infrastructure including the ability to detect and repulse emerging cyber-attacks as they occur;
- Assess the Airport's ability to respond and mitigate follow-up on attacks as attackers spread inside a compromised network;
- Assess the Airport's ability to respond to cyber-related issues in accordance with digital forensic and incident response guidelines established by US-CERT and the U.S. Department of Justice;
- Identify and manage cyber-security threats and incidents as directed by the Chief Information Officer (CIO);
- Identify techniques to promote secure communications and the appropriate protection of information across all Airport divisions as well as promoting a common and consistent information security program framework;
- Provide technical and budgetary oversight with respect to the cyber-security needs of SFO;
- Oversee the design, implementation, and monitoring of technical controls related to information security across all Airport divisions as directed by the CIO;
- Oversee the design, implementation, and monitoring of all remote-access mechanisms associated with Airport information assets; identify and remediate threats and vulnerabilities to these assets;
- Coordinate and serve as the liaison with Airport subcontractors on matters related to Airport cyber-security issues and concerns;
- Attend SFO management meetings and maintain cooperative relations with other City and Airport Units, vendors, contractors, and the general public;
- Maintain skills and expertise appropriate to the field of enterprise software engineering, applied cryptography, digital forensics, and information security;
- Maintain necessary Airport compliance certifications, such as PCI;
- Provide strategic direction and oversight within the field of information security and forensics as directed by the Chief Information Officer (CIO); and
- Investigate potential misuses of information resources as directed by the CIO.

Core Values

Safety and Security is our first priority
We are one team
We treat everyone with respect
We communicate fully and help one another
We strive to be the best
We are innovative
We are open to new ideas
We are committed to SFO being a great place to work for all employees
We are each responsible for the Airport's success
We take pride in SFO and in our accomplishments

The Ideal Candidate

The ideal candidate will have recent director level cyber security management experience underpinned by a broader technology background with emphasis on telecommunication networks. This top caliber individual will have a demonstrable background in working with business stakeholder groups to develop and deliver an organization-wide cyber security agenda. Additionally, this telecommunication expert will have a proven track record of assessing organizational cyber security threats and vulnerabilities at an organizational level and delivering specific remediation actions and initiatives. Importantly, this highly qualified individual will have also successfully coordinated an immediate response to specific cyber security threats.

This ideal candidate will also have a unique blend of people skills and an uncanny ability to move swiftly to resolution in a fast-paced and complex environment. This skilled individual will have the ability to work well with other technology staff to discern desired functionality and requirements, and fashion innovative technological and procedural solutions while at the same time preserving the highest level of security available.

Personal qualities desired in this ideal candidate for CISO include being a strategic thinker and strong communicator, with the ability to deal effectively with local partners and high-level federal regulatory agencies to quickly assess, mitigate, and resolve potential security breaches.

Additionally, top candidates for consideration will:

- Eagerly embrace the Airport's Core Values;
- Be a highly ethical and forthright individual able to demonstrate integrity and professionalism in all aspects of work;
- Be politically astute and skilled in what and how to convey the situation and the message effectively;
- Have the confidence to assertively and quickly solicit and marshal resources from others; and
- Have the ability to listen, articulate, and act with sound judgment on behalf of the organization and the public.

A copy of the Airport's Core Values can be obtained on Ralph Andersen & Associates' website.

Qualifications

Minimum qualifications required at time of submittal:

Experience: Six (6) years of recent and verifiable experience as a Cyber Security Specialist that includes three (3) years of experience in the leadership of cyber security operations and initiatives; and three (3) years of experience in a cyber security management role.

The ideal candidate would have recent director level experience in dealing with telecommunications infrastructures such as telephony, wireless, fiber optics, Sonet, and ATM systems for converged video, voice and data networks, and/or director level experience in project engineering, fault isolation on complex networks, and systems design in voice, data, and wireless networks.

Education: Bachelor's degree in information technology, telecommunications, management information systems, computer science, computer engineering, business administration, public administration, or a closely related field.

Highly desirable certifications, although not required, may include the following (or a recognized professionally accepted equivalent):

- Certification, International System Security Certification Consortium (ISC2)
- Certified Information Systems Security Professional (CISSP)
- Certification, Information Systems Audit and Control Association (ISACA)
- Certified in Risk and Information Systems Control (CRISC)
- Security Clearance: Current or previous Federal security clearance at the SECRET level or higher. Individuals with previous clearance must be eligible to re-apply for security clearance. Additional information regarding security clearances can be found at: www.state.gov/m/ds/clearances/c10978.htm.

Appointment Type

Permanent exempt full-time: This position is exempt from Civil Service rules pursuant to San Francisco Charter Section 10.104 and serves at the discretion of Appointing Officer.

Compensation

The salary range may be up to $191,308. Appointments may be considered at a higher level. For further discussion, inquiries on compensation should be directed to Ralph Andersen & Associates.

The City & County of San Francisco's (CCSF) benefits package can be found at: sfdhr.org/benefits-overview.

Other outstanding benefits offered with this position include:

- Medical, Dental and Life Insurance; Long-term Disability Plan;
- Defined Retirement Plan; Deferred Compensation; and Social Security;
- Paid Management Training Program; Wellness Program; and
- Vacation/Holiday/Sick Time; and Administrative Leave.

To Be Considered

Ralph Andersen & Associates is working exclusively with SFO Leadership to encourage highly qualified candidates to submit for this outstanding career opportunity. Review and evaluation of candidates by Ralph Andersen & Associates will be done upon receipt of completed materials. ***This position will be considered "open" until a final selection is made.*** Candidates are encouraged to apply prior to ***Monday, January 14, 2019*** for optimal consideration. ***Electronic submittals are strongly preferred*** and should include a compelling cover letter and comprehensive resume. Professional references will be required later in the process along with other background and verifications.

Electronic submittals should be sent to: apply@ralphandersen.com.

Interested candidates may also apply via U.S. Mail: Ralph Andersen & Associates, 5800 Stanford Ranch Road, Suite 410, Rocklin, California 95765.

Ralph Andersen & Associates will conduct the initial evaluation of submitted materials to determine the best overall match with the established criteria as outlined in this recruitment profile. SFO's Leadership will make the final selection of top candidates and will design a comprehensive selection process that may include other dimensions. The top candidate selected will need to take a management battery test and also be required to obtain TSA clearance for employment.

Confidential inquiries regarding this position are welcomed and should be directed to Heather Renschler at (916) 630-4900.

The City and County of San Francisco is committed to equal employment opportunity.