SFO

San Francisco International Airport
is accepting applications for the position of

Chief Information Security Officer

Cyber Security Career Opportunity of a Lifetime!

A truly rare opportunity to join an award winning and progressive organization, the San Francisco International Airport (SFO), has become available. 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 cyber security field 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 airport that serves nearly 58 million passengers annually. SFO offers nonstop flights to 51 international cities on 43 international carriers. The Bay Area's largest airport also connects nonstop with 86 U.S. cities on 12 domestic airlines.

SFO's mission is to provide an exceptional airport in service to our communities, and its core values are Safety and Security, Teamwork, Excellence, and Care. The airport is committed to redefining air travel by providing the highest level of service to their guests.

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. The Airport Director Ivar C. Satero, is responsible for the day-to-day operation of the Airport.

The Airport, an enterprise department of the City & County of San Francisco, has a workforce of approximately 1,700 City employees and strives to be a diverse, equitable, and inclusive employer. For more information, visit www.flysfo.com and watch this video about careers at SFO.

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 Airport's 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 of 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;
- Manage 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 and also manage the Airport's ability to respond and mitigate follow-up on attacks as attackers spread inside a compromised network;
- Manage 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;

- Address periodic and on-going audit results and recommendations for infractions and penetrations in a timely fashion that is well documented and implemented including updates to policies and internal operating procedures as needed;
- 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 Payment Card Industry (PCI) standards and other related criteria in an airport environment;
- Provide strategic direction and oversight within the field of information security and forensics as directed by the Chief Information Officer (CIO);
- Investigate potential misuses of information resources as directed by the CIO; and importantly, manage effectively to deliver results and apply practical experience to meet the continually evolving cyber security needs in a robust and dynamic environment; and
- Deliver results and apply practical experience to meet the continually evolving cyber security needs in a robust and dynamic environment.

The Ideal Candidate

The ideal candidate will have recent director level cyber security management experience underpinned by a broader technology background. Importantly, the ideal candidate will be able to address security needs "inside the fence" at a major airport and effectively deal with a variety of key stakeholders including airlines, concessionaires, retailers, travelers, airport staff and the general public.

This top caliber individual will have a demonstrable background in working with varied stakeholder groups including business interests to develop and deliver an organization-wide cyber security agenda. Additionally, this cyber security expert will have a proven track record of assessing organizational threats and vulnerabilities at an operational level and delivering specific remediation actions and initiatives. This highly qualified individual will also have successfully coordinated an immediate response to specific cyber security threats. This would include the ability to revise and document internal operational procedures to avoid future attacks.

The selected 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 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 highly ethical and forthright individuals able to demonstrate integrity and professionalism in all aspects of their work;
- Be politically astute and skilled in how to convey the situation and the message effectively;
- Have the confidence to assertively and quickly solicit and marshal resources from others; and
- Effectively listen, articulate, and act with sound judgment on behalf of the organization and the public.

Qualifications

Candidates will be expected to meet (and preferably "exceed") the minimum qualifications listed below required at time of submittal:

Experience: Six (6) years of recent and verifiable managerial experience in the cyber security domain of a multi-faceted and complex operational environment. Beyond airport specific experience, candidates may draw from experience in a multi-faceted environment such as hospitals, universities or other large, complex environments dealing with protection of critical national infrastructure. Supervision and oversight of staff is required within the operational setting of the dynamic and robust environment.

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

Substitution: Additional qualifying experience as described above may be substituted for the education requirement on a year for year basis for up to two (2) years. (One year of work experience is equal to 30 semester or 45 quarter units).

Certifications: Industry certifications are highly desirable and should be suitable to the managerial level of this position. An example of this may be the Certification of Information Systems Security Management Professional (CISSP-ISSMP) awarded by International System Security Certification Consortium (ISC2). Other certifications obtained should be detailed and presented in the applicant's submitted material for review and evaluation.

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 normal salary range is $155,948 to $199,030. Appointments above this range, up to $230,412 annually based on experience/qualifications, may be considered for a top candidate and requires a special approval process. The City & County of San Francisco's (CCSF) benefits package can be found at: http://sfdhr.org/benefits-overview.

Other outstanding benefits offered with this position include:

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

How to Apply

The Chief Information Security Officer (CISO) position is being conducted on a national basis by our executive search consultants, The Hawkins Company. They will review all written materials submitted and will screen and evaluate all candidates. The most highly qualified candidates will be invited to participate in a formal selection process. This is a confidential process and will be handled accordingly throughout the various stages of the recruitment. References will not be contacted until mutual interest has been established. ***Candidates are encouraged to apply by June 12, 2020. This position will be considered "open" until a final selection is made.***

Interested and qualified candidates are encouraged to submit a letter of interest, including major accomplishments, and resume, electronically to sfo.ciso@thehawkinscompany.com. Preference is for electronic submissions however materials may be mailed to:

THE HAWKINS COMPANY
8939 S. Sepulveda Blvd., #110-216
Los Angeles, CA 90045

Confidential inquiries are encouraged and should be directed to: Bill Hawkins, (310) 348-8800, bill@thehawkinscompany.com or Todd Hawkins, (213) 300-9342, todd@thehawkinscompany.com or Tisa Jones, (213) 309-7984, tisa@thehawkinscompany.com.

The candidate selected for employment will be required to undergo a Management Assessment and obtain Transportation Security Administration (TSA) Security Clearance.

Management Test Battery (MTB)
Top candidate(s) will be invited to participate in a computer-based examination designed to measure competencies in job-related areas that may include but are not limited to: Problem Solving; Leadership; Decision-Making; Interpersonal Skills; Human Resource Management; Team Building: Communication; Conflict Management; and Process Improvement. For more information about this Management Assessment (and a suggested reading list) please visit: www.sfdhr.org/index.aspx?page=343.

The City & County of San Francisco is an equal opportunity employer, values workforce diversity and seeks to create an environment and culture that embraces employee differences. All qualified applicants are considered in accordance with applicable laws, prohibiting discrimination on the basis of race, religion, color, gender, age, national origin, sexual orientation, physical or mental disability, marital status or veteran status or any other legally protected status. We will provide assistance in the recruitment, application and selection process to applicants with disabilities who request such assistance.