FILE NO. 211294 ORDINANCE NO.

[Administrative Code - Office of Cyber Security; Chief Information Security Officer]

Ordinance amending the Administrative Code to establish the Office of Cyber Security and the position of Chief Information Security Officer (CISO) who, in coordination with department technology professionals, is responsible for preventing, detecting, and remediating the damage to City infrastructure and information resources from cyber-related incidents; require departments to appoint a Department Information Security Officer; add the CISO as a permanent member of the Committee on Information Technology (COIT); name the City Administrator or designee as Chair of COIT; and provide that the City Administrator with the Mayor's concurrence appoints the Chief Information Officer (CIO).

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in ~~*strikethrough italics Times New Roman font*~~.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. Chapter 22A of the Administrative Code is hereby amended by revising Sections 22A.3 and 22A.4, to read as follows:

SEC. 22A.3. COMMITTEE ON INFORMATION TECHNOLOGY.

Establishment and Composition. There is hereby created a Committee on Information Technology (COIT).

(a) COIT shall be composed of ~~seven~~ *eight* permanent members consisting of the Mayor, the President of the Board of Supervisors, the Controller, the City Administrator, the Clerk of the Board of Supervisors, the Executive Director of the Human Rights Commission, ~~*and*~~ the *Chief Information Officer (*CIO), *and the Chief Information Security Officer (CISO)*, or their designees. ~~*The Mayor, the President of the Board of Supervisors, the Controller, the City Administrator, the Clerk of the Board of Supervisors, the Executive Director of the Human Rights Commission, and the CIO, shall elect a Chair, who shall serve for a two-year term. All of the permanent members of COIT shall be eligible to serve as Chair.*~~ *The City Administrator or the City Administrator's designee shall serve as Chair.* Five additional Department Heads shall be recommended by the Chair and approved by the permanent members for two-year terms, one representing each of the major service areas: (a) Public Protection, (b) Human Welfare and Neighborhood Development, (c) Community Health, (d) Culture and Recreation, and (e) General Administration and Finance; and three additional non-permanent members representing the major service area of Public Works, Transportation, and Commerce. The ~~*seven*~~ *eight* permanent members and eight non-permanent members ~~*will*~~ *shall* be voting members of COIT.

* * * *

SEC. 22A.4. CHIEF INFORMATION OFFICER.

(a) **Establishment and Composition:** There is hereby created the position of Chief Information Officer (CIO) for the City and County of San Francisco. The CIO shall:

(1) Be appointed by the *City Administrator, with the concurrence of the* Mayor.

(2) Serve as a permanent member of the Committee on Information Technology (COIT) with the authority and responsibility to develop recommendations and implement COIT standards, policies, and procedures for all City Departments.

(3) Serve as the Director of the Department of Technology with responsibility for making recommendations regarding development, implementation, maintenance, operation, and support of all citywide ICT.

(b) **Purpose and Duties:** The CIO shall (i) monitor trends and advances in ICT; (ii) advise the Mayor, Board of Supervisors, and City Departments regarding opportunities to provide higher quality, more timely, and more cost-effective governmental services; (iii) ensure coordinated and non-duplicative acquisition of ICT technologies for maximum cost effectiveness and use; (iv) ensure sharing of ICT technologies among City Departments as the most cost-effective method of providing the highest quality and most timely governmental services that could otherwise be cost prohibitive; (v) develop uniform policies and coordinated systems for the use, acquisition, and implementation of ICT technologies; ~~*and*~~ (vi) establish Citywide standards~~,~~ and procedures to ensure cost-effective and useful retrieval and exchange of information both within and among the various City Departments and from the City to the people of San Francisco*; and (vii) direct the City's cyber security program*.

(c) The CIO shall (i) consult with City Departments about ICT staffing needs and develop an ICT staffing plan for review and approval by COIT; and (ii) monitor hiring of ICT staff and adherence to the ICT staffing plan adopted by COIT.

(d) The CIO shall develop for the review and approval of COIT policies and procedures for the effective management of technology investments throughout their entire life-cycle, including~~,~~ but not limited to project definition, procurement, development, implementation, operation, performance evaluation, and enhancement or retirement.

Section ~~3~~2. The Administrative Code is hereby amended by adding Chapter 22I, consisting of Sections 22I.1, 22I.2, 22I.3, 22I.4, 22I.5, and 22I.6, to read as follows:

CHAPTER 22I: OFFICE OF CYBER SECURITY AND

DUTIES OF THE CHIEF INFORMATION SECURITY OFFICER

SEC. 22I.1. FINDINGS.

On June 4, 2021, Mayor London Breed issued Executive Directive No. 21-02, announcing that protecting the City's technology and information is vital to the proper functioning of the City and the ability of City departments and personnel to serve residents. In order to further the protection of City assets, the prevention, detection, and remediation of cyber-related incidents is a top priority of the City and essential to the security of San Francisco government and its residents. In the directive, the Mayor directed the City's Chief Information Officer and the City Administrator to recommend changes to the Administrative Code to formalize and strengthen the City's cyber security functions and programs.

SEC. 22I.2. PURPOSE OF CHAPTER.

(a) The purpose of this Chapter 22I is to strengthen and coordinate the City's security of information resources. The creation of the Office of Cyber Security will improve the City's information security by doing the following:

(1) ensure coordination of City Departments' response to cyber security threats;

(2) identify primary responsibility for the City's response during emergencies caused by cyber security attacks;

(3) share best information security practices, procedures, and requirements with City Departments;

(4) provide review of proposed technology purchases by City Departments to address cyber security risks during procurement; and

(5) avoid uncoordinated and duplicative information or system security purchases by City Departments when such technology can be more effectively purchased as part of a coordinated City effort for maximum cost effectiveness and use.

(b) In enacting and implementing this Chapter 22I, the City is assuming an undertaking only to promote the general welfare. It is not assuming, nor is it imposing on its officers and employees, an obligation for breach of which it is liable in money damages to any person who claims that such breach proximately caused injury.

(c) Municipal Transportation Agency. Consistent with Charter Section 8A.101(d), the Municipal Transportation Agency shall comply with the provisions of this Chapter 22I and shall be solely responsible for its administration and enforcement with respect to matters within the Municipal Transportation Agency's jurisdiction. The Municipal Transportation Agency Board of Directors shall provide the City Administrator with an annual report of reported incidents and its compliance with the established City information security standard.

(d) Public Utilities Commission. Consistent with Charter Section 8B.121(a), the Public Utilities Commission shall comply with the provisions of this Chapter 22I and shall be solely responsible for its administration and enforcement with respect to matters within the Public Utilities Commission's jurisdiction. The Public Utilities Commission shall provide the City Administrator with an annual report of reported incidents and its compliance with the established City information security standard.

SEC. 22I.3. DEFINITIONS.

For purposes of this Chapter 22I, the following definitions shall apply:

"City" means the City and County of San Francisco and all of its units or components of government.

"Chief Information Officer" means the Chief Information Officer for the City appointed pursuant to Administrative Code Section 22A.4.

"City Department" means any unit or component of City government, including but not limited to named departments, boards and commissions, offices, agencies, and officials.

"Committee on Information Technology" or "COIT" means the committee established in Administrative Code Section 22A.3.

"Information and Communications Technology" or "ICT" means information and communications technology and computer-based equipment and related services designed for the storage, manipulation, and retrieval of data by electronic or mechanical means, or both.

"Information Resources" means Information and Communications Technology operated by or for the City, including equipment, facilities, systems, applications, and cloud services that relate directly to data processing equipment or services which are directly managed by various departmental divisions for Management Information Systems (MIS), including but not limited to, the Controller's Information Services Division (ISD), the Airport's MIS Division, the Public Utilities Commission's Bureau of MIS, and the Department of Public Health's MIS.

"Information Security Standards" means standard requirements created by the Chief Information Security Officer for the protection and resiliency of the City's information resources.

SEC. 22I.4. OFFICE OF CYBER SECURITY.

*(a) **Establishment.** The Office of Cyber Security is hereby created within the Department of Technology and shall be headed by the Chief Information Security Officer and staffed by such officers and employees as are authorized pursuant to the budgetary and fiscal provisions of the Charter.*

*(b) **Mission and Purposes.** The Office of Cyber Security shall have these missions and purposes:*

(1) Advising the Mayor, the Board of Supervisors, the City Administrator, the City Chief Information Officer, and City Departments regarding information security for City Departments.

(2) Advising the Committee on Information Technology (COIT) on compliance with adopted information security standards, policies, and funding plans, and serving as a permanent member of COIT.

(3) Protecting City-connected technology and information resources.

(4) Continuously improving the City's ability to detect cyber security events, contain and eradicate compromises to security, and restore information resources to a secure and operational status.

(5) Evaluating technology vendors and partners to identify cyber security risks to City operations.

SEC 22I.5. CITY CHIEF INFORMATION SECURITY OFFICER.

*(a) **Establishment of Position.** There is hereby created the position of Chief Information Security Officer (CISO) for the City and County of San Francisco. The CISO shall:*

(1) Be appointed by the Chief Information Officer *following consultation with the City Administrator.*

(2) Serve as a permanent member of COIT with the authority and responsibility to develop information security recommendations and implement COIT information security standards, policies, and procedures for all City Departments.

(3) Head the Office of Cyber Security.

*(b) **Purpose and Duties.** The CISO's duties shall include, but are not limited to the following:*

(1) Develop and maintain a centralized cyber security detection, response, and recovery program, tools and operational capability for preventing and responding to compromises of City information resources for City Departments.

(2) Develop and maintain training, tools, and operational capability to minimize cyber security vulnerabilities of City information resources for City Departments.

(3) Provide a citywide information security standard to reduce the risk of compromise to the City's information resources, including but not limited to receiving and responding to security incidents from City Departments, and mitigating the risks to City information resources.

(4) Conduct risk-based assessment of new vendor technologies or technology-related services during the procurement process.

(5) Support City Departments' cyber emergency exercises and conduct periodic citywide cyber security emergency exercises with City Departments.

(6) Test cyber security preparedness of City Departments on a regular basis.

(7) Work with City Departments through the designated Departmental Information Security Officers to reduce the City's risk to cyber security incidents.

(8) Develop and update citywide cyber security requirements to mitigate the City's risk profile, and comply with legal and regulatory cyber security requirements.

(9) Support City Departments' implementation of the City's information security standards.

(10) Provide the Mayor and City Administrator with an annual report of reported incidents and each City Department's compliance with the established City information security standard.

SEC.22I.6. CITY DEPARTMENTS.

(a) City Departments. Each City Department, ("Department") shall:

(1) Appoint a Departmental Information Security Officer (DISO) to coordinate cyber security efforts with the CISO.

(2) Adopt the City's information security standard for reducing the risk of compromise to the City's information resources as a basis of their Department's cyber security program.

(3) Consult with the Office of Cyber Security to evaluate cyber security risk prior to initiating new information technology projects, implementing major changes to information systems, or selecting vendors of technologies or vendors providing technology-related services.

(4) Support cyber incident response in accordance with the then-existing San Francisco Unified Cyber Command Plan.

(5) Conduct and update a Department cyber security risk assessment based on standards established by the Office of Cyber Security.

(6) Test and update the Department's cyber security emergency response plan based on standards established by the Office of Cyber Security.

(7) Maintain Department cyber security requirements that are equivalent to or greater than the citywide information security standards and provide non-standard Department requirements to the Office of Information Security.

(8) Participate in citywide cyber security forum meetings organized by the Office of Cyber Security.

(b) Given the broad definition of "City Department" under Section 22I.3, and the wide range of sizes of City Departments, the requirement in subsection (a), above, that each City Department appoint a DISO shall not be understood to preclude the same person from serving as DISO for more than one City Department, nor preclude the DISO for a City Department from having other responsibilities.

Section 3. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

Section 4. Scope of Ordinance. In enacting this ordinance, the Board of Supervisors intends to amend only those words, phrases, paragraphs, subsections, sections, articles, numbers, punctuation marks, charts, diagrams, or any other constituent parts of the Municipal Code that are explicitly shown in this ordinance as additions, deletions, Board amendment additions, and Board amendment deletions in accordance with the "Note" that appears under the official title of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/
MARGARITA GUTIERREZ
Deputy City Attorney

n:\legana\as2021\2200032\01587123.docx