CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: HONORABLE MAYOR AND
CITY COUNCIL

FROM: Julie Edmonds-Mares
Margaret McCahan

**SUBJECT: AMENDMENTS TO THE CITY
PAY PLAN**

DATE: January 18, 2018

Approved _Dringer A Maguire_   Date _1-24-18_

RECOMMENDATION

1. Adopt a resolution to amend the City of San José Pay Plan effective February 6, 2018, to create the following classification:
   a. City Information Security Officer U (1366) with a salary range of $133,868.78 - $208,668.73 annually.

2. Approve the following position changes to the Information Technology Department:
   a. Add 1.0 City Information Security Officer U (1366); and
   b. Eliminate 1.0 Deputy Director U (1640).

OUTCOME

If the above recommendation is approved, the City of San José Pay Plan will be amended to create the new classification of City Information Security Officer U (1366); and Information Technology Department staffing will be changed to reflect the addition of the new classification.

BACKGROUND

When new job classifications are added or deleted, job titles are changed, or salaries are revised, the City of San José Pay Plan must be amended by Council resolution. The City Pay Plan reflects all job classification and compensation changes made through Council Resolution, and is on file in the Human Resources Department, and published on the City's Internet and Intranet sites.

ANALYSIS

The 2017-2018 Adopted Operating Budget included the creation of the Cybersecurity Office within the Information Technology Department and added 1.0 Deputy Director position to serve as the City Information Security Officer (CISO). The Cybersecurity Office was created to manage the City's cybersecurity risks, build organizational resilience, and administer increasing Federal, State, and industry compliance requirements. The addition of this new position is part of the IT Strategic Plan and addresses a series of audit recommendations from the City Auditor's Office and the City's external auditors.

In September 2017, the City attempted to recruit for a Deputy Director level CISO to complete initial policy and compliance work as part of the organization's Cybersecurity Work Plan. The recruitment was unsuccessful in finding qualified candidates primarily due to the competitiveness of the salary range for this level of work and talent shortages in the profession and area. Applicant profiles and salary feedback made it clear that the City was not competitive for a CISO level professional in the current market. Given the recruitment challenges, the Information Technology Department and Human Resources Department collaborated to reevaluate the position. A salary survey was conducted with the City's Bay Area comparator agencies. It was determined the level and scope of work required by the CISO classification is more appropriately aligned at the Assistant Director level. Salaries are increasing for cybersecurity roles due to high demand, low supply, and the growing risks and losses experienced by organizations worldwide. In order to attract and retain quality candidates and remain competitive with our comparator agencies, the proposed classification and salary is recommended to be comparable to the Assistant Director classification.

The creation of the proposed CISO classification is a single incumbent position, designated to lead the City's new Cybersecurity Office. The CISO will work across departments with citywide authority to administer all security measures and programs required to maintain the City's compliance and ability to resume operations in the event of a cyber-attack. Specialized job requirements are incorporated into the proposed classification specification to meet the technical, regulatory, clearance level, certification, and oversight requirements essential to performing the duties of the position.

    a. City Information Security Officer U, with an annual pay range of $133,868.78 - $208,668.73: This classification manages the design, development, operation, and maintenance of the City's information cybersecurity services. The CISO leads the cybersecurity requirements, strategy, and programs at an enterprise-level across all departments. The CISO directs information security staff and advanced cybersecurity services to ensure information assets and processes are protected; identifies, evaluates, and leads resolution of information and system security risks; oversees cybersecurity training programs for all City staff; enables business resilience through continuity planning and solutions; ensures compliance with regulatory requirements; manages audit and incident responses; and aligns the overall risk posture of the City.

EVALUATION AND FOLLOW-UP

No additional City Council action is expected following the adoption of the proposed resolution. Revisions to the Pay Plan are reported to the Civil Service Commission at the first regularly scheduled meeting following Council action.

PUBLIC OUTREACH

This memorandum will be posted on the City's website for the February 6, 2018 City Council Agenda.

COORDINATION

This memorandum was coordinated with the Office of Employee Relations, City Attorney's Office, and Information Technology Department.

COMMISSION RECOMMENDATION/INPUT

There is no City Commission input regarding these actions.

COST SUMMARY/IMPLICATIONS

The 2017-2018 Adopted Operating Budget included the addition of 1.0 Deputy Director U to serve as the City's Information Security Officer. The elimination of this Deputy Director position and the addition of the new CISCO classification is recommended in this memorandum. The cost of the new CISO at top step is approximately $276,000 per year, which exceeds the costs of the Deputy Director position by approximately $33,000 annually. In 2017-2018, the higher costs will be absorbed in the Information Technology Department General Fund budget. The ongoing costs will be included as part of the 2018-2019 Base Budget process.

CEQA

Not a Project, File No. PP10-068(b), Municipal Code, Title 3.

Julie Edmonds-Mares
Deputy City Manager/
Acting Human Resources Director

Margaret McCahan
Budget Director

For questions please contact Aracely Rodriguez, Employment Division Manager at (408) 975-1411.

Attachment:
City Information Security Officer U Class Specification

City of San José
CLASS SPECIFICATION

Title: City Information Security Officer U (1366)

DEPARTMENT	ACCOUNTABLE TO	FLSA STATUS
Information Technology	Director, Information Technology U	Exempt

CLASS SUMMARY
Under general direction, manages the design, development, operation, and maintenance of the City's information cybersecurity services. The City Information Security Officer (CISO) leads the cybersecurity requirements, strategy, and programs at an enterprise-level across all departments. The CISO directs information security staff and advanced cybersecurity services to ensure information assets and processes are protected; identifies, evaluates, and leads resolution of information and system security risks; oversees cybersecurity training programs for all City staff; enables business resilience through continuity planning and solutions; ensures compliance with regulatory requirements; manages audit and incident responses; and aligns the overall risk posture of the City. Performs related work as required.

DISTINGUISHING CHARACTERISTICS
This classification is unclassified and manages a critical division in the Information Technology Department. This class is distinguished from the Assistant Director classification in that the latter has a broader scope of responsibility. The City of San José's City Information Security Officer is a highly-specialized, single position classification, reporting directly to the Director, Information Technology/City's Chief Information Officer.

QUALIFICATIONS
(These qualifications are typically required. An equivalent combination of education and experience sufficient to satisfactorily perform the duties of the job may be substituted.)

<u>Minimum Qualifications</u>

Education and Experience
A Bachelor's degree from an accredited college or university in computer science, management information systems, business/public administration, or a closely related field AND seven (7) years of increasingly responsible experience in cybersecurity application and infrastructure, technology management, or telecommunications, including a combination of five (5) years of supervisory and project personnel management experience, with at least three (3) years of supervision experience in direct support of information security programs of significant scale and scope similar to a large government, to include budgeting, contracting, procurement, and supervision of staff and technical project teams in delivering goals and measured service levels.

Acceptable Substitution
A Master's Degree in a relevant field from an accredited college or university may be substituted for one (1) year of the required three (3) years of supervision experience in direct support of information security programs of significant scale and scope similar to a large municipal government, to include budgeting, contracting, procurement, and supervision of staff and technical project teams.

Required Licensing (such as driver's license, certifications, etc.)
Possess and maintain a current, terminal level cybersecurity credential such as:
- Certified Information Systems Security Professional (CISSP);
- Certified Information Systems Auditor (CISA);
- Certified Information Security Manager (CISM);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified in Risk and Information Systems Control (CRISC); or

City of San José
CLASS SPECIFICATION

Title: City Information Security Officer U (1366)

- An equivalent professional, industry recognized certification acceptable to the City.
- Obtain and maintain SECRET Security Clearance within a reasonable period of time acceptable to the City.

Other Qualifications
(Incumbents may be required to have different combinations of the listed qualifications, or more specific job-related qualifications depending on the position.)

Basic Competencies
(Needed at entry into the job in order to perform the essential duties.)

- Job Expertise – Demonstrates knowledge of and experience with applicable professional/technical principles and practices, Citywide and departmental procedures/policies and federal and state rules and regulations.

- Communication Skills - Effectively conveys information and expresses thoughts and facts clearly, orally and in writing; demonstrates effective use of listening skills and displays openness to other people's ideas and thoughts.

- Collaboration – Develops networks and builds alliances; engages in cross-functional activities.

- Analytical Thinking - Approaching a problem or situation by using a logical, systematic, sequential approach.

- Vision/Strategic Thinking – Support, promote, and ensure alignment with the organization's vision and values. Understand how an organization must change in light of internal and external trends and influences. Builds a shared vision with others and influence others to translate vision to action.

- Initiative – Exhibits resourceful behaviors toward meeting job objectives; anticipates problems, is proactive, and avoids difficulties by planning ahead; displays willingness to assume extra responsibility and challenges; pursues continuing education opportunities that promotes job performance.

- Project Management – Ensures support for projects and implements agency goals and strategic objectives.

- Supervision - Sets effective long and short-term goals based on a good understanding of management practices; establishes realistic priorities within available resources; provides motivational support; empowers others; assigns decision-making and work functions to others in an appropriate manner to maximize organizational and individual effectiveness.

Additional Competencies and/or Desirable Qualifications
(Competencies, knowledge, skills and abilities that are more position specific and/or likely to contribute to more successful job performance.)

Knowledge of:
- Cybersecurity standards and framework applicable to the municipal setting.
- Technologies typical of the City's operating environment, including but not limited to:
  - Server, desktop, and mobile operating systems,
  - Network Directory and operating systems,
  - Productivity software products,
  - IP-based networks,

City of San José
CLASS SPECIFICATION

Title: City Information Security Officer U (1366)

- Principles of deskside and mobile computing,
- Software development practices and architectures,
- Identity and authentication solutions, and
- Industrial and supervisory control systems.

DUTY NO.	TYPICAL CLASS ESSENTIAL DUTIES: (These duties and estimated frequency are a representative sample; position assignments may vary depending on the business needs of the department.) Duties may include, but are not limited to, the following:	FREQUENCY*
1.	Manages the design, development, operation, and maintenance of the City's information cybersecurity services; provides strategic and operational information security and technology leadership Citywide; establishing support, and continuously improving enterprise information security and privacy technology.	Daily
2.	Supervises subordinates and other staff to include: prioritizing and assigning work; conducting performance evaluations; ensuring staff are trained; and making hiring, termination, and disciplinary recommendations. Evaluates training needs and workload balance for staff and prepares plan for implementation.	Daily
3.	Manages the City's responses to incidents and ensures they are appropriately addressed, documented, and reported.	Daily
4.	Manages security incidents and events; monitors environments for emerging threats and advises stakeholders on the appropriate course of action.	Daily
5.	Administers contracts, vendor services, and enterprise architecture processes related to the City's cybersecurity profile, including participating in negotiations and directing the preparation of agreements.	Daily
6.	Serves as a primary liaison to departments and offices regarding information security policies, practices, standards, and incident reporting; works with departments to implement and maintain controls.	Daily
7.	Supports and sustains cybersecurity alliances for intelligence sharing and joint response across agencies.	Weekly
8.	Represents the City and its interests with partner agencies, including the Department of Homeland Security, Federal Bureau of Investigations, State of California departments, law enforcement, and advisory groups.	Weekly
9.	Formulates, implements, and monitors a detailed program budget for all information security projects.	Weekly
10.	Develops and administers up-to-date information on security policies; oversees the approval, training, and dissemination of security policies and practices; manages security and risk awareness, training, and reporting programs Citywide.	As Required
11.	Ensures the City is in compliance with applicable regulatory requirements, laws, directives, policies, and customer requirements regarding information security.	As Required
12.	Implements new concepts and innovations using technological developments and applications to improve operations and controls.	As Required

13.	Provides support to the department head in the acquisition, compilation, and presentation of statistical and other data required to obtain regulatory funds for various projects. Plans and directs research projects, prepares recommendations, and prepares regular reports.	As Required
14.	Manages business plans and exercises with departments and offices to design, implement, test, and validate recovery processes to ensure the City can restore operations within set recovery time and recovery point objectives.	As Required
15.	Directs audit responses and cybersecurity assessments, monitoring of threat activity and alerts, and remediation of risks and alerts of high potential impact to the City across departments.	As Required
16.	Performs other related duties as assigned.	As Required

*Frequency defined as Daily/Several Times, Daily, Weekly, Intermittent, or As Required

PHYSICAL/ENVIRONMENTAL ELEMENTS
The following is a general statement for the classification. Individual positions may have additional or different physical/environmental elements.

In an office environment, possess ability to:
- Operate, access, enter, and retrieve data using standard office equipment, including but not limited to a computer or tablet;
- Read printed materials and a computer screen;
- Communicate in person and over the telephone;
- Lift, carry, push, and pull materials and objects up to 60 pounds, or heavier weights, in all cases with the use of proper equipment;
- Move between/within work areas, including but not limited to sitting, walking, and standing on various surfaces, turning, bending, grasping, and making repetitive hand movements;
- Be exposed to moderate noise levels and controlled temperature conditions;
- Maintain professional demeanor during interactions with staff, customers, and the public.

CLASSIFICATION HISTORY *Created 02/18; s000*