5-96

SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FROM: Human Resources Dept.

SUBMITTAL DATE:
July 9, 2007

SUBJECT: Establishment of a New Classification of Chief Information Security Officer, and amend Ordinance No. 440 pursuant to Resolution No. 440-8734

RECOMMENDED MOTION: That the Board approve the recommendation in the attached Resolution No. 440-8734.

BACKGROUND: Human Resources (HR) conducted a classification study at the request of Riverside County Information Technology Department (RCIT), and as a result of this study HR recommends adding a new single-position classification of Chief Information Security Officer. The incumbent would direct countywide information security programs that are designed to provide for the protection and confidentiality of data, along with other information assets of Riverside County.

Ronald W. Komers
Asst. County Executive Officer/Human Resources Dir.

FINANCIAL DATA				
	Current F.Y. Total Cost:	$ 0	In Current Year Budget:	N/A
	Current F.Y. Net County Cost:	$ 0	Budget Adjustment:	N/A
	Annual Net County Cost:	$ 0	For Fiscal Year:	2007/08

SOURCE OF FUNDS:

Positions To Be Deleted Per A-30 ☐

Requires 4/5 Vote ☐

C.E.O. RECOMMENDATION:

APPROVE

BY: Steve P. Schubert

County Executive Office Signature

☐ Consent ☒ Policy

☐ Consent ☐ Policy

Dep't Recomm.:

Per Exec. Ofc.:

Prev. Agn. Ref.: | **District:** | **Agenda Number:** 3.34

G:\EXEC\Form 11\Class & Comp\Chief Info Security Officer.doc

BACKGROUND continued

Currently, these duties are assigned to an Information Technology Officer II position, but the position has evolved as we expanded our IT infrastructure and heightened our information security and privacy standards and practices, making the current classification increasingly unsuitable. Since the incumbent has submitted her resignation from County employment effective August 15, 2007, RCIT wishes to begin immediate recruitment for appropriate candidates.

We recommend establishing a new classification of Chief Information Security Officer that would properly define the expanded concept, duties and scope of responsibilities expected of a qualified incumbent, including the specific requirement to maintain current 'Information Systems Security' certification. Since this request is only to add this classification to the Class and Salary Listing, there is no cost impact at this time.

CLASSIFICATION ADDITION

Chief information Security Officer: It is recommended to add this class to the Class and Salary Listing at MCO 670 L13 ($91,484 - $125,791). This salary is within 1% of the mean of the HR compensation survey: Contra Costa, Fresno, Los Angeles and Monterey Counties have equivalent classes, although they don't require certification. Their maximum mean annual salary is $124,824. In order to offer a competitive salary to viable candidates in this high demand profession, the maximum mean survey salary should be used to establish an appropriate salary plan/grade. The classification specification is attached.

RESOLUTION NO. 440-8734

BE IT RESOLVED by the Board of Supervisors of the County of Riverside, State of California, in regular session assembled on July 17, 2007, that pursuant to Section 4.C. of Ordinance No. 440, the Assistant County Executive Officer/Human Resources Director is authorized to amend the Class and Salary Listing of Ordinance No. 440, operative the beginning of the pay period following approval, as follows:

Job Code	+/-	Class Title	Salary Plan/Grade
77271	+	Chief Information Security Officer	MCO 670

/kc
07/09/2007
440 Resolutions\KC

CHIEF INFORMATION SECURITY OFFICER

Class Code: 77271

COUNTY OF RIVERSIDE
Established Date: Jul 19, 2007
Revision Date: Jul 19, 2007

SALARY RANGE

$43.98 – $60.48 Hourly $7,623.63 – $10,482.54 Monthly $91,483.60 – $125,790.50 Annually

CLASS CONCEPT:
Under general direction of the County Chief Information Officer, directs countywide information security programs that are designed to provide the protection and confidentiality of data, along with other information assets of Riverside County. This single position class has Countywide responsibility for formulating and promulgating policy for, and developing, managing and integrating Countywide information security and privacy related programs designed to protect all County information systems and data.

The Chief Information Security Officer (CISO) directs Countywide information security and related privacy efforts through subordinate staff and through department designated Information Security Officers. The incumbent must exercise strong organizational and team leadership skills to facilitate interdepartmental compliance and to ensure that departmental IT security staffs fully integrate appropriate security and privacy practices. The Chief Information Security Officer is the official HIPAA Security Officer of the County and shall coordinate and oversee generally all HIPAA security requirements for the County.

The position requires extensive, up-to-date technical knowledge in information systems, detailed knowledge of security and privacy technologies and best practices, the Health Insurance Portability and Accountability Act (HIPAA) and the Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley) privacy-related requirements, and use of appropriate security controls and methods. This position also requires an extensive knowledge of County information system resources and applications, information security and privacy legislation and related policy issues, and must possess the ability to develop and maintain effective interpersonal relationships with internal and external managers, IT technical staff, legal staff, and related industry experts. This position represents the County's interests before State and Federal agencies and regulatory bodies.

REPRESENTATION UNIT: Unrepresented Management

EXAMPLES OF ESSENTIAL DUTIES:
(Depending on the area of assignment, duties may include, but are not limited to, the following)

- Oversees the development and implementation of Countywide information security policies and procedures to protect the County from internal and external IT threats and vulnerabilities.
- Represents the Chief Information Officer to County departments, information technology advisory bodies, and other committees or agencies involving County policies, plans, methodologies and programs related to security, privacy and confidentiality of data and information technology assets.
- Directs the preparation of short and long term strategies for optimizing the County's Information Security Plan, and formulates and recommends Countywide policies for detecting, deterring and mitigating information security threats.
- Directs and participates in the identification of security risks, development and implementation of security management practices, and the measurement and monitoring of security protection measures.

• Directs the handling of information security breaches and related incidents, including overseeing the activation of the County Network Security Emergency Response Team (CoNSERT) or departmental incident response teams.

• Manage a computer crime or incident scene, including recognition of the proper investigative approach, conducting a field of search to establish probable cause for seizure, proper collection methods, evidence preservation, transportation, computer forensic analysis and case management; use various security tools and prepare reports on findings; submit cases and work with the County Sheriff 'Computer And Technology Crime High-tech' (CATCH) Response Team in the event of a possible legal violation by a County employee or other person using County IT resources.

• Through the CIO, serves as a subject matter expert and internal consultant on the data security implications of proposed new major information technology projects and programs, and makes recommendations to the Board of Supervisors and affected departments.

• Reviews and recommends the professional development curriculum for County IT security and privacy staff to ensure adequate and appropriate training standards in information security and protection measures, and coordinates related training and awareness programs.

• Directs the development and promotion of security and privacy awareness training and education for all levels of the county organization structure on an ongoing basis.

• Participates in the development and implementation of disaster recovery and business continuity plans, to ensure that appropriate IT security measures are addressed.

• Participates in the development, implementation and compliance monitoring of IT security agreements, business associate agreements, chain-of-trust agreements, and Memoranda of Understanding (MOUs) that involve access to or exchange of County information to ensure all security concerns are addressed.

• Leads vendor activities, writes and evaluates proposals, and negotiates contracts for Countywide information security related software, equipment and services, and presents recommendations for funding and approvals to the Chief Information Officer.

• Maintains current knowledge of applicable federal and state information security laws and standards to facilitate County adaptation and compliance.

RECRUITING GUIDELINES:

Education: Graduation from a recognized college with a Bachelor's degree, preferably with major course work in computer science, information systems, electronics engineering, voice/data communications, public/business administration, or a related field. Additional qualifying experience may be substituted for the required education on the basis of one year of experience for 60 semester or 90 quarter units of education.

Experience: Ten years of management experience in the information technology profession with five years concentrated in information security. Five years experience as a County Information Security Analyst III, with management experience, may substitute for this experience requirement. Must have experience with firewalls, anti-virus, Intrusion Detection/Intrusion Prevention Systems (IDA/IPS), virtual private networks (VPN), remote access systems (RAS), public key infrastructure (PKI), encryption, digital certificates, routers, sniffers, distributed denial of service attacks (DDOS), biometrics, DMZ/ Transaction Zones, business continuity planning, auditing, HIPAA and Sarbanes-Oxley regulatory compliance requirements, risk management, contract and vendor negotiation, and physical security.

Knowledge Of: Standard security practices, network architecture, routing and TCP/IP protocols, general business processes and standards associated with areas of assignment, Risk/Threat assessment processes and practices, project planning and management, business continuity planning, documentation and evaluation, managing the evidentiary process, the use of Third Party Applications and native scripts and languages, maintaining the chain-of-custody process and procedures; strong working knowledge of pertinent law and the law enforcement community, and knowledge of the principals and methods used in the analysis and development of information security, systems and procedures; currently accepted information security standards, guidelines and theories; advanced computer technology, equipment

operation, capacity and capability.

Skill In: Superior interpersonal and communication skills (oral and written), strong customer service skills, mediation process presentation and public speaking, extensive skill in investigation/coordination of security anomalies and events, extensive skill in performing a security incident investigation or forensic analysis of a security incident or event.

Ability To: Analyze and interpret complex data, effectively supervise personnel and motivate and direct the work of others, prepare and present effective, clear and concise reports and correspondence, identify and recommend information security needs for the County, analyze problems and identify alternative solutions, deal effectively and harmoniously with County executives, department and assigned staff, customers and the general public.

SUPPLEMENTAL INFORMATION:
Perform and/or direct subordinates and others to:

• Respond to and assist in due diligence and audit requests; conduct periodic departmental audits.

• Monitor and review intrusion detection systems and firewall logs; analyze events and patterns; review firewall and router rules and access control lists; perform network based vulnerability scans and penetration tests.

• Research technical and security topics and maintain information on industry trends.

• Analyze system and access logs; develop and maintain scripts, routines and software to perform vulnerability threat assessments.

• Advise management of risks and best security practices; coordinate County disaster recovery and business continuity tasks.

• Ensure that technology decisions made are compliant with Enterprise Security Architecture; collaborate with departments on security solutions.

• Participate in systems design to ensure implementation of appropriate security policies; evaluate the security posture of computers and networks.

• Respond to network and system intrusive activity and analyze network traffic and system logs to determine corrective action and implement countermeasures; evaluate security incidents, develop solutions and communicate results to end users and technical staff.

• Manage a computer crime or incident scene, including recognition of the proper investigative approach, conducting a field of search to establish probable cause for seizure, proper collection methods, evidence preservation, transportation, analysis and case management.

OTHER REQUIREMENTS:
License/Certificate:

Must possess and maintain current certification within guidelines established by the International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ as a Certified Information Systems Security Professional (CISSP).

Possession of a valid California Driver License may be required.

PRE-EMPLOYMENT:
All employment offers are contingent upon successful completion of both a pre-employment physical exam, including a drug/alcohol test, and a criminal background investigation, which involves fingerprinting. (A felony or misdemeanor conviction may disqualify the applicant from County employment).