CITY OF LINCOLN
SYSTEMS SECURITY ANALYST I/II/SENIOR

Class specifications are only intended to present a descriptive summary of the range of duties and responsibilities associated with specified positions. Therefore, specifications may not include all duties performed by individuals within a classification. In addition, specifications are intended to outline the minimum qualifications necessary for entry into the class and do not necessarily convey the qualifications of incumbents within the position.

DEFINITION:

To perform a variety of professional level work, including the design, implementation, evaluation, and daily management of security systems and solutions; and to perform duties related to threat detection and prevention, education, risk assessment, compliance, governance, business recovery, forensics, and incident response.

DISTINGUISHING CHARACTERISTICS:

Systems Security Analyst I

The **Systems Security Analyst I** is the entry level in the Systems Security Analyst class series. This classification may be alternatively staffed with the Systems Security Analyst II and incumbents may advance to the higher-level after gaining experience and demonstrating a level of proficiency that meets the qualifications of the higher-level class. This class is distinguished from the journey level by the performance of the more routine tasks and duties assigned to positions within this series. Employees work under general supervision while learning job tasks.

Systems Security Analyst II

The **Systems Security Analyst II** is the journey level in the Systems Security Analyst class series and is responsible for the full range of duties. This class is distinguished from the next higher classification of Senior Systems Security Analyst in that the latter is an advanced journey level and performs more complex assignments and may have lead responsibilities. Employees at this level receive only occasional instruction or assistance as new, unusual or unique situations arise and are fully aware of the operating procedures and policies within the work unit. Positions in this class are flexibly staffed and are normally filled by advancement from the Systems Security Analyst I.

Senior Systems Security Analyst

The **Senior Systems Security Analyst** is the advanced journey level in the Systems Security Analyst class series. Incumbents are the recognized experts in their field, including possessing extensive experience designing and architecting complex information technology and security solutions, as well as demonstrating successful technical project management by the advanced level of knowledge and experience required. Positions at this level are distinguished from other classes within the series by the provision of the highest level of technical expertise and knowledge in the performance of duties.

SUPERVISION RECEIVED/EXERCISED:

Systems Security Analyst I

Receives supervision from the Chief Innovation and Technology Officer. Incumbents of this class do not routinely exercise supervision.

Systems Security Analyst II

Receives supervision from the Chief Innovation and Technology Officer. Incumbents of this class do not routinely exercise supervision.

Senior Systems Security Analyst
Receives general direction from the Chief Innovation and Technology Officer. Exercises technical and functional supervision over professional and technical personnel for assigned projects.

ESSENTIAL FUNCTIONS: *(include but are not limited to the following)*

- Architect, implement, monitor, maintain, and troubleshoot various security systems that protect the City's networks, IT/OT systems (including SCADA), applications and critical infrastructure.
- Design, organize, modify, install, secure and support security infrastructure; and provide technical support for network and security issues associated with enterprise applications.
- Analyze both raw and processed security alerts, logs and event data to identify potential security incidents, threats, mitigations, and vulnerabilities.
- Architect, implement, maintain, and troubleshoot the City's business continuity plan and emergency response plan as it relates to redundant, secure infrastructure.
- Investigate, analyze, produce reports, and remediate security incidents that occur on City systems and applications, both on-premises as well as in the cloud.
- Confirm viable backups, test, maintain and monitor both on-premises and within the cloud.
- Review Cyber Security threat information and assists with mitigating vulnerabilities identified.
- Conduct a variety of Cyber Security policy compliance tasks such as discovering unauthorized devices, conducting site surveys for non-compliance, and ensuring network access requirements are met.
- Perform risk assessments and execute tests of network, backups and information systems to ensure technology processes are secure.
- Facilitate administrator and end-user cyber security training and security awareness programs; track and report on end-user training compliance.
- Facilitates penetration testing of all City systems and infrastructure.
- Ensure systems and procedures are compliant with relevant industry requirements and government regulations (e.g., PCI-DSS, CJIS, NIST, NERC CIP, ISO 27000, etc.).
- Engage in continuous information security training to maintain awareness of changes within the information security field.
- Performs other or related duties as assigned.

PHYSICAL, MENTAL AND ENVIRONMENTAL WORKING CONDITIONS:

Position requires prolonged sitting, standing, walking, reaching, twisting, turning, kneeling, bending, squatting, stooping, and intermittently climbing stairs and/or ladders to rooftops and walking rooftops perimeter in the performance of daily activities. The position also requires grasping, repetitive hand movement and fine coordination in keeping records and preparing reports using a computer keyboard. Additionally, the position requires near and far vision in reading written reports and work-related documents and acute hearing is required when providing phone and personal service. The nature of the work may require the incumbent to lift equipment and materials weighing up to 25 pounds or more.

QUALIFICATIONS:

The following are minimal qualifications necessary for entry into the classification.

Education and/or Experience:

Any combination of education and experience that has provided the knowledge, skills and abilities necessary for a **Systems Security Analyst I/II/Senior**. A typical way of obtaining the required qualifications is to possess the equivalent of:

Systems Security Analyst I
Two years of full-time, paid technical experience in the field of cybersecurity or a closely related field, and a bachelor's degree from an accredited college or university, preferably with major course work in computer science, information technology, cybersecurity, information systems, business management, business information systems, or a related field.

Systems Security Analyst II
Four years of full-time, paid increasingly difficult technical experience in the field of cybersecurity or a closely related field, and a bachelor's degree from an accredited college or university, preferably with major course work in computer science, information technology, cybersecurity, information systems, business management, business information systems, or a related field.

Senior Systems Security Analyst
Six years of full-time, paid increasingly difficult technical experience in the field of cybersecurity or a closely related field, and a bachelor's degree from an accredited college or university, preferably with major course work in computer science, information technology, cybersecurity, information systems, business management, business information systems, or a related field.

License/Certificate
Possession of, or ability to obtain, a valid class C California driver's license.

KNOWLEDGE/SKILLS/ABILITIES: *(The following are a representative sample of the KSAs necessary to perform essential duties of the position. The level and scope of the knowledge and abilities listed below vary between the I and II levels.)*

Knowledge of:

Systems Security Analyst I: Basic concepts of management, configuration, and deployment of next-generation firewalls; basic concepts of network security intrusion detection and prevention; methods for system administration, supporting multiple platforms and applications; client to site and site to site VPN technologies and protocols; security appliance, server, and network hardware configuration, installation, maintenance, and troubleshooting; basic concepts of cyber security incident response; information security standards, compliance mandates, and regulations; application and System Vulnerability Scanning and Mitigation; principles and practices of authenticating users and devices including Active Directory authentication protocols; Public Key Infrastructure (PKI) and secure web server architectures; server and network virtualization technologies including, but not limited to VMWare, Hyper-V, and Software-defined networking; networking protocols, services and operating systems, to include but not limited to, OSI Model, TCP/IP, LDAP, RADIUS, IPSec, HTTP, HTTPS, SSL, SSH, SFTP, SMTP, SMB, SNMP, Windows and Linux; and design techniques, tools, and principles involved in the production of precise technical plans, blueprints, drawings, and models.

Systems Security Analyst II/Senior Systems Security Analyst: All knowledge from the Systems Security Analyst I level, and NIST 800-series cyber security standards, CIS Top-20 Critical Security Controls, Payment Card Industry Data Security Standards (PCI-DSS), and Criminal Justice Information Security (CJIS) requirements; principles and practices of securing cloud-hosted systems and applications; principles and practices of complex operating system design, analysis, and documentation; current hacker techniques, exploits, active defense detection and prevention measures, penetration testing tools, tactics, techniques, and procedures (TTPs); unified threat management (UTM) firewalls and associated components including, but not limited to, URL/Content filtering, file scanning and blocking, DNS sinkholing, and data leakage prevention; endpoint detection and response (EDR) platform deployment, monitoring and management; business continuity planning, documentation, and testing best practices; computer and network forensic tools, techniques and analysis including root cause and comprehensive cause and effect analysis of cyber attacks and breaches; scripting languages (e.g. PowerShell, Python, BASH, etc.) at an expert level; single sign-on, Multi-factor authentication and SAML concepts and applications; eDiscovery processes and techniques for messaging and other social media platforms; network monitoring tools and techniques used to perform security troubleshooting, including packet capture and protocol analysis tools; network routing and switching protocols (i.e., BGP, EIGRP, OSPF, RIP, VLANs, STP, VTP, IOS, NX-OS, HSRP, CDP, and LLDP); principles and practices of project management; file storage technologies, file structures, and file systems; and methods of application integration.

<u>Skill to</u>: Operate an office computer and a variety of word processing and software applications.

<u>Ability to:</u>

Systems Security Analyst I: Perform professional work involving the evaluation, implementation, and daily management of security systems; intermittently analyze work papers, reports and special projects; identify and interpret technical and numerical information; observe and problem solve operational and technical policy and procedures; create accurate network diagrams and detailed technical documentation and reports for designing, planning, and supporting security systems; understand and administer security and separation of duty requirements for enterprise applications and systems; analyze and diagnose security-related issues with networks and systems; maintain and administer security systems and procedures; train or instruct stakeholders in the proper use of security-related applications and procedures; assist with the building and maintenance of security systems and applications; prepare a variety of reports and maintain accurate records and files; maintain confidentiality as necessary; work weekends, evenings or standby, as required; communicate clearly and concisely, both orally and in writing; and establish and maintain effective working relationships.

Systems Security Analyst II/Senior Systems Security Analyst: All abilities from the Systems Security Analyst I level, and independently manage security-related projects, investigations, operations, and incident response; independently perform professional work involving the evaluation, implementation, and daily management of information security systems; implement and maintain compliance with all required information security rules, regulations, mandates, standards, and best practices; design, document, and implement secure network, system, and application architectures; on an ongoing basis, identify and declare observed risks, threats and vulnerabilities and propose practical steps to minimize or mitigate them; participate in, or lead, cross functional teams and meetings; perform and/or work with professional service providers to conduct risk assessments and/or ethical hacking/penetration testing against city systems to determine and mitigate vulnerabilities and other security issues; perform governance tasks, including research, analysis and evaluation, and provide recommendations regarding proposed security, network, and user systems and applications; and conduct various security awareness programs such as citywide cyber security training campaigns, phishing testing, and periodic targeted training initiatives.

FLSA: Exempt
Employee Group: Professional/Administrative, Local 39
Adopted: 01/16/2025