



<b>Job Title</b>	<b>Cyber Security Analyst II</b>	<b>FLSA Status</b>	<b>Exempt</b>
<b>Band</b>	<b>PRO</b>	<b>Probationary Period</b>	<b>12 Months</b>
<b>Zone</b>	<b>9</b>	<b>Job Code</b>	<b>12719</b>

## Class Specification – Cyber Security Analyst II

### **Summary Statement:**

The purpose of this position is to be accountable for the process and procedures to harden City of Colorado Springs IT assets from unauthorized or malicious modification, disclosure, or destruction. This position will provide cyber security operations, analytics, and support by planning, coordinating, integrating, and synchronizing cyber defense and prevention activities throughout IT. This position will monitor and report on IT's and the City's compliance with applicable cyber governance, policy, and controls with a goal of ensuring information availability, protection, and delivery.

### **DISTINGUISHING CHARACTERISTICS:**

This is the full journey level class within the Cyber Security Analyst series. Employees within this class are distinguished from the (I level) by the performance of the full range of duties as assigned. Employees at this level receive only occasional instruction or assistance as new or unusual situations arise, and are fully aware of the operating procedures and policies of the work unit. Positions in this class are flexibly staffed and are normally filled by advancement from level I, or when filled from the outside, have prior experience.

<b>Essential Functions</b>	Note: Regular and predictable attendance is an essential function in the performance of this job.
<b>Time %</b> (All below must add to 100%)	Note: Time spent on each essential function will vary based on operational needs and is only intended to be an approximation over the course of a full year.
30%	Ensure proper IT system and data security is practiced at all times. Triage cyber events, incident response, network analysis, threat detection, trend analysis, vulnerability, and exploit information and resolve advanced vector attacks such as botnets and advanced persistent malware. Cyber requirements analysis, strategic support to operations, and malware analysis. Provide prompt and comprehensive incident response, keeping stakeholders aware of situational awareness. Identify and escalate issues affecting the enterprise operations and defense per process and procedure. Consume and analyze data from cyber organizations; and prepare and deliver situational awareness to IT leadership.
20%	Maintain situational awareness of cyber activity and compliance in the IT industry by reviewing open source reporting for new vulnerabilities, malware, or other threats that



<b>Job Title</b>	<b>Cyber Security Analyst II</b>	<b>FLSA Status</b>	<b>Exempt</b>
<b>Band</b>	<b>PRO</b>	<b>Probationary Period</b>	<b>12 Months</b>
<b>Zone</b>	<b>9</b>	<b>Job Code</b>	<b>12719</b>

	<p>have the potential to impact operations of the City Enterprise or security policies and procedures and recommend appropriate technical changes to maintain security. Monitor security events received through the Security Incident and Event Management (SIEM) or other security tools and perform analysis of log files. Provide incident investigation, handling and documentation; and ensure remediation steps timelines are understood. As an operator, using multiple toolsets, investigate, report, and act (per process and procedure) on suspicious or malicious activity data and/or alerts.</p>
30%	<p>Provide daily and weekly metrics for security and vulnerability incidents. Provide tuning recommendations of policy in security control tools to leadership and tool administrators based on findings during investigations or threat information reviews. Support the development, maintenance, and publishing of City information security policy, process and procedure. Proactively protects the confidentiality, integrity, and availability of City information systems. Report to supervisor regarding the effectiveness of current cyber security measures. Provide support for required industry cyber security audits.</p>
20%	<p>Collaborate with multiple IT teams on the monitoring of intrusion detection tools and procedures to prevent intrusions, hacking, and any other unauthorized or malicious activity. Provide support for the development of City cyber security education programs and awareness of cyber security, risk, controls, and technologies. Log all customer contact (calls, E-Mails, web forms, chat sessions, or voicemails) into the correct ITSM tool. Develop and promote standard operating procedures and the population and use of the Knowledge Management System (KMS).</p>

<p><b>Competencies Required:</b></p>
<p><b>Human Collaboration Skills:</b> Interactions have significant impact and may involve recommendations regarding potential policy development and implementation. Position evaluates customer satisfaction, develops cooperative associations, and utilizes resources to continuously improve customer satisfaction.</p>
<p><b>Reading:</b> Advanced - Ability to read literature, books, reviews, scientific or technical journals, abstracts, financial reports, and/or legal documents. Ordinarily, such education is obtained at the college level or above. However, it may be obtained from experience and self-study.</p>
<p><b>Math:</b> Intermediate - Ability to deal with system of real numbers; practical application of fractions, percentages, ratios/proportions and measurement. Ordinarily, such education is obtained in high</p>



<b>Job Title</b>	Cyber Security Analyst II	<b>FLSA Status</b>	Exempt
<b>Band</b>	PRO	<b>Probationary Period</b>	12 Months
<b>Zone</b>	9	<b>Job Code</b>	12719

school up to college. However, it may be obtained from experience and self-study.

Writing: Intermediate - Ability to write reports, prepare business letters, expositions, and summaries with proper format, punctuation, spelling, and grammar, using all parts of speech. Ordinarily, such education is obtained in high school up to college. However, it may be obtained from experience and self-study.

**Technical Skills Required:**

Advanced Skills and Knowledge: Work requires advanced skills and knowledge in approaches and systems, which affect the engineering, architecture, design and implementation of major programs and/or processes organization-wide. Independent judgment and decision-making abilities are necessary to apply technical skills effectively.

**Relevant Background and Formal Education:** Demonstrated skills, competencies, and knowledge required for this job are most often acquired through the following practical experience and level of academic education and training as suggested below.

Education: Bachelor’s degree from an accredited college or university with major coursework in computer science, information systems, or a related field.

Experience: Three years of full-time work experience in a Cyber Security Analyst role or Cyber Security support role.

**Education and Experience Equivalency:**

One (1) year of the appropriate type and level of experience may be substituted for each required year of post-high school education.

Additional appropriate education may be substituted for the minimum experience requirements.

**Certifications and Licenses:** Must possess or be able to acquire the following certifications and/or licenses.

Certifications required in accordance with standards established by departmental policy.

**Supervision Exercised:**

Work requires the occasional direction of helpers, assistants, seasonal employees, interns, or temporary employees.

**Supervision Received:**



<b>Job Title</b>	Cyber Security Analyst II	<b>FLSA Status</b>	Exempt
<b>Band</b>	PRO	<b>Probationary Period</b>	12 Months
<b>Zone</b>	9	<b>Job Code</b>	12719

Receives General Direction: This job title normally performs the job by following established standard operating procedures and/or policies. There is a choice of the appropriate procedure or policy to apply to duties. Performance reviewed periodically.

**Fiscal Responsibility:**

The job title has no budgetary/ fiscal responsibility.

**Physical Demands:**

Exerting up to 10 lbs. occasionally or negligible weights frequently; sitting most of the time.

<b>Environmental Conditions</b>	<b>Frequency</b>
Primary Work Environment	Office Environment
Extreme Temperature	Never
Wetness and Humidity	Never
Respiratory Hazards	Never
Noise and Vibrations	Never
Physical Hazards	Never
Mechanical and/or Electrical Hazards	Occasionally
Exposure to Communicable Diseases	Never

**Machines, Tools, Equipment, and Work Aids:** Computer, printer, copier, telephone, and standard office equipment.

**Specialized Computer Equipment and Software:** Microsoft Office.

*The description above is intended to represent only the key areas of responsibilities; specific job assignments, duties, and environmental conditions will vary depending on the business need of the department and the particular assignment.*

Original Date: December 2016