



# Cybersecurity Analyst I

Salary Group: B25

Class Code: 0320

<u>CLASS TITLE</u>	<u>CLASS CODE</u>	<u>SALARY GROUP</u>	<u>SALARY RANGE</u>
CYBERSECURITY ANALYST I	0320	B25	\$63,104 - \$103,491
CYBERSECURITY ANALYST II	0322	B27	\$76,356 - \$129,137
CYBERSECURITY ANALYST III	0324	B29	\$92,390 - \$156,256

## GENERAL DESCRIPTION

Performs complex (journey-level) cybersecurity analysis work. Work involves protecting cybersecurity assets and delivering cybersecurity incident detection, incident response, threat assessment, cyber intelligence, software security, and vulnerability assessment services. May provide guidance to others. Works under general supervision, with moderate latitude for the use of initiative and independent judgment.

## EXAMPLES OF WORK PERFORMED

Monitors and analyzes cybersecurity alerts from cybersecurity tools, network devices, and information systems.

Monitors and maintains cybersecurity infrastructure and/or policies and procedures to protect information systems from unauthorized use.

Designs, develops, modifies, tests, and integrates database or computer hardware systems to protect against cyber threats.

Performs cybersecurity incident detection, analysis, and prevention.

Performs vulnerability scans of networks and applications to assess effectiveness and identify weaknesses.

Performs forensic analysis of information systems and portable devices and forensic recovery of data using assessment tools.

Researches and analyzes cybersecurity threat indicators and their behaviors, and recommends threat mitigation strategies.

Delivers cybersecurity awareness training.

May provide guidance to others.

Performs related work as assigned.

## **GENERAL QUALIFICATION GUIDELINES**

### **EXPERIENCE AND EDUCATION**

Experience in cybersecurity analysis, information security analysis, or digital forensics. Graduation from an accredited four-year college or university with major coursework in cybersecurity, information technology security, computer engineering, computer information systems, computer science, management information systems, or a related field is generally preferred. Education and experience may be substituted for one another.

### **KNOWLEDGE, SKILLS, AND ABILITIES**

Knowledge of the limitations and capabilities of computer systems and technology; of operational support of networks, operating systems, Internet technologies, databases, and security infrastructure; of cybersecurity and information security controls, practices, procedures, and regulations; and of incident response program practices and procedures.

Skill in the use of a computer and applicable software; and in configuring, deploying, and monitoring security infrastructure.

Ability to resolve complex security issues in diverse and decentralized environments; to plan, develop, monitor, and maintain cybersecurity and information technology security processes and controls; to communicate effectively; and to provide guidance to others.