



Cybersecurity Analyst II

Salary Group: B27

Class Code: 0322

<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 advanced (senior-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 supervise the work of others. Works under limited supervision, with considerable latitude for the use of initiative and independent judgment.

DISTINGUISHING CHARACTERISTICS

The Cybersecurity Analyst job classification series is a subset of information security, which focuses on protecting data from cyber-related attacks. Employees typically monitor for any trace of invasion or improper access of data by performing threat and incident detection, incident response, and forensics activities. In contrast, the Information Security Analyst job classification series does not focus only on protecting data from cyber-related attacks; rather, employees in that series are responsible for protecting information throughout the business process. Employees typically perform governance, risk assessments, and compliance, which involves developing and documenting system security plans, policy development, and process analysis.

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.

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.

Defines plans; organizes designs; and develops, modifies, tests, and integrates database or computer hardware systems to protect against cyber threats.

Reviews, develops, and delivers cybersecurity awareness training.

Researches and implements new security risk and mitigation strategies, tools, techniques, and solutions for the prevention, detection, containment, and correction of data security breaches.

Assists in advising management and users regarding security procedures.

May occasionally manage multiple projects.

May supervise the work of 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; operational support of networks, operating systems, Internet technologies, databases, and security infrastructure; cybersecurity and information security controls, practices, procedures, and regulations; and incident response program practices and procedures.

Skill in the use of a computer and applicable software; and in the 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 supervise the work of others.