Cybersecurity Analyst

CLASS TITLE	CLASS CODE	SALARY GROUP	SALARY RANGE
CYBERSECURITY ANALYST I	0319	B23	$58,184 - $94,913
CYBERSECURITY ANALYST II	0320	B25	$66,259 - $108,666
CYBERSECURITY ANALYST III	0321	B27	$80,174 - $135,594
CYBERSECURITY ANALYST IV	0322	B29	$97,010 - $164,069
CYBERSECURITY ANALYST V	0323	B31	$117,383 - $198,522

GENERAL DESCRIPTION

Performs information security and cybersecurity analysis work involving planning, implementing, and monitoring security measures for the protection of information systems and infrastructure. Work also includes protecting cybersecurity assets and delivering cybersecurity incident detection, incident response, threat assessment, cyber intelligence, software security, and vulnerability assessment services.

EXAMPLES OF WORK PERFORMED

Performs technical risk assessments and reviews of account permissions, computer data access needs, security violations, programming changes, and new and existing applications and systems, including data center physical security and environment.

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.

Monitors systems and procedures to protect data systems and databases from unauthorized access.

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

Supports the implementation of computer system security plans with agency personnel and outside vendors.

Develops plans to safeguard computer configuration and data files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.

Modifies and monitors computer configuration and data files to incorporate new software and virus protection systems, correct errors, or change individual access status.

Implements continuous automated security compliance capabilities.

Researches and analyzes cybersecurity threat indicators and their behaviors for the prevention, detection, containment, and correction of data security breaches, and recommends threat mitigation strategies.

Trains users and promotes security awareness to ensure system security and improve application, server, and network efficiency.

Performs related work as assigned.

DESCRIPTION OF LEVELS

Examples of work and descriptions are meant to progress through the levels. For example, an employee at level V may also perform work listed within the previous levels.

***Note**: Factors that may distinguish between journey levels include the level of independence in performing the work and the complexity of the work and may include the years of related experience and education. Employees at the journey levels may independently perform the full range of work listed in the examples or may assist others in that work.*

CYBERSECURITY ANALYST I (Merged IT Security Analyst with this series 9-1-2023): Performs moderately complex (journey-level) information security and cybersecurity analysis work. Works under general supervision, with moderate latitude for the use of initiative and independent judgment. Employees at this level may rely on direction from others to solve problems that are not standard. Employees may also assist other staff in performing work of greater complexity.

CYBERSECURITY ANALYST II: Performs complex (journey-level) information security and cybersecurity analysis work. Works under general supervision, with limited latitude for the use of initiative and independent judgment**.** Employees at this level may work more independently than those at the previous levels and may routinely assist other staff in performing work of greater complexity. Employees may:

- Develop plans to safeguard computer configuration and data files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Coordinate agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.
- Design, develop, modify, test, and integrate database or computer hardware systems to protect against cyber threats.
- Design, automate, manage, and deploy security applications and infrastructure program activities.

- Participate in the development of information technology disaster recovery and business continuity planning.

***Note**: A senior-level employee (levels III-V) may serve as a team lead or supervisor; however, supervisory responsibilities within this job classification series will normally be found at levels IV and V.*

A senior-level employee may perform the full range of work identified in the preceding levels and may coordinate, evaluate, or oversee that work for others. Factors that may distinguish between senior levels include the scope of responsibility and oversight, the size and complexity of information security and cybersecurity duties, and the employee's related experience, education, and certifications. Other factors may include the type, nature, scope, and complexity of the assigned project.

CYBERSECURITY ANALYST III: Performs highly complex (senior-level) information security and cybersecurity analysis work. Works under limited supervision, with considerable latitude for the use of initiative and independent judgment. Employees at this level may research and implement new security risk and mitigation strategies, tools, techniques, and solutions for the prevention, detection, containment, and correction of data security breaches.

CYBERSECURITY ANALYST IV: Performs advanced (senior-level) information security and cybersecurity analysis work. Works under limited supervision, with considerable latitude for the use of initiative and independent judgment. Employees at this level may independently perform the most complex information security and cybersecurity work and advise management and users regarding security configurations and procedures.

CYBERSECURITY ANALYST V (Added 9-1-2023): Performs highly advanced (senior-level) information security and cybersecurity analysis work. Works under minimal supervision, with extensive latitude for the use of initiative and independent judgment. Employees at this level may be considered technical experts in the field and may occasionally manage multiple projects, and/or some of the most complex information security and cybersecurity projects.

GENERAL QUALIFICATION GUIDELINES

EXPERIENCE AND EDUCATION

Experience and/or education in a field relevant to the work being performed. Agencies have the discretion to identify the general or specialized experience, education, or certifications required for positions and may tailor qualification requirements to be specific and meet the agency's business needs. Agencies also may substitute experience and education for one another, if appropriate and allowed by statute.

KNOWLEDGE, SKILLS, AND ABILITIES

For all levels

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

- Skill in the use of applicable software and the configuring, deploying, monitoring, and automating of security applications and 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; and to communicate effectively.

Additional for Cybersecurity III - V levels

- Ability to oversee and/or supervise the work of others.