Information Security Analyst II

Salary Group: B25
Class Code: 0236

CLASS TITLE	CLASS CODE	SALARY GROUP	SALARY RANGE
INFORMATION SECURITY ANALYST I	0235	B23	$55,184 - $90,393
INFORMATION SECURITY ANALYST II	**0236**	**B25**	**$63,104 - $103,491**
INFORMATION SECURITY ANALYST III	0237	B27	$76,356 - $129,137

GENERAL DESCRIPTION

Performs highly complex (senior-level) information security analysis work. Work involves coordinating and/or planning, implementing, and monitoring security measures for the protection of information systems and infrastructure. May supervise the work of others. Works under limited supervision, with considerable latitude for the use of initiative and independent judgment.

DISTINGUISHING CHARACTERISTICS

The Information Security Analyst job classification series is intended for employees responsible for protecting information throughout the agency. Employees typically perform governance, risk assessments, and compliance, which involves developing and documenting system security plans, developing policy, and performing process analysis. In contrast, the Cybersecurity Analyst job classification series is a subset of information security, which focuses on protecting data from cyber-related attacks. Employees in that series monitor for any trace of invasion or improper access of data by performing threat and incident detection, incident response, and forensics activities.

EXAMPLES OF WORK PERFORMED

Coordinates and/or implements computer system security plans with agency personnel and outside vendors.

Coordinates agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.

Advises management and users regarding security configurations and procedures.

Designs, automates, manages, and deploys security applications and infrastructure program activities.

Develops and recommends plans to safeguard computer configurations 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.

Plans and deploys continuous automated security compliance capabilities.

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

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

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

Researches, evaluates, and recommends systems and procedures for the prevention, detection, containment, and correction of data security breaches.

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

May supervise the work of others.

Performs related work as assigned.

GENERAL QUALIFICATION GUIDELINES

EXPERIENCE AND EDUCATION

Experience in information security analysis work. Graduation from an accredited four-year college or university with major coursework in information technology security, 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; technology across all mainstream network, operating system, and application platforms; operational support of networks, operating systems, Internet technologies, databases, and security applications; and information security practices, procedures, and regulations.

Skill in the use of computers and 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 learn new information and security technologies, to communicate effectively, and to supervise the work of others.