

**Information Security Analyst III**

Salary Group: B27

Class Code: 0237

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

**GENERAL DESCRIPTION**

Performs advanced (senior-level) information security analysis work. Work involves overseeing and/or planning, implementing, and monitoring security measures for the protection of information systems and infrastructure. May supervise the work of others. Works under minimal supervision, with extensive 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**

Oversees and/or performs the design, automation, and deployment of security applications and infrastructure program activities.

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

Develops and/or coordinates the development of agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.

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

Develops information technology disaster recovery and business continuity planning.

Advises management and users regarding security configurations and procedures.

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.

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

Designs and plans deployment of continuous automated security compliance capabilities.

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

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 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, communicate, and teach new information and security technologies; to communicate effectively; and to supervise the work of others.