Cybersecurity Officer

Salary Group: B30
Class Code: 0326

CLASS TITLE	CLASS CODE	SALARY GROUP	SALARY RANGE
CYBERSECURITY OFFICER	**0326**	**B30**	**$101,630 - $171,881**
CHIEF CYBERSECURITY OFFICER	0328	B31	$111,793 - $189,069

GENERAL DESCRIPTION

Performs highly advanced and/or supervisory (senior-level) cybersecurity analysis work providing direction and guidance in strategic operations and planning. Work involves overseeing cybersecurity programs and environments; the prevention, detection and remediation of cybersecurity threats and intrusions; cybersecurity policies and monitoring protocols; and leading the development of a security plan, with an emphasis on technical infrastructure and long-term risk mitigation. May supervise the work of others. Works under minimal supervision, with extensive latitude for the use of initiative and independent judgment.

DISTINGUISHING CHARACTERISTICS

The Cybersecurity Officer job classification series is intended for employees that oversee the prevention of data breaches and the monitoring of and reacting to cyber-related attacks. Employees typically direct the analysis and assessment of vulnerabilities in the infrastructure, investigate available tools and countermeasures to remedy the detected vulnerabilities, and recommend solutions and best practices. In contrast, the Information Security Officer job classification series is intended for employees that direct and determine enterprise-wide information security standards. Those employees typically develop and implement information security standards and procedures, ensuring that all information systems are functional and secure.

EXAMPLES OF WORK PERFORMED

Directs the deployment of cybersecurity infrastructure and protects critical infrastructure services.

Directs and/or conducts research related to cybersecurity trends and technology; and evaluates cybersecurity trends, tools, and techniques for potential application to infrastructure and research areas.

Oversees cybersecurity management initiatives.

Oversees detection activities and advises on cybersecurity threats and vulnerabilities.

Oversees the initiation, implementation, and development of incident response plans and recovery programs; the evaluation and obtainment of forensics tools; the review of intrusion and misuse detection reports; and the guidance for corrective action.

Develops and implements appropriate safeguards to ensure system resiliency.

Develops cybersecurity awareness training programs for employees, contractors, and users; and facilitates cyber preparedness exercises.

Represents the agency at business meetings, hearings, trials, legislative sessions, conferences, and seminars or on boards, panels, and committees.

May supervise the work of others.

Performs related work as assigned.

GENERAL QUALIFICATION GUIDELINES

EXPERIENCE AND EDUCATION

Experience in cybersecurity analysis work, with emphasis on security operations, incident management, intrusion detection, firewall deployment, and security event analysis. 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. Experience and education may be substituted for one another.

KNOWLEDGE, SKILLS, AND ABILITIES

Knowledge of local, state, and federal laws and regulations relevant to cybersecurity, privacy, and computer crime; the principles and practices of public administration and management; the limitations and capabilities of computer systems; technology across all network layers and computer platforms; operational support of networks, operating systems, Internet technologies, databases, and security applications; cybersecurity controls, procedures, and regulations; and incident response program practices and procedures.

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

Ability to manage and oversee the development, monitoring, and maintenance of cybersecurity processes and controls; to identify problems, evaluate alternatives, and implement effective solutions; to develop and evaluate policies and procedures; to prepare reports; to implement cybersecurity best practices and awareness; to communicate effectively; and to supervise the work of others.

REGISTRATION, CERTIFICATION, OR LICENSURE

May require certification as a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), or Certified in Risk and Information Systems Control (CRISC).