Information Systems Security Developer

NICE Framework Reference	Securely Provision, SP-SYS-001, Information Systems Security Developer
Functional Description	Develops, creates, integrates, tests, and maintains information system security throughout the systems life cycle, and reports on information system performance in providing confidentiality, integrity, and availability and recommends corrective action to address deficiencies.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is an entry level role in cybersecurity that leverages previous IT and systems experience, following cybersecurity technical training, this work can lead to increased responsibilities in cybersecurity infrastructure roles and technical expertise.
Other titles	IT Security Systems Administrator Cybersecurity systems technician
Related NOCs	2171 Information systems analysts and consultants 2174 Computer programmers and interactive media developers
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Define and review an organization's information systems, and ensure security requirements recognize appropriate disaster recovery plans and business continuity functions, including any failover or backup requirements for system restoration ▪ Analyze existing security systems and make recommendations for changes or improvements ▪ Prepare cost estimates and constraints, and identify integration issues or risks to organization ▪ Research and develop a system security context, and define security assurance requirements based on industry standards and cybersecurity policies and practices ▪ Ensure the acquired or developed systems are consistent with an organization's cybersecurity policies and practices ▪ Develop and conduct information system testing and validation procedures and report on functionality and resiliency ▪ Plan and support vulnerability testing and security reviews on information systems or networks to identify gaps, and examine controls and measures required to protect the confidentiality and integrity of information under different operating conditions ▪ Conduct trial runs of information systems to ensure security levels and procedures are correct and develop a security risk management plan; ▪ Support development of disaster recovery and continuity of operations plans for information systems under development ▪ Prepare technical reports that document system development process and subsequent revisions

	▪ Document and address security throughout a system life cycle; ▪ Update and upgrade information systems as needed to correct errors, and to improve performance and interfaces ▪ Prepare reports on information systems patches or releases that would leave networks or systems vulnerable ▪ Develop countermeasures and risk mitigation strategies against potential exploitations of vulnerabilities in networks or systems ▪ Perform risk analysis whenever a system undergoes a change ▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role	
Required qualifications	Education	Post-secondary education in a cyber or IT related field (e.g., Computer Science, IT systems administration, Computer Engineering or equivalent).
	Training	Supporting training can include cybersecurity systems development tools, techniques and practices as well as Security throughout the system development lifecycle
	Work experience	Previous training and experience in system development.
Tools & Technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks, ▪ Cybersecurity risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems	
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Basic application of the following KSAs: ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Risk management policies, requirements, and practices; ☐ Business continuity and disaster response planning; ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management ☐ Costing models and cost benefit analysis ☐ Cryptography and cryptographic key management concepts; ☐ Identity and access management ☐ Vulnerability management and penetration testing planning and processes ☐ Data security conceptions and functions, analysis methodologies, testing, and protocols ☐ Secure coding and configuration techniques ☐ Cybersecurity program management, measures and monitoring	

	Advanced application of the following KSAs: ☐ Industry standards and organizationally accepted system analysis principles and methods ☐ System design tools, methods, and techniques ☐ Computer architecture, data structures, and algorithms ☐ System life cycle management principles, including software security and usability ☐ System testing and evaluation methodologies and processes; ☐ System, application and data security threats, risks and vulnerabilities; ☐ Designing countermeasures to identified security risks; ☐ Configuring and using software-based computer protection tools ☐ Considerations for designing and hardware and software solutions ☐ Incident management and system recovery
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities and system to system interactions, access and accountabilities. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks throughout the system development life-cycle. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required, and system security responses developed and exercised. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization and across all systems that handle sensitive data.