CAREER PATHWAY SYSTEMS DEVELOPER (632)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 632-SYSTEMS DEVELOPER

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 632-Systems Developer.

Table 1. 632-Systems Developer Work Role Overview

NICE Role Description	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
OPM Occupational Series	Personnel performing the 632-Systems Developer work role are most commonly aligned to the following Occupational Series: (Top 5 Shown) - 2210 – Information Technology – 43% - 855 – Electronics Engineering – 23% - 801 – General Engineering – 12% - 1550 – Computer Science – 11% - 854 – Computer Engineering – 5%
Work Role Pairings	Personnel performing the 632- Systems Developer work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 622-Secure Software Assessor - 32% - 641-Systems Requirements Planner - 17% - 621-Software Developer - 17% - 651-Enterprise Architect - 9% - 671-System Testing and Evaluation Specialist - 5%
Functional Titles	Personnel performing the 632-Systems Developer work role may unofficially or alternatively be called: - Database Developer - DevOps Engineer - Information Assurance (IA) Developer - Information Assurance (IA) Engineer - Information Systems Security Engineer - Systems Engineer - System Integration Engineer - Systems Security Engineer
Distribution of GS-Levels	Personnel performing the 632-Systems Developer are most commonly found within the following grades on the General Schedule. * - ☐ GS-5 – redacted**

	- ☐ GS-6 – redacted** - ☐ GS-7 – redacted** - ☐ GS-8 – redacted** - ☐ GS-9 – redacted** - ☐ GS-10 – redacted** - ☐ GS-11 – redacted** - ☒ GS-12 – 11% - ☒ GS-13 – 23% - ☒ GS-14 – 6% - ☐ GS-15 – redacted** *54% of all 632s are in non-GS pay plans and excluded from this section **percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 632-Systems Developer work role: - 422-Data Analyst - 441-Network Operations Specialist - 621-Software Developer - 641-Systems Requirements Planner - 671-System Testing and Evaluation Specialist
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 632-Systems Developer. This is not an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles: - 422-Data Analyst - 631-Information Systems Security Developer - 641-Systems Requirements Planner - 651-Enterprise Architect - 652-Security Architect - 661-Research and Development Specialist - 671-System Testing and Evaluation Specialist *Note: Leveraging the knowledge, skills, abilities, and tasks of the 632-Systems Developer work role, individuals may prepare themselves to transition into one or more of the following cross-functional work roles: - *711- Cyber Instructional Curriculum Developer* - *712-Cyber Instructor* - *732-Privacy Compliance Manager / Officer* - *751-Cyber Workforce Developer and Manager* - *752-Cyber Policy and Strategy Planner*

	- *802-IT Project Manager* - *803-Product Support Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 632-Systems Developer work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 632-Systems Developer Core Tasks

Task ID	Task Description	Core or Additional
T0560	Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	Core
T0447	Design hardware, operating systems, and software applications to adequately address requirements.	Core
T0464	Develop detailed design documentation for component and interface specifications to support system design and development.	Core
T0406	Ensure design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.	Core
T0488	Implement designs for new or existing system(s).	Core
T0012	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider lifecycle support.	Additional
T0558	Analyze user needs and requirements to plan and conduct system development.	Additional
T0021	Build, test, and modify product prototypes using working models or theoretical models.	Additional
T0350	Conduct a market analysis to identify, assess, and recommend commercial, GOTS, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	Additional
T0053	Design and develop cybersecurity or cybersecurity-enabled products.	Additional
T0358	Design and develop system administration and management functionality for privileged access users.	Additional
T0056	Design or integrate appropriate data backup capabilities into overall system designs, and ensure appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Additional
T0449	Design to security requirements to ensure requirements are met for all systems and/or applications.	Additional
T0359	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Additional
T0061	Develop and direct system testing and validation procedures and documentation.	Additional
T0067	Develop architectures or system components consistent with technical specifications.	Additional
T0559	Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.	Additional
T0070	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Additional

Task ID	Task Description	Core or Additional
T0466	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Additional
T0326	Employ configuration management processes.	Additional
T0107	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Additional
T0109	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Additional
T0480	Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.	Additional
T0119	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	Additional
T0304	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Additional
T0378	Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle).	Additional
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Additional
T0518	Perform security reviews and identify security gaps in architecture.	Additional
T0201	Provide guidelines for implementing developed systems to customers or installation teams.	Additional
T0528	Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials	Additional
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Additional
T0538	Provide support to test and evaluation activities.	Additional
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Additional
T0541	Trace system requirements to design components and perform gap analysis.	Additional
T0242	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Additional
T0544	Verify stability, interoperability, portability, and/or scalability of system architecture.	Additional

1.3 CORE KNOWLEDGE, SKILLS, AND ABILITIES

The table below provides a ranking of KSAs that represent the Core, or baseline, expectations for performance in the 632-Systems Developer work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 632-Systems Developer Core KSAs

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to All Work Roles
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to All Work Roles
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence	Foundational to All Work Roles
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to All Work Roles
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
K0322	Knowledge of embedded systems.	Infrastructure Design	Core
S0031	Skill in developing and applying security system access controls.	Identity Management	Core
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance	Core
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/ Network Security	Core
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/ Network Security	Core
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development	Core
K0082	Knowledge of software engineering.	Software Development	Core
K0227	Knowledge of various types of computer architectures.	System Administration	Core
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration	Core
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration	Core
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration	Core

KSA ID	Description	Competency	Importance to Work Role
K0102	Knowledge of the systems engineering process.	Systems Integration	Core
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation	Core
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation	Core
K0032	Knowledge of resiliency and redundancy.	Business Continuity	Additional
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages	Additional
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages	Additional
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense	Additional
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	Computer Network Defense	Additional
K0055	Knowledge of microprocessors.	Computers and Electronics	Additional
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).	Computers and Electronics	Additional
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161).	Contracting/Procurement	Additional
K0066	Knowledge of Privacy Impact Assessments.	Data Privacy and Protection	Additional
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Additional
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection	Additional
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection	Additional
K0024	Knowledge of database systems.	Database Management Systems	Additional
K0018	Knowledge of encryption algorithms.	Encryption	Additional
K0308	Knowledge of cryptology.	Encryption	Additional
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture	Additional
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture	Additional
K0067	Knowledge of process engineering concepts.	Enterprise Architecture	Additional
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management	Additional

KSA ID	Description	Competency	Importance to Work Role
K0065	Knowledge of policy-based and risk adaptive access controls.	Identity Management	Additional
K0336	Knowledge of access authentication methods.	Identity Management	Additional
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance	Additional
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Additional
K0276	Knowledge of security management.	Information Systems/ Network Security	Additional
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/ Network Security	Additional
S0097	Skill in applying security controls.	Information Systems/ Network Security	Additional
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/ Network Security	Additional
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment	Additional
S0146	Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU specifications).	Information Technology Assessment	Additional
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment	Additional
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design	Additional
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design	Additional
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design	Additional

KSA ID	Description	Competency	Importance to Work Role
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Additional
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design	Additional
K0015	Knowledge of computer algorithms.	Mathematical Reasoning	Additional
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning	Additional
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	Mathematical Reasoning	Additional
S0160	Skill in the use of design modeling (e.g., unified modeling language).	Modeling and Simulation	Additional
K0207	Knowledge of circuit analysis.	Network Management	Additional
S0136	Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management	Additional
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management	Additional
K0060	Knowledge of operating systems.	Operating Systems	Additional
S0145	Skill in integrating and applying policies that meet system security objectives.	Policy Management	Additional
S0018	Skill in creating policies that reflect system security objectives.	Policy Management	Additional
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management	Additional
K0084	Knowledge of structured analysis principles and methods.	Risk Management	Additional
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration	Additional
K0036	Knowledge of human-computer interaction principles.	Systems Integration	Additional
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Systems Integration	Additional
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration	Additional
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness	Additional

KSA ID	Description	Competency	Importance to Work Role
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).	Telecommunications	Additional
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis	Additional
K0297	Knowledge of countermeasure design for identified security risks.	Threat Analysis	Additional
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 632-Systems Developer work role, and their associated importance. Listed competencies are collections of three or more similar Knowledge, Skills, or Abilities aligned to the Work Role. *These competencies originate from the NICE Framework Competency Pivot Tool.*

Table 4. 632-Systems Developer Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Data Privacy and Protection	C014	This area contains KSAs that relate to the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them	• Knowledge of Privacy Impact Assessments. (K0066) • Knowledge of Personally Identifiable Information (PII) data security standards. (K0260) • Knowledge of Payment Card Industry (PCI) data security standards. (K0261) • Knowledge of Personal Health Information (PHI) data security standards. (K0262)	Core
Identity Management	C020	This area contains KSAs that relate to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons"	• Skill in developing and applying security system access controls. (S0031) • Knowledge of policy-based and risk adaptive access controls. (K0065) • Knowledge of access authentication methods. (K0336) • Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). (K0056)	Core
Information Assurance	C022	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	• Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). (K0203) • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (A0123) • Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (S0367) • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (K0044) • Knowledge of organization's enterprise information security architecture. (K0027)	Core
Information Systems/ Network Security	C024	This area contains KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore	• Knowledge of cybersecurity and privacy principles. (K0004) • Skill in applying security controls. (S0097) • Knowledge of security management. (K0276) • Knowledge of information security systems engineering principles (NIST SP 800-160). (K0045) • Skill in discerning the protection needs (i.e., security controls) of information systems and networks. (S0034)	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
		security of information systems and network services.	• Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). (K0049) • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). (K0179)	
Infrastructure Design	C026	This area contains KSAs that relate to the architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.	• Knowledge of computer networking concepts and protocols, and network security methodologies. (K0001) • Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs. (K0333) • Knowledge of local area and wide area networking principles and concepts including bandwidth management. (K0050) • Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. (K0170) • Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. (K0332) • Knowledge of embedded systems. (K0322) • Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). (K0061)	Core
Systems Integration	C049	This area contains KSAs that relate to the principles, methods, and procedures for installing, integrating, and optimizing information systems components.	• Knowledge of human-computer interaction principles. (K0036) • Knowledge of the systems engineering process. (K0102) • Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design. (K0087) • Knowledge of installation, integration, and optimization of system components. (K0035) • Skill in designing the integration of hardware and software solutions. (S0024) • Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools. (K0086) • Knowledge of system life cycle management principles, including software security and usability. (K0090)	Core
Network Management	C033	This area contains KSAs that relate to the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.	• Knowledge of circuit analysis. (K0207) • Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. (S0136) • Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. (K0180)	Additional

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Risk Management	C044	This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.	• Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. (K0169) • Knowledge of structured analysis principles and methods. (K0084) • Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). (K0002)	Additional
Enterprise Architecture	C018	This area contains KSAs that relate to the principles, concepts, and methods of enterprise architecture to align information technology (IT) strategy, plans, and systems with the mission, goals, structure, and processes of the organization.	• Knowledge of parallel and distributed computing concepts. (K0063) • Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). (K0200) • Knowledge of process engineering concepts. (K0067)	Additional
Information Technology Assessment	C025	This area contains KSAs that relate to the principles, methods, and tools (for example, surveys, system performance measures) to assess the effectiveness and practicality of information technology systems.	• Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations. (A0170) • Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU specifications). (S0018) • Skill in conducting audits or reviews of technical systems. (S0085)	Additional
Mathematical Reasoning	C031	This area contains KSAs that relate to devising strategies to solve a wide variety of math problems and determine if an assertion is correct.	• Knowledge of computer algorithms. (K0015) • Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). (K0052) • Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression). (K0325)	Additional
Vulnerabilities Assessment	C057	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Knowledge of cyber threats and vulnerabilities. (K0005) • Skill in evaluating the adequacy of security designs. (S0036) • Knowledge of specific operational impacts of cybersecurity lapses. (K0006)	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 632-Systems Developer Suggested Qualifications / Capability Indicators

For indicators of capability for the 632-Systems Developer work role, please see Draft NISTR 8193 - National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators.

Section to be populated with updated DoD-8140 Qualification Matrix for 632-Systems Developer.

2 APPENDIX: 632-SYSTEMS DEVELOPER TASK ANALYSIS AND KSA MAPPING

2.1 KEY TO READING THE TASK ANALYSIS AND KSA MAPPING

Table 6. Key to Reading the Task Analysis and KSA Mapping

Proficiency	Task Statement	Importance
As Written	Task as written within the NICE Cybersecurity Workforce Framework (NICE Framework).	Overall Importance to Work Role
Entry	*Example behavioral indicator / task permutation for performing this task at an Entry skills proficiency level.*	
Intermediate	*Example behavioral indicator / task permutation for performing this task at an Intermediate skills proficiency level.*	
Advanced	*Example behavioral indicator / task permutation for performing this task at an Advanced skills proficiency level.*	

Table 7. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
ID of K, S, or A	Knowledge, Skill or Ability needed to perform the task as written within the NICE Framework	Competency mapped to the individual K, S, or A.

2.2 632-SYSTEMS DEVELOPER TASK ANALYSIS AND KSA MAPPING

Table 8. T0560 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	Core
Entry	*Collaborate with peers and teams on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).*	
Intermediate	*Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).*	
Advanced	*Collaborate with senior leaders on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).*	

Table 9. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	Computer Network Defense
S0031	Skill in developing and applying security system access controls.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security

KSA ID	Description	Competency
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0097	Skill in applying security controls.	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 10. T0447 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design hardware, operating systems, and software applications to adequately address requirements.	Core
Entry	*Help with designing hardware, operating systems, and software applications to adequately address requirements.*	
Intermediate	*Design routine hardware, operating systems, and software applications to adequately address requirements.*	
Advanced	*Oversee the design of hardware, operating systems, and software applications to adequately address requirements.*	

Table 11. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0015	Knowledge of computer algorithms.	Mathematical Reasoning
K0024	Knowledge of database systems.	Database Management Systems
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0060	Knowledge of operating systems.	Operating Systems
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0082	Knowledge of software engineering.	Software Development
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security

KSA ID	Description	Competency
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness
K0227	Knowledge of various types of computer architectures.	System Administration
K0308	Knowledge of cryptology.	Encryption
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0336	Knowledge of access authentication methods.	Identity Management
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
S0031	Skill in developing and applying security system access controls.	Identity Management
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance

Table 12. T0464 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop detailed design documentation for component and interface specifications to support system design and development.	Core
Entry	*Help with developing detailed design documentation for component and interface specifications to support system design and development.*	
Intermediate	*Develop detailed design documentation for component and interface specifications to support system design and development.*	
Advanced	*Oversee the development of detailed design documentation for component and interface specifications to support system design and development.*	

Table 13. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0336	Knowledge of access authentication methods.	Identity Management
S0031	Skill in developing and applying security system access controls.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security

KSA ID	Description	Competency
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0097	Skill in applying security controls.	Information Systems/Network Security
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0060	Knowledge of operating systems.	Operating Systems
S0145	Skill in integrating and applying policies that meet system security objectives.	Policy Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0082	Knowledge of software engineering.	Software Development
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0102	Knowledge of the systems engineering process.	Systems Integration
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 14. T0406 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.	Core
Entry	*Help to ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.*	
Intermediate	*Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.*	
Advanced	*Oversee all efforts to ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.*	

Table 15. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0067	Knowledge of process engineering concepts.	Enterprise Architecture
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0082	Knowledge of software engineering.	Software Development
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
K0102	Knowledge of the systems engineering process.	Systems Integration
K0276	Knowledge of security management.	Information Systems/Network Security
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment

Table 16. T0488 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Implement designs for new or existing system(s).	Core
Entry	*Assist with the implementation of designs for new or existing system(s).*	
Intermediate	*Implement routine designs for new or existing system(s).*	
Advanced	*Oversee the implementation of designs for new or existing system(s).*	

Table 17. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0024	Knowledge of database systems.	Database Management Systems
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0060	Knowledge of operating systems.	Operating Systems
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0066	Knowledge of Privacy Impact Assessments.	Data Privacy and Protection
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness
K0227	Knowledge of various types of computer architectures.	System Administration

KSA ID	Description	Competency
K0276	Knowledge of security management.	Information Systems/Network Security
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0336	Knowledge of access authentication methods.	Identity Management
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
S0097	Skill in applying security controls.	Information Systems/Network Security
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment