CAREER PATHWAY RESEARCH & DEVELOPMENT SPECIALIST (661)

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

November 2020

Table of Contents

1 661-RESEARCH AND DEVELOPMENT SPECIALIST

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 661- Research and Development Specialist.

Table 1. 661-Research and Development Specialist Work Role Overview

NICE Role Description	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
OPM Occupational Series	Personnel performing the 661-Research and Development Specialist work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 1550-Computer Science – 37% - 0855-Electronics Engineering – 16% - 2210-Information Technology – 16% - 0830-Mechanical Engineering – 6% - 0854-Computer Engineering – 6%
Work Role Pairings	Personnel performing the 661-Research and Development Specialist work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 651-Enterprise Architect – 17% - 671-System Testing and Evaluation Specialist – 11% - 621-Software Developer – 9% - 422-Data Analyst – 8% - 801-Program Manager – 8%
Functional Titles	Personnel performing the 661-Research and Development Specialist work role may unofficially or alternatively be called: - Capabilities and Development Specialist - Cybersecurity Research Analyst - Emerging Technology Specialist - Research & Development Engineer / Scientist / Analyst - Technology Research Analyst / Associate
Distribution of GS-Levels	Personnel performing the 661-Research and Development Specialist work role are most commonly found within the following grades on the General Schedule. - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☐ GS-11 – redacted**

	- ☒ GS-12 – 3% - ☒ GS-13 – 5% - ☒ GS-14 – 9% - ☐ GS-15 – redacted** *78% of all 661s are in non-GS pay plans and excluded from this section **Percentages below 3% are redacted.
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 661-Research and Development Specialist work role: - 422-Data Analyst - 621-Software Developer - 622-Secure Software Assessor - 632-Systems 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 661-Research and Development Specialist. 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: - 651-Enterprise Architect - 671-System Testing & Evaluation Specialist - 622-Secure Software Assessor - 631-Information Systems Security Developer - 652-Security Architect *Note: Leveraging the knowledge, skills, abilities, and tasks of the 661-Research and Development Specialist 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 661 - Research and Development Specialist work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 661- Research and Development Specialist Core Tasks

Task ID	Task	Core or Additional
T0249	Research current technology to understand capabilities of required system or network.	Core
T0250	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.	Core
T0283	Collaborate with stakeholders to identify and/or develop appropriate solutions technology.	Core
T0329	Follow software and systems engineering life cycle standards and processes.	Core
T0547	Research and evaluate available technologies and standards to meet customer requirements.	Core
T0064	Review and validate data mining and data warehousing programs, processes, and requirements.	Additional
T0284	Design and develop new tools/technologies as related to cybersecurity.	Additional
T0327	Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.	Additional
T0409	Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.	Additional
T0410	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.	Additional
T0411	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Additional
T0413	Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce.	Additional
T0411	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Additional
T0413	Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce.	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 661 - Research and Development Specialist work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 661 - Research and Development Specialist Core Knowledge, Skills, and Abilities

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
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration	Core
S0140	Skill in applying the systems engineering process.	Systems Integration	Core
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness	Core
K0268	Knowledge of forensic footprint identification.	Computer Forensics	Additional
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	Computer Network Defense	Additional
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement	Additional
S0017	Skill in creating and utilizing mathematical or statistical models.	Data Analysis	Additional
S0072	Skill in using scientific rules and methods to solve problems.	Data Analysis	Additional
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption	Additional
K0321	Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/software.	Enterprise Architecture	Additional

KSA ID	Description	Competency	Importance to Work Role
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture	Additional
K0288	Knowledge of industry standard security models.	External Awareness	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
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design	Additional
K0174	Knowledge of networking protocols.	Infrastructure Design	Additional
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	Infrastructure Design	Additional
K0209	Knowledge of covert communication techniques.	Intelligence Analysis	Additional
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence	Additional
K0271	Knowledge of operating system structures and internals (e.g., process management, directory structure, installed applications).	Operating Systems	Additional
K0499	Knowledge of operations security.	Operations Support	Additional
A0018	Ability to prepare and present briefings.	Presenting Effectively	Additional
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management	Additional
K0172	Knowledge of middleware (e.g., enterprise service bus and message queuing).	Software Development	Additional
S0172	Skill in applying secure coding techniques.	Software Development	Additional
S0148	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.	Systems Integration	Additional
K0269	Knowledge of mobile communications architecture.	Telecommunications	Additional
K0171	Knowledge of hardware reverse engineering techniques.	Threat Analysis	Additional
K0175	Knowledge of software reverse engineering techniques.	Threat Analysis	Additional
K0009	Knowledge of application vulnerabilities.	Vulnerabilities Assessment	Additional
K0272	Knowledge of network analysis tools used to identify software communications vulnerabilities.	Vulnerabilities Assessment	Additional

KSA ID	Description	Competency	Importance to Work Role
K0310	Knowledge of hacking methodologies.	Vulnerabilities Assessment	Additional
K0314	Knowledge of industry technologies' potential cybersecurity vulnerabilities.	Vulnerabilities Assessment	Additional
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment	Additional
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment	Additional
K0176	Knowledge of Extensible Markup Language (XML) schemas.	Web Technology	Additional
A0019	Ability to produce technical documentation.	Written Communication	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 661- Research and Development Specialist 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. 661 - Research and Development Specialist Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Infrastructure Design	C026	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. - Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. - Knowledge of networking protocols. - Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	Core
Systems Integration	C049	KSAs that relate to the principles, methods, and procedures for installing, integrating, and optimizing information systems components.	- Knowledge of system life cycle management principles, including software security and usability. - Skill in applying the systems engineering process. - Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.	Core
Vulnerabilities Assessment	C057	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. - Knowledge of specific operational impacts of cybersecurity lapses. - Knowledge of application vulnerabilities. - Knowledge of network analysis tools used to identify software communications vulnerabilities. - Knowledge of hacking methodologies. - Knowledge of industry technologies' potential cybersecurity vulnerabilities. - Knowledge of penetration testing principles, tools, and techniques. - Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Core

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 661 - Research and Development Specialist Suggested Qualifications / Capability Indicators

For indicators of capability for the 661 - Research and Development Specialist 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 661 - Research and Development Specialist.

2 APPENDIX: 661 - RESEARCH AND DEVELOPMENT SPECIALIST 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.

2.2 661 - RESEARCH AND DEVELOPMENT SPECIALIST TASK ANALYSIS AND KSA MAPPING

Table 8. T0249 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Research current technology to understand capabilities of required system or network.	Core
Entry	*Research current and new technology researched to understand capabilities of required systems, applications or network.*	
Intermediate	*Research current and new technology to make recommendations on capabilities for required systems, applications or network.*	
Advanced	*Guide others, as well as review, approve, and advise stakeholders on recommendations from research applicable to required systems, applications or network.*	

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

KSA ID	Description	Competency
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
K0288	Knowledge of industry standard security models.	External Awareness
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	Infrastructure Design
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
A0019	Ability to produce technical documentation.	Written Communication

Table 10. T0250 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.	Core
Entry	*Identify cyber capabilities strategies for hardware and software development based on mission requirements.*	
Intermediate	*Evaluating and recommending specific cyber capabilities strategies for hardware and software development based on mission requirements.*	
Advanced	*Review, approve, and advise stakeholders on recommended cyber capabilities strategies for hardware and software development based on mission requirements.*	

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

KSA ID	Description	Competency
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
K0288	Knowledge of industry standard security models.	External Awareness
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness

Table 12. T0283 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Collaborate with stakeholders to identify and/or develop appropriate solutions technology.	Core
Entry	*Identify appropriate solutions technology.*	
Intermediate	*Evaluate and recommend appropriate solutions technology.*	
Advanced	*Review, approve, and advise on recommendations to acquire and/or develop an appropriate solutions technology.*	

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

KSA ID	Description	Competency
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
K0288	Knowledge of industry standard security models.	External Awareness
K0004	Knowledge of cybersecurity and privacy principles.	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
A0018	Ability to prepare and present briefings.	Presenting Effectively
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
S0140	Skill in applying the systems engineering process.	Systems Integration
S0148	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.	Systems Integration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
A0019	Ability to produce technical documentation.	Written Communication

Table 14. T0329 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Follow software and systems engineering life cycle standards and processes.	Core
Entry	*Following SOPs, follow software and systems engineering life cycle standards and processes.*	
Intermediate	*Make recommendations to enhance software and systems engineering life cycle standards and processes.*	
Advanced	*Develop, review, and approve recommendations to software and systems engineering life cycle standards and processes.*	

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

KSA ID	Description	Competency
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
S0140	Skill in applying the systems engineering process.	Systems Integration
S0148	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.	Systems Integration

Table 16. T0547 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Research and evaluate available technologies and standards to meet customer requirements.	Core
Entry	*Research and evaluate of available technologies and standards to meet customer requirements.*	
Intermediate	*Evaluate and provide recommendations on available technologies and standards to meet customer requirements.*	
Advanced	*Review, approve, and provide guidance on researching and evaluation of available technologies and standards to meet customer requirements.*	

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

KSA ID	Description	Competency
K0321	Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/software.	Enterprise Architecture
A0018	Ability to prepare and present briefings.	Presenting Effectively
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0314	Knowledge of industry technologies' potential cybersecurity vulnerabilities.	Vulnerabilities Assessment
A0019	Ability to produce technical documentation.	Written Communication