CAREER PATHWAY COMMUNICATIONS SECURITY (COMSEC) MANAGER (723)

November 2020

5

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 723-COMMUNICATIONS SECURITY (COMSEC) MANAGER

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 723-Communications Security (COMSEC) Manager.

Table 1. 723-Communications Security (COMSEC) Manager Work Role Overview

NICE Role Description	*Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).*
OPM Occupational Series	Personnel performing the 723-Communications Security (COMSEC) Manager work role are most commonly aligned to the following Occupational Series: (Top 5 Shown) - 2210-Information Technology Management – 36% - 0391-Telecommunications – 35% - 0080-Security Administration – 18% - 0301-Miscellaneous Administration and Program – 4% - 0343-Management and Program Analysis – 1%
Work Role Pairings	Personnel performing the 723- Communications Security (COMSEC) Manager work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 722-Information Systems Security Manager – 12% - 451-System Administrator – 11% - 411-Technical Support Specialist – 11% - 441-Network Operations Specialist – 8% - 723-COMSEC Manager – 10%
Functional Titles	Personnel performing the 723-Communications Security (COMSEC) Manager work role may unofficially or alternatively be called: - Keying Material Manager - Network Services and Data Communications Specialist - Security Specialist (Crypto) - Telecommunications Specialist
Distribution of GS-Levels	Personnel performing the 723-Communications Security (COMSEC) Manager work role are most commonly found within the following grades on the General Schedule.*

	- ☐ GS-6 – redacted** - ☐ GS-7 – redacted** - ☒ GS-9 – 8% - ☐ GS-10 – redacted** - ☒ GS-11 – 25% - ☒ GS-12 – 24% - ☒ GS-13 – 21% - ☒ GS-14 – 7% - ☐ GS-15 – redacted** *10% of all 723s 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 723-Communications Security (COMSEC) Manager work role: - 722-Information Systems Security Manager
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 723-Communications Security (COMSEC) Manager work role. 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: - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 723-Communications Security (COMSEC) Manager 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 Officer / Privacy Compliance Manager* - *802-IT Project Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 723-Communications Security (COMSEC) Manager work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 723-Communications Security (COMSEC) Manager Core Tasks

Task ID	Task Description	Core or Additional
T0003	Advise senior management (e.g., CIO) on risk levels and security posture.	Core
T0089	Ensure security improvement actions are evaluated, validated, and implemented as required.	Core
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.	Core
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Core
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.	Additional
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Additional
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Additional
T0095	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Additional
T0099	Evaluate cost benefit, economic, and risk analysis in decision making process.	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 723-Communications Security (COMSEC) Manager work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 723-Communications Security (COMSEC) Manager Core KSAs

KSA ID	Description	Competency	Importance to Work Role
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to all Work Roles
K0005	Knowledge of cyber threats and vulnerabilities.	Risk Management	Foundational to all Work Roles
K0004	Knowledge of cybersecurity principles.	Legal, Government, and Jurisprudence	Foundational to all Work Roles
K0003	Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	Information Systems/Network Security	Foundational to all Work Roles
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Vulnerabilities Assessment	Foundational to all Work Roles
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to all Work Roles
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Core
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance	Core
K0026	Knowledge of disaster recovery continuity of operations plans.	Business Continuity	Core
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	Encryption	Core
K0042	Knowledge of incident response and handling methodologies.	Incident Management	Core
K0163	Knowledge of critical information technology (IT) procurement requirements.	Contracting/Procurement	Core
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management	Core

KSA ID	Description	Competency	Importance to Work Role
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	Legal, Government, and Jurisprudence	Core
K0126	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	Contracting/Procurement	Core
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration	Core
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture	Core
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment	Additional
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	Encryption	Additional
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption	Additional
A0163	Ability to interpret Communications Security (COMSEC) terminology, guidelines and procedures.	Data Privacy and Protection	Additional
A0164	Ability to identify the roles and responsibilities for appointed Communications Security (COMSEC) personnel.	Data Privacy and Protection	Additional
A0165	Ability to manage Communications Security (COMSEC) material accounting, control and use procedure.	Data Privacy and Protection	Additional
A0166	Ability to identify types of Communications Security (COMSEC) Incidents and how they're reported.	Incident Management	Additional
A0167	Ability to recognize the importance of auditing Communications Security (COMSEC) material and accounts.	Data Privacy and Protection	Additional
A0168	Ability to Identify the requirements of In-Process accounting for Communications Security (COMSEC).	Data Privacy and Protection	Additional
A0177	Ability to recognize the unique aspects of the Communications Security (COMSEC) environment and hierarchy.	Data Privacy and Protection	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 723-Communications Security (COMSEC) Manager 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. 723-Communications Security (COMSEC) Manager Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Data Privacy and Protection	C014	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	• Ability to interpret Communications Security (COMSEC) terminology, guidelines and procedures. • Ability to identify the roles and responsibilities for appointed Communications Security (COMSEC) personnel. • Ability to manage Communications Security (COMSEC) material accounting, control and use procedure. • Ability to recognize the importance of auditing Communications Security (COMSEC) material and accounts. • Ability to Identify the requirements of In-Process accounting for Communications Security (COMSEC). • Ability to recognize the unique aspects of the Communications Security (COMSEC) environment and hierarchy.	Core
Encryption	C017	KSAs that relate to the process of transforming information to make it unreadable for unauthorized users.	• Skill in using Virtual Private Network (VPN) devices and encryption. • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). • Knowledge of encryption algorithms • Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.	Core

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 723-Communications Security (COMSEC) Manager Suggested Qualifications

For indicators of capability for the 511-Cyber Defense Analyst 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 723-Communications Security (COMSEC) Manager.*

2 APPENDIX: 723-COMMUNICATIONS SECURITY (COMSEC) MANAGER 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.

2.2 723-COMMUNICATIONS SECURITY (COMSEC) MANAGER TASK ANALYSIS AND KSA MAPPING

Table 8. T0003 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Advise senior management (e.g., CIO) on risk levels and security posture.	Core
Entry	*Understand advisement given to senior management (e.g., CIO) on risk levels and security posture.*	
Intermediate	*Advise senior management (e.g., CIO) on risk levels and security posture.*	
Advanced	*Analyze and make recommendations to senior management (e.g., CIO) on risk levels and security posture.*	

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

KSA ID	Description	Competency
TO BE COMPLETED		

Table 10. T0089 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure security improvement actions are evaluated, validated, and implemented as required.	Core
Entry	*Understand how to ensure that security improvement actions are evaluated, validated, and implemented as required.*	
Intermediate	*Ensure security improvement actions are evaluated, validated, and implemented as required.*	
Advanced	*Evaluate when security improvement actions are evaluated, validated, and implemented as required.*	

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

KSA ID	Description	Competency
TO BE COMPLETED		

Table 12. T0215 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Recognize a possible security violation and take appropriate action to report the incident, as required.	Core
Entry	*Recognize and describe a possible security violation and the appropriate action to report the incident, as required.*	
Intermediate	*Recognize a possible security violation and take appropriate action to report the incident, as required.*	
Advanced	*Evaluate and analyze a possible security violation and take appropriate action to report the incident, as required.*	

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

KSA ID	Description	Competency
TO BE COMPLETED		

Table 14. T0229 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	
Entry	*Recommend protective or corrective measures when a cybersecurity incident or vulnerability is discovered.*	
Intermediate	*Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.*	
Advanced	*Evaluate and analyze protective or corrective measures when a cybersecurity incident or vulnerability is discovered.*	

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

KSA ID	Description	Competency
TO BE COMPLETED		