

# CAREER PATHWAY CYBER WORKFORCE DEVELOPER AND MANAGER (751)

January 2021

CLEARED  
For Open Publication  
Apr 07, 2021

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

## Developed By:

The Interagency  
Federal Cyber  
Career  
Pathways Working  
Group

## Endorsed By:



## TABLE OF CONTENTS

<b>1</b>	<b>751-CYBER WORKFORCE DEVELOPER AND MANAGER</b>	<b>3</b>
1.1	Work Role Overview	3
1.2	Core Tasks	6
1.3	Core Knowledge, Skills, and Abilities	8
1.4	Core Competencies	10
1.5	Suggested Qualifications / Capability Indicators	12
<b>2</b>	<b>APPENDIX: 751-CYBER WORKFORCE DEVELOPER AND MANAGER TASK ANALYSIS AND KSA MAPPING</b>	<b>13</b>
2.1	Key to Reading the Task Analysis and KSA Mapping	13
2.2	751-Cyber Workforce Developer and Manager Task Analysis and KSA Mapping	14

# 1 751-CYBER WORKFORCE DEVELOPER AND MANAGER

## 1.1 Work Role Overview

The table below provides an overview of various role-specific elements related to 641-Systems Requirements Planner.

*Table 1. 751-Cyber Workforce Developer and Manager Work Role Overview*

<b>NICE Role Description</b>	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
<b>OPM Occupational Series</b>	<p>Personnel performing the 751-Cyber Workforce Developer and Manager work role are most commonly aligned to the following Occupational Series (Top 5 Shown):</p> <ul style="list-style-type: none"> <li>- 2210-Information Technology – 65%</li> <li>- 0343-Management and Program Analysis – 10%</li> <li>- 0301-Miscellaneous Administration and Program – 6%</li> <li>- 0201-Human Resources Management – 4%</li> <li>- 0855-Electronics Engineering – 3%</li> </ul>
<b>Work Role Pairings</b>	<p>Personnel performing the 751-Cyber Workforce Develop and Manager work role are most commonly paired with the following complimentary Work Roles (Top 5 shown):</p> <ul style="list-style-type: none"> <li>- 752-Cyber Policy and Strategy Planner – 30%</li> <li>- 801-Program Manager – 14%</li> <li>- 431-Knowledge Manager – 8%</li> <li>- 722-Information Systems Security Manager – 7%</li> <li>- 802-IT Project Manager – 6%</li> </ul>
<b>Functional Titles</b>	<p>Personnel performing the 751-Cyber Workforce Developer and Manager work role may unofficially or alternatively be called:</p> <ul style="list-style-type: none"> <li>- Cyber Workforce Development and Planning Specialist</li> <li>- Chief Human Capital Officer</li> <li>- Human Capital Specialist</li> <li>- Manpower Analyst</li> <li>- Workforce Development Project/Program Manager</li> <li>- Workforce Development Specialist</li> <li>- Workforce Planner</li> <li>- Workforce Planning Analyst</li> <li>- Workforce Research Analyst</li> </ul>
<b>Distribution of GS-Levels</b>	<p>Personnel performing the 751-Cyber Workforce Developer and Manager work role are most commonly found within the following grades on the General Schedule.</p> <ul style="list-style-type: none"> <li>- <input type="checkbox"/> GS-7 – redacted**</li> </ul>

	<ul style="list-style-type: none"> <li>- <input type="checkbox"/> GS-9 – redacted**</li> <li>- <input type="checkbox"/> GS-10 – redacted*</li> <li>- <input checked="" type="checkbox"/> GS-11 – 5%</li> <li>- <input checked="" type="checkbox"/> GS-12 – 13%</li> <li>- <input checked="" type="checkbox"/> GS-13 – 29%</li> <li>- <input checked="" type="checkbox"/> GS-14 – 23%</li> <li>- <input checked="" type="checkbox"/> GS-15 – 8%</li> </ul> <p>*19% of all personnel performing the 751-Cyber Workforce Developer and Manager work role are in non-GS pay plans and are excluded from this section</p> <p>** percentages less than 3% have been redacted</p>
<b>On Ramps</b>	<p>The following work roles are examples of possible roles an individual may perform prior to transitioning into the 751-Cyber Workforce Developer and Manager work role:</p> <ul style="list-style-type: none"> <li>- 211-Forensics Analyst</li> <li>- 212-Cyber Defense Forensics Analyst</li> <li>- 221-Cyber Crime Investigator</li> <li>- 411-Technical Support Specialist</li> <li>- 421-Database Administrator</li> <li>- 422-Data Analyst</li> <li>- 431-Knowledge Manager</li> <li>- 441-Network Operations Specialist</li> <li>- 451-System Administrator</li> <li>- 461-Systems Security Analyst</li> <li>- 511-Cyber Defense Analyst</li> <li>- 521-Cyber Defense Infrastructure Support Specialist</li> <li>- 531-Cyber Defense Incident Responder</li> <li>- 541-Vulnerability Assessment Analyst</li> <li>- 612-Security Control Assessor</li> <li>- 621-Software Developer</li> <li>- 631-Information Systems Security Developer</li> <li>- 632-Systems Developer</li> <li>- 641-Systems Requirements Planner</li> <li>- 661-Research and Development Specialist</li> <li>- 671-System Testing and Evaluation Specialist</li> <li>- 711-Cyber Instructional Curriculum Developer</li> <li>- 712-Cyber Instructor</li> <li>- 722-Information Systems Security Manager (ISSM)</li> <li>- 732-Privacy Officer/Privacy Compliance Manager</li> <li>- 752-Cyber Policy and Strategy Planner</li> <li>- 801-Program Manager</li> <li>- 802-IT Project Manager</li> <li>- 803-Product Support Manager</li> </ul>
<b>Off Ramps</b>	<p>The following work roles are examples of common transitions an individual may pursue after having performed the 751-Cyber Workforce Developer and Manager work role. This is not</p>

	<p>an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles:</p>
--	--

- 711-Cyber Instructional Curriculum Developer
- 712-Cyber Instructor
- 752-Cyber Policy and Strategy Planner
- 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 751-Cyber Workforce Developer and Manager work role, as well as additional tasks that those in this role may be expected to perform.

*Table 2. 751-Cyber Workforce Developer and Manager Core Tasks*

<b>Task ID</b>	<b>Task Description</b>	<b>Core or Additional</b>
T0341	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Core
T0355	Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.	Core
T0362	Develop and implement standardized position descriptions based on established cyber work roles.	Core
T0363	Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies.	Core
T0368	Ensure that cyber career fields are managed in accordance with organizational HR policies and directives.	Core
T0369	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	Core
T0372	Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.	Core
T0374	Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.	Core
T0375	Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.	Core
T0376	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	Core
T0387	Review and apply cyber career field qualification standards.	Core
T0388	Review and apply organizational policies related to or influencing the cyber workforce.	Core
T0390	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Core
T0391	Support integration of qualified cyber workforce personnel into information systems life cycle development processes.	Core
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Core
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Core
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Additional
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Additional

T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Additional
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Additional
T0074	Develop policy, programs, and guidelines for implementation.	Additional
T0094	Establish and maintain communication channels with stakeholders.	Additional
T0099	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Additional
T0116	Identify organizational policy stakeholders.	Additional
T0222	Review existing and proposed policies with stakeholders.	Additional
T0226	Serve on agency and interagency policy boards.	Additional
T0352	Conduct learning needs assessments and identify requirements.	Additional
T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Additional
T0364	Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.	Additional
T0365	Develop or assist in the development of training policies and protocols for cyber training.	Additional
T0373	Establish and oversee waiver processes for cyber career field entry and training qualification requirements.	Additional
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Additional
T0408	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Additional
T0425	Analyze organizational cyber policy.	Additional
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Additional
T0437	Correlate training and learning to business or mission requirements.	Additional
T0441	Define and integrate current and future mission environments.	Additional
T0472	Draft, staff, and publish cyber policy.	Additional
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Additional
T0506	Seek consensus on proposed policy changes from stakeholders.	Additional
T0529	Provide policy guidance to cyber management, staff, and users.	Additional
T0533	Review, conduct, or participate in audits of cyber programs and projects.	Additional
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Additional
T0537	Support the CIO in the formulation of cyber-related policies.	Additional
T0552	Review and approve a supply chain security/risk management policy.	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 751-Cyber Workforce Developer and Manager work role, as well as additional KSAs that those in this role may be expected to demonstrate.

*Table 3. 751-Cyber Workforce Developer and Manager 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
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness	Core
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness	Core
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	External Awareness	Core
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness	Core
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management	Core
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.	Strategic Planning	Core
K0243	Knowledge of organizational training and education policies, processes, and procedures.	Teaching Others	Core
A0053	Ability to determine the validity of workforce trend data.	Workforce Management	Core
S0108	Skill in developing workforce and position qualification standards.	Workforce Management	Core



K0234	Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).	Computer Network Defense	Additional
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture	Additional
A0023	Ability to design valid and reliable assessments.	Information Technology Assessment	Additional
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	Legal, Government, and Jurisprudence	Additional
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence	Additional
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness	Additional
K0072	Knowledge of resource management principles and techniques.	Project Management	Additional
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management	Additional
K0204	Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).	Teaching Others	Additional
K0215	Knowledge of organizational training policies.	Teaching Others	Additional
K0309	Knowledge of emerging technologies that have potential for exploitation.	Technology Awareness	Additional
K0311	Knowledge of industry indicators useful for identifying technology trends.	Technology Awareness	Additional
K0335	Knowledge of current and emerging cyber technologies.	Technology Awareness	Additional
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	Vulnerabilities Assessment	Additional
A0042	Ability to develop career path opportunities.	Workforce Management	Additional
S0128	Skill in using manpower and personnel IT systems.	Workforce Management	Additional

## 1.4 Core Competencies

The table below is a compilation of competencies aligned to the 751-Cyber Workforce Developer and Manager work role, and their associated importance. *These competencies originate from the NICE Framework Competency Pivot Tool.*

Table 4. 751-Cyber Workforce Developer and Manager Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
External Awareness	C019	This area contains KSAs that relate to identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization	<ul style="list-style-type: none"> <li>- Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.</li> <li>- Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.</li> <li>- Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research &amp; Development).</li> </ul>	Core
Legal, Government, and Jurisprudence	C030	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.	<ul style="list-style-type: none"> <li>- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.</li> <li>- Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).</li> <li>- Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.</li> </ul>	Core
Teaching Others	C052	This area contains KSAs that relate to imparting knowledge of or giving information about or instruction in (a subject or skill)	<ul style="list-style-type: none"> <li>- Knowledge of organizational training and education policies, processes, and procedures.</li> <li>- Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).</li> <li>- Knowledge of organizational training policies.</li> </ul>	Core
Workforce Management	C059	This area contains KSAs that relate to the activities needed to maintain a productive workforce	<ul style="list-style-type: none"> <li>- Ability to determine the validity of workforce trend data.</li> <li>- Skill in developing workforce and position qualification standards.</li> <li>- Ability to develop career path opportunities.</li> <li>- Skill in using manpower and personnel IT systems.</li> </ul>	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Technology Awareness	C053	This area contains KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results	<ul style="list-style-type: none"> <li>- Knowledge of emerging technologies that have potential for exploitation.</li> <li>- Knowledge of industry indicators useful for identifying technology trends.</li> <li>- Knowledge of current and emerging cyber technologies.</li> </ul>	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.	<ul style="list-style-type: none"> <li>- Knowledge of cyber threats and vulnerabilities.</li> <li>- Knowledge of specific operational impacts of cybersecurity lapses.</li> <li>- Knowledge of emerging security issues, risks, and vulnerabilities.</li> </ul>	Additional

## 1.5 Suggested Qualifications / Capability Indicators

*Table 5. 751-Cyber Workforce Developer and Manager Suggested Qualifications*

*For indicators of capability for the 751-Cyber Workforce Developer and Manager 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 751-Cyber Workforce Developer and Manager.*

## 2 APPENDIX: 751-CYBER WORKFORCE DEVELOPER AND 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	Behavioral indicator for performing this task at the foundational skills proficiency level.	
Intermediate	Behavioral indicator for performing this task at the Intermediate skills proficiency level.	
Advanced	Behavioral indicator for performing this task at the 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.

## 2.2 751-Cyber Workforce Developer and Manager Task Analysis and KSA Mapping

Table 8. T0341 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Core
Entry	<i>Earns support at appropriate organizational levels for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.</i>	
Intermediate	<i>Advocates to leadership and a broad base of stakeholders for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.</i>	
Advanced	<i>Champion at the senior leadership level for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.</i>	

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

KSA ID	Description	Competency
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	External Awareness
K0072	Knowledge of resource management principles and techniques.	Project Management
K0243	Knowledge of organizational training and education policies, processes, and procedures.	Teaching Others
K0215	Knowledge of organizational training policies.	Teaching Others
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	Vulnerabilities Assessment

Table 10. T0355 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.	Core
Entry	<i>Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.</i>	
Intermediate	<i>Lead coordination with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.</i>	
Advanced	<i>Oversee others who coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.</i>	

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

KSA ID	Description	Competency
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	External Awareness
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	Vulnerabilities Assessment
S0108	Skill in developing workforce and position qualification standards.	Workforce Management

Table 12. T0362 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop and implement standardized position descriptions based on established cyber work roles.	Core
<i>Entry</i>	<i>Develop and implement routine standardized position descriptions based on established cyber work roles.</i>	
<i>Intermediate</i>	<i>Develop and implement complex or novel standardized position descriptions based on established cyber work roles.</i>	
<i>Advanced</i>	<i>Oversee the development and implementation of standardized position descriptions based on established cyber work roles.</i>	

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

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	Vulnerabilities Assessment
S0108	Skill in developing workforce and position qualification standards.	Workforce Management



Table 14. T0363 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies.	Core
Entry	<i>Develop and reviews routine recruiting, hiring, and retention procedures in accordance with current HR policies.</i>	
Intermediate	<i>Develop and reviews complex or novel recruiting, hiring, and retention procedures in accordance with current HR policies.</i>	
Advanced	<i>Oversee the development and review of recruiting, hiring, and retention procedures in accordance with current HR policies.</i>	

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

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
A0023	Ability to design valid and reliable assessments.	Information Technology Assessment
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0072	Knowledge of resource management principles and techniques.	Project Management
K0243	Knowledge of organizational training and education policies, processes, and procedures.	Teaching Others
K0215	Knowledge of organizational training policies.	Teaching Others
S0108	Skill in developing workforce and position qualification standards.	Workforce Management
A0042	Ability to develop career path opportunities.	Workforce Management

Table 16. T0368 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure that cyber career fields are managed in accordance with organizational HR policies and directives.	Core
Entry	<i>Ensure that cyber career fields are managed in accordance with organizational HR policies and directives.</i>	
Intermediate	<i>Lead efforts to ensure that cyber career fields are managed in accordance with organizational HR policies and directives.</i>	
Advanced	<i>Oversee all efforts to ensure that cyber career fields are managed in accordance with organizational HR policies and directives.</i>	

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

KSA ID	Description	Competency
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0072	Knowledge of resource management principles and techniques.	Project Management

Table 18. T0369 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	Core
Entry	<i>Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.</i>	
Intermediate	<i>Lead efforts to ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.</i>	
Advanced	<i>Oversee all efforts to ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.</i>	

Table 19. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management

Table 20. T0372 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.	Core
Entry	<i>Establish and collects metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.</i>	
Intermediate	<i>Establish and collects complex or novel metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.</i>	
Advanced	<i>Oversee the establishment and collection of metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.</i>	

Table 21. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
K0072	Knowledge of resource management principles and techniques.	Project Management
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.	Strategic Planning
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
S0128	Skill in using manpower and personnel IT systems.	Workforce Management
A0053	Ability to determine the validity of workforce trend data.	Workforce Management

Table 22. T0374 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.	Core
Entry	<i>Establish routine cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.</i>	
Intermediate	<i>Establish complex or novel cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.</i>	
Advanced	<i>Oversee the establishment of cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.</i>	

Table 23. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	External Awareness
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0243	Knowledge of organizational training and education policies, processes, and procedures.	Teaching Others
S0108	Skill in developing workforce and position qualification standards.	Workforce Management
A0042	Ability to develop career path opportunities.	Workforce Management

Table 24. T0375 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.	Core
Entry	<i>Establish routine manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.</i>	
Intermediate	<i>Establish complex or novel manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.</i>	
Advanced	<i>Oversee the establishment of manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.</i>	

Table 25. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
A0053	Ability to determine the validity of workforce trend data.	Workforce Management
S0128	Skill in using manpower and personnel IT systems.	Workforce Management
S0108	Skill in developing workforce and position qualification standards.	Workforce Management

Table 26. T0376 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	Core
Entry	<i>Establish, resource, implement and assess routine cyber workforce management programs in accordance with organizational requirements.</i>	
Intermediate	<i>Establish, resources and update complex or novel cyber workforce management programs in accordance with organizational requirements.</i>	
Advanced	<i>Oversee the establishment, resourcing, implementation, and assessment of cyber workforce management programs in accordance with organizational requirements.</i>	

Table 27. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0072	Knowledge of resource management principles and techniques.	Project Management
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
A0053	Ability to determine the validity of workforce trend data.	Workforce Management

Table 28. T0387 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Review and apply cyber career field qualification standards.	Core
<i>Entry</i>	<i>Assist with reviewing cyber career field qualification standards.</i>	
<i>Intermediate</i>	<i>Review cyber career field qualification standards.</i>	
<i>Advanced</i>	<i>Lead and oversee the review and application of cyber career field qualification standards.</i>	

Table 29. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
S0108	Skill in developing workforce and position qualification standards.	Workforce Management



Table 30. T0388 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Review and apply organizational policies related to or influencing the cyber workforce.	Core
<i>Entry</i>	<i>Assist with reviewing organizational policies related to or influencing the cyber workforce.</i>	
<i>Intermediate</i>	<i>Review organizational policies related to or influencing the cyber workforce.</i>	
<i>Advanced</i>	<i>Lead and oversee the review and application of organizational policies related to or influencing the cyber workforce.</i>	

Table 31. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0243	Knowledge of organizational training and education policies, processes, and procedures.	Teaching Others
K0215	Knowledge of organizational training policies.	Teaching Others
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment

Table 32. T0390 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Core
Entry	Assist with reviewing/assessing cyber workforce effectiveness to adjust skill and/or qualification standards.	
Intermediate	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	
Advanced	Oversee the review/assessment of cyber workforce effectiveness to adjust skill and/or qualification standards.	

Table 33. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0023	Ability to design valid and reliable assessments.	Information Technology Assessment
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.	Strategic Planning
K0204	Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).	Teaching Others
K0335	Knowledge of current and emerging cyber technologies.	Technology Awareness
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	Vulnerabilities Assessment
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
S0128	Skill in using manpower and personnel IT systems.	Workforce Management
A0053	Ability to determine the validity of workforce trend data.	Workforce Management

Table 34. T0391 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Support integration of qualified cyber workforce personnel into information systems life cycle development processes.	Core
Entry	<i>Support integration of qualified cyber workforce personnel into information systems life cycle development processes.</i>	
Intermediate	<i>Integrate integration of qualified cyber workforce personnel into information systems life cycle development processes.</i>	
Advanced	<i>Develop integration of qualified cyber workforce personnel into information systems life cycle development processes.</i>	

Table 35. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0023	Ability to design valid and reliable assessments.	Information Technology Assessment
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
A0042	Ability to develop career path opportunities.	Workforce Management
S0108	Skill in developing workforce and position qualification standards.	Workforce Management

Table 36. T0445 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.	Core
Entry	<i>Help with designing/integrating a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.</i>	
Intermediate	<i>Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.</i>	
Advanced	<i>Oversee the design/integration a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.</i>	

Table 37. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	External Awareness
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0072	Knowledge of resource management principles and techniques.	Project Management
K0243	Knowledge of organizational training and education policies, processes, and procedures.	Teaching Others
K0215	Knowledge of organizational training policies.	Teaching Others
K0335	Knowledge of current and emerging cyber technologies.	Technology Awareness
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment

K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	Vulnerabilities Assessment
-------	--	----------------------------

Table 38. T0481 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Core
Entry	<i>Support the identification of cyber workforce planning and management issues (e.g. recruitment, retention, and training).</i>	
Intermediate	<i>Identify and address routine cyber workforce planning and management issues (e.g. recruitment, retention, and training).</i>	
Advanced	<i>Oversee cyber workforce planning and management issues (e.g. recruitment, retention, and training).</i>	

Table 39. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
A0023	Ability to design valid and reliable assessments.	Information Technology Assessment
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0241	Knowledge of organizational human resource policies, processes, and procedures.	Organizational Awareness
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0072	Knowledge of resource management principles and techniques.	Project Management
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.	Strategic Planning
K0243	Knowledge of organizational training and education policies, processes, and procedures.	Teaching Others
K0215	Knowledge of organizational training policies.	Teaching Others
S0108	Skill in developing workforce and position qualification standards.	Workforce Management
A0042	Ability to develop career path opportunities.	Workforce Management