CAREER PATHWAY CYBER POLICY AND STRATE PLANNER (752)

January 2021

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

CIO COUNCIL

CHIEF HUMAN CAPITAL OFFICERS COUNCIL
CHCO COUNCIL
UNITED STATES OF AMERICA

Table of Contents

CAREER PATHWAY CYBER POLICY STRATEGY PLANNER (752) 1

1 752-CYBER POLICY AND STRATEGY PLANNER 3

1.1 Work Role Overview 3

1.2 Core Tasks 6

1.3 Core Knowledge, Skills, and Abilities 7

1.4 Core Competencies 9

1.5 Suggested Qualifications / Capability Indicators 10

2 APPENDIX: 752-CYBER POLICY AND STRATEGY PLANNER TASK ANALYSIS AND KSA MAPPING 11

2.1 Key to Reading the Task Analysis and KSA Mapping 11

2.2 752-Cyber Policy and Strategy Planner Task Analysis and KSA Mapping 12

1 752-CYBER POLICY AND STRATEGY PLANNER

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 752-Cyber Policy and Strategy Planner.

Table 1. 752-Cyber Policy and Strategy Planner Work Role Overview

NICE Role Description	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
OPM Occupational Series	Personnel performing the 752-Cyber Policy and Strategy Planner work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 71% - 0301-Miscellaneous Administration and Program – 6% - 0343-Management and Program Analysis – 6% - 0391-Telecommunications – 3% - 0801-General Engineering – 3%
Work Role Pairings	Personnel performing the 752-Cyber Policy and Strategy Planner work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 801-Program Manager – 17% - 641-Systems Requirements Planner – 10% - 751-Cyber Workforce Developer and Manager – 8% - 802-IT Project Manager - 7% - 332-Cyber Ops Planner – 7%
Functional Titles	Personnel performing the 752-Cyber Policy and Strategy Planner work role may unofficially or alternatively be called: - Cyber Policy Writer and Strategist - Cyber Strategic Advisor - Governance Specialist / Manager - Policy Analyst - Policy and Planning Analyst - Policy and Strategy Manager - Policy Compliance Analyst - Policy Manager - Regulatory Affairs Analyst - Strategic IT Policy Planner - Strategic Planning Manager

Distribution of GS-Levels	Personnel performing the 752-Cyber Policy and Strategy Planner work role are most commonly found within the following grades on the General Schedule. - ☐ GS-6 – redacted** - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☒ GS-11 – 4% - ☒ GS-12 – 12% - ☒ GS-13 – 25% - ☒ GS-14 – 24% - ☒ GS-15 – 14% *18% of all 752s 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 752-Cyber Policy and Strategy Planner work role: - 211-Forensics Analyst - 212-Cyber Defense Forensics Analyst - 221-Cyber Crime Investigator - 411-Technical Support Specialist - 421-Database Administrator - 422-Data Analyst - 431-Knowledge Manager - 441-Network Operations Specialist - 451-System Administrator - 461-Systems Security Analyst - 511-Cyber Defense Analyst - 521-Cyber Defense Infrastructure Support Specialist - 531-Cyver Defense Incident Responder - 541-Vulnerability Assessment Analyst - 611-Authorizing Official/Designating Representative - 612-Security Control Assessor - 621-Software Developer - 631-Information Systems Security Developer - 632-Systems Developer - 641-Systems Requirements Planner - 651-Enterprise Architect - 652-Security Architect - 661-Research and Development Specialist - 671-System Testing and Evaluation Specialist - 711-Cyber Instructional Curriculum Developer - 712-Cyber Instructor - 722-Information Systems Security Manager (ISSM) - 732-Privacy Officer/Privacy Compliance Manager

	- 751-Cyber Workforce Developer and Manager - 801-Program Manager - 802-IT Project Manager - 803-Product Support Manager - 804-IT Investment/Portfolio Manager - 805-IT Program Auditor
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 752-Cyber Policy and Strategy Planner. 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: - 611-Authorizing Official/Designated Representative - 711-Cyber Instructional Curriculum Developer - 712-Cyber Instructor - 732-Privacy Officer/Privacy Compliance Manager - 751-Cyber Workforce Developer and Manager - 801-Program Manager - 802-It Project Manager - 901-Executive Cyber Leadership

1.2 Core Tasks

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 752-Cyber Policy and Strategy Planner work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 752-Cyber Policy and Strategy Planner Core Tasks

Task ID	Task	Core or Additional
T0074	Develop policy, programs, and guidelines for implementation.	Core
T0094	Establish and maintain communication channels with stakeholders.	Core
T0222	Review existing and proposed policies with stakeholders.	Core
T0226	Serve on agency and interagency policy boards.	Core
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.	Core
T0408	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Core
T0425	Analyze organizational cyber policy.	Core
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Core
T0441	Define and integrate current and future mission environments.	Core
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.	Core
T0472	Draft, staff, and publish cyber policy.	Core
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Core
T0506	Seek consensus on proposed policy changes from stakeholders.	Core
T0529	Provide policy guidance to cyber management, staff, and users.	Core
T0533	Review, conduct, or participate in audits of cyber programs and projects.	Core
T0537	Support the CIO in the formulation of cyber-related policies.	Core
T0341	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Additional
T0369	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	Additional
T0390	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	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 752-Cyber Policy and Strategy Planner work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 752-Cyber Policy and Strategy Planner 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
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	Core
K0146	Knowledge of the organization's core business/mission processes.	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
K0248	Knowledge of strategic theory and practice.	Strategic Planning	Core
K0309	Knowledge of emerging technologies that have potential for exploitation.	Technology Awareness	Core
K0335	Knowledge of current and emerging cyber technologies.	Technology Awareness	Core
K0234	Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).	Computer Network Defense	Additional
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	External Awareness	Additional
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	Legal, Government, and Jurisprudence	Additional
K0311	Knowledge of industry indicators useful for identifying technology trends.	Technology Awareness	Additional
A0003	Ability to determine the validity of technology trend data.	Technology Awareness	Additional

KSA ID	Description	Competency	Importance to Work Role
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management	Additional
S0250	Skill in preparing plans and related correspondence.	Written Communication	Additional

1.4 Core Competencies

The table below is a compilation of competencies aligned to the 752-Cyber Policy and Strategy Planner 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. 752-Cyber Policy and Strategy Planner Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Legal, Government, and Jurisprudence	C030	KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.	- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. - Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure). - 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.	Core
Technology Awareness	C053	KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results	- Knowledge of emerging technologies that have potential for exploitation. - Knowledge of industry indicators useful for identifying technology trends. - Knowledge of current and emerging cyber technologies. - Ability to determine the validity of technology trend data.	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 system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). - Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Additional

1.5 Suggested Qualifications / Capability Indicators

Table 5. 752-Cyber Policy and Strategy Planner Suggested Qualifications / Capability Indicators

For indicators of capability for the752-Cyber Policy and Strategy Planner 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 752-Cyber Policy and Strategy Planner.

2 APPENDIX: 752-CYBER POLICY AND STRATEGY PLANNER 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.

2.2 752-Cyber Policy and Strategy Planner Task Analysis and KSA Mapping

Table 8. 0074 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop policy, programs, and guidelines for implementation.	Core
Entry	*Support the documentation and development of organizational cyber policy, programs, and guidelines for implementation.*	
Intermediate	*Develop organizational cyber policy, programs, and guidelines for implementation.*	
Advanced	*Oversee and define organizational cyber policy, programs, and guidelines for implementation.*	

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

KSA ID	Description	Competency
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
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0335	Knowledge of current and emerging cyber technologies.	Technology Awareness
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 10. 0094 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Establish and maintain communication channels with stakeholders.	Core
Entry	*Maintain and support communication channels with stakeholders.*	
Intermediate	*Establish and maintain communication channels with stakeholders.*	
Advanced	*Establish, maintain, and foster effective communication channels with stakeholders.*	

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

KSA ID	Description	Competency
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	Legal, Government, and Jurisprudence
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 12. 0222 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Review existing and proposed policies with stakeholders.	Core
Entry	*Review and edit existing and proposed policies with stakeholders.*	
Intermediate	*Develop and evaluate existing and proposed policies with stakeholders.*	
Advanced	*Communicate and make recommendations on existing and proposed policies with stakeholders.*	

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

KSA ID	Description	Competency
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
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	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
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management

Table 14. 0226 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Serve on agency and interagency policy boards.	Core
Entry	*Reference and apply the resources developed by agency and interagency policy boards.*	
Intermediate	*Serve on agency and interagency policy boards.*	
Advanced	*Serve and lead others on agency and interagency policy boards.*	

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

KSA ID	Description	Competency
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	External Awareness
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	External Awareness
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
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0248	Knowledge of strategic theory and practice.	Strategic Planning
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management

Table 16. 0341 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	*Support supervisor in advocating for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.*	
Intermediate	*Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.*	
Advanced	*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.*	

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

KSA ID	Description	Competency
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0248	Knowledge of strategic theory and practice.	Strategic Planning
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management

Table 18. 0384 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	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.	Core
Entry	*Support the promotion of awareness of cyber policy and strategy as appropriate among management and ensure sound cyber principles are reflected in the organization's mission, vision, and goals.*	
Intermediate	*Promote awareness of cyber policy and strategy as appropriate among management and ensure sound cyber principles are reflected in the organization's mission, vision, and goals.*	
Advanced	*Champion awareness of cyber policy and strategy as appropriate among management and ensure sound cyber principles are reflected in the organization's mission, vision, and goals.*	

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

KSA ID	Description	Competency
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 20. 0408 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Core
Entry	*Interpret and analyze routine applicable laws, statutes, and regulatory documents*	
Intermediate	*Interpret, evaluate, and apply applicable laws, statutes, and regulatory documents to policy.*	
Advanced	*Integrate current policies and/or develop new policies compliant with applicable laws, statutes, and regulatory documents.*	

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

KSA ID	Description	Competency
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	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
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
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 22. 0425 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze organizational cyber policy.	Core
Entry	*Document and apply organizational cyber policy.*	
Intermediate	*Analyze and evaluate organizational cyber policy.*	
Advanced	*Oversee analysis and evaluation of organizational cyber policy in support of policy development.*	

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

KSA ID	Description	Competency
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
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
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 24. 0429 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Core
Entry	*Support assessment of policy needs and collaboration with stakeholders to develop policies to govern cyber activities.*	
Intermediate	*Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.*	
Advanced	*Oversee the assessment of policy needs and collaboration with stakeholders to develop policies to govern cyber activities.*	

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

KSA ID	Description	Competency
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
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 26. 0441 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Define and integrate current and future mission environments.	Core
Entry	*Help with defining and integrating current and future mission environments.*	
Intermediate	*Define and integrate current and future mission environments.*	
Advanced	*Lead the definition and integration of current and future mission environments.*	

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

KSA ID	Description	Competency
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
K0309	Knowledge of emerging technologies that have potential for exploitation.	Technology Awareness
K0311	Knowledge of industry indicators useful for identifying technology trends.	Technology Awareness
K0335	Knowledge of current and emerging cyber technologies.	Technology Awareness

Table 28. 0445 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	*Help with designing/integrating a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.*	
Intermediate	*Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.*	
Advanced	*Oversee the design/integration a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.*	

Table 29. 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
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
K0248	Knowledge of strategic theory and practice.	Strategic Planning
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 30. 0472 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Draft, staff, and publish cyber policy.	Core
Entry	*Support the drafting and publishing of cyber policy.*	
Intermediate	*Draft, staff, and publish cyber policy.*	
Advanced	*Oversee the publishing of cyber policy.*	

Table 31. 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
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
K0248	Knowledge of strategic theory and practice.	Strategic Planning
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 32. 0505 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Core
Entry	*Support monitoring of rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.*	
Intermediate	*Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.*	
Advanced	*Lead rigorous review of how cyber policies, principles, and practices are applied in the delivery of planning and management services.*	

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

KSA ID	Description	Competency
K0248	Knowledge of strategic theory and practice.	Strategic Planning
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management

Table 34. 0506 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Seek consensus on proposed policy changes from stakeholders.	Core
Entry	*Work with supervisor to garner consensus on proposed policy changes from stakeholders.*	
Intermediate	*Seek consensus on proposed policy changes from stakeholders.*	
Advanced	*Champion consensus for proposed policy changes with senior leadership, staff, and internal and external stakeholders.*	

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

KSA ID	Description	Competency
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 36. 0529 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide policy guidance to cyber management, staff, and users.	Core
Entry	*Provide routine policy guidance to cyber management, staff, and users.*	
Intermediate	*Provide policy guidance to cyber management, staff, and users.*	
Advanced	*Oversee the provision of policy guidance to cyber management, staff, and users.*	

Table 37. 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
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 38. 0533 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Review, conduct, or participate in audits of cyber programs and projects.	Core
Entry	*Assist with audits of cyber programs and projects.*	
Intermediate	*Review, conduct, or participate in audits of cyber programs and projects.*	
Advanced	*Lead the audits of cyber programs and projects.*	

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

KSA ID	Description	Competency
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
S0250	Skill in preparing plans and related correspondence.	Written Communication

Table 40. 0537 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Support the CIO in the formulation of cyber-related policies.	Core
Entry	*Under supervision, support leadership to engage the CIO in the formulation of cyber-related policies.*	
Intermediate	*Support the CIO in the formulation of cyber-related policies.*	
Advanced	*Lead coordination with the CIO in the formulation of cyber-related policies.*	

Table 41. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
K0248	Knowledge of strategic theory and practice.	Strategic Planning
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	Workforce Management