DoD Cyber Training Standards - Guidebook

January 2020

Table of Contents

BACKGROUND

The Department of Defense (DoD) must be able to effectively identify, develop, and manage the cyber workforce to overcome new and evolving challenges posed by our adversaries. In support of this objective, the Department published DoD Directive 8140.01 directing the development of qualification standards for military, civilian, and contracted support personnel assigned to cyber work roles.

The DoD Cyber Workforce Qualification and Management Program (hereafter referred to as Qualification Program) consists of baseline qualifications (i.e., education, training, personnel certifications), resident qualifications (i.e., on-the-job qualifications, environment-specific requirements), and continuous professional development. A key requirement for successful implementation of the Qualification Program is the availability of training courses that meet DoD 8140 standards.

As a result, the DoD Office of the DoD Chief Information Officer (CIO) developed terminal learning objectives (TLOs) that align to the DoD Cyber Workforce Framework (DCWF) to support implementation of the Qualification Program. These TLOs establish Enterprise baseline standards for cyber training across the DoD. They will also assist military school houses and training institutions in developing and refreshing cyber training courses, resulting in cost savings and enhancing interoperability of the workforce. This work supports the National Defense Strategy and DoD Cyber Strategy 2018.

Disclaimer

The Cyber Training Standards outlined in this document are intended to serve as a resource for Components in updating or creating training courses. Implementation of the TLOs contained in this document is not mandated by the Department.

CREATION OF TRAINING STANDARDS

Terminal Learning Objectives (TLOs)

With the assistance of cyber subject matter experts (SMEs) across the Department, DoD CIO created TLOs for 53 of 54 of the work roles within the DCWF[1]. TLOs identify broad learning outcomes that learners should be able to demonstrate upon completion of training.

The TLOs are purposefully written at a lower level (i.e., Basic) to ensure a basic understanding of the concept by learners. This approach establishes a common Enterprise baseline, and Components are encouraged to adjust the TLOs to meet their specific mission needs. The number of TLOs in each work role differs based on the number of core tasks and knowledge, skills, abilities (KSAs) for the work role. As a result, there is a minimum of one TLO and a maximum of 6 TLOs per work role.

TLO: Describe strategies for designing a knowledge management framework.

Figure 1: TLO Example

Indicators of Learning (IOLs)

In addition to TLOs, DoD CIO created indicators of learning (IOLs) with the assistance of cyber SMEs. IOLS identify specific learning outcomes that are derived from TLOs. They provide Components with ideas for how learners can demonstrate progress toward meeting TLOs in a training setting.

Each TLO has three corresponding IOLs to reflect these proficiency levels: 1) Basic; 2) Intermediate; and, 3) Advanced. To determine the proficiencies of the IOLs, DoD CIO leveraged *Bloom's Revised Taxonomy of Learning*[2], which arranges learning hierarchically from lower-level cognition to higher-order thought.

Based on Bloom's Taxonomy of Learning in Figure 2, the IOL proficiencies are as follows:

- Basic proficiency correlates with Bloom's Remember and Understand;
- Intermediate proficiency correlates with Apply and Analyze; and,
- Advanced proficiency correlates with Evaluate and Create.

[1] TLOs and IOLs were not created for the Executive Cyber Leadership (901) work role because the task analysis for the work role has not been completed.
[2] For more information about Bloom's taxonomy, see Section 3 of the Appendix.

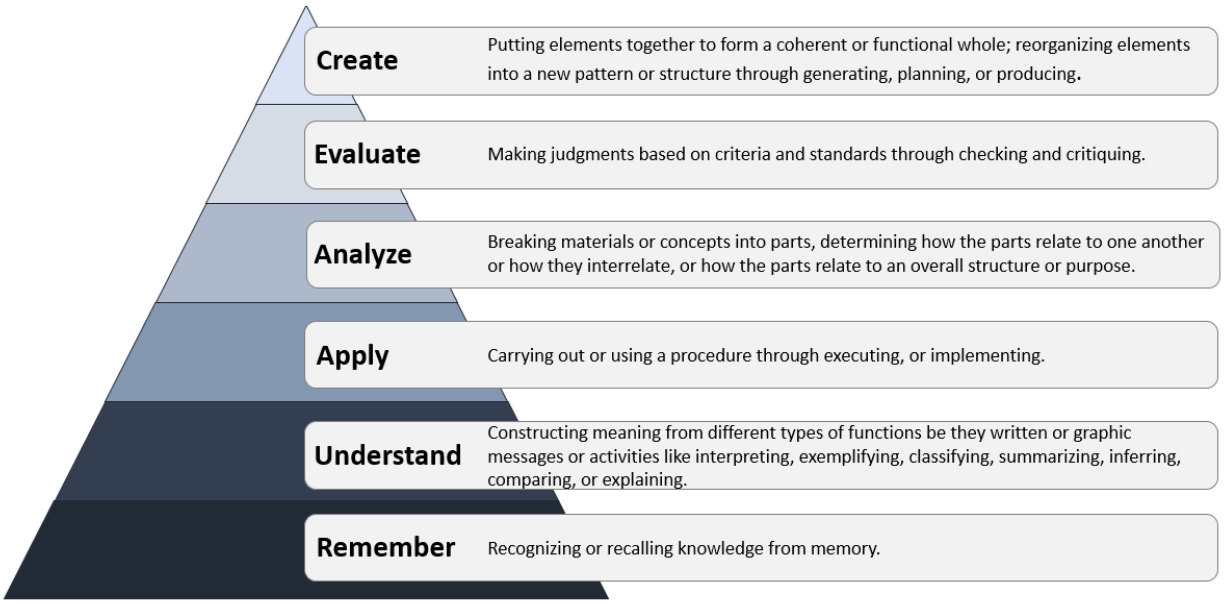

Figure 2: Bloom's Taxonomy of Learning

As with the TLOs, the IOLs serve only as *examples* for Components to leverage when developing and/or updating their own cyber training courses. Table 1 provides an example of a TLO and associated IOLs for the Knowledge Manager work role.

TABLE 1: SAMPLE TRAINING STANDARD FOR KNOWLEDGE MANAGER WORK ROLE

TLO:	**Describe strategies for designing a knowledge management framework.**
Basic IOL	Explain the value of a knowledge management framework to an organization.
Intermediate IOL	Estimate the potential challenges of implementing a new knowledge management framework.
Expert IOL	Evaluate an organization's knowledge management framework.

TRAINING STANDARDS

Overview of DCWF Work Roles

The DCWF serves as the authoritative lexicon for cyber work and supports the identification, development, and qualification of the cyber workforce. It provides standardized qualification criteria to improve interoperability and unity of action throughout the DoD and with mission partners across the nation. Figure 3 shows the DCWF Categories and 53 work roles[3].

Figure 3: DCWF Categories and Work Roles

The work roles are grouped into seven Categories: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate. For the organization of this section, the TLOs and corresponding IOLs are grouped into the same seven categories as the DCWF.

Each of the following seven sections comprise of the TLOs and IOLs developed for each work role.

[3] Terminal learning objectives and indicators of learning were not created for the Executive Cyber Leadership (901) work role because the task analysis for the work role has not been completed.

Authorizing Official/Designating Representative (611)

Work Role Description in DCWF
Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).

1. LO	**Discuss the key functions of the Authorizing Official/Designating Representative role.**
Basic IOL	Explain how Authorizing Officials assess and authorize risk.
Intermediate IOL	Compare the types of tasks Authorizing Officials and Designated Representatives perform and the necessary skills for each.
Advanced IOL	Assess how the Authorizing Official's decisions affect each step in the Risk Management Framework process.
2. LO	**Identify key laws, regulations, policies, and ethics related to cybersecurity.**
Basic IOL	Summarize key laws and regulations related to managing cybersecurity risk.
Intermediate IOL	Assess how improvements to an organization's IT supply chain security and risk management policies could affect its mission.
Advanced IOL	Evaluate an organization's risk management policies to ensure compliance with laws and regulations.
3. LO	**Explain the purpose of authorization boundaries.**
Basic IOL	Explain the importance of authorization boundaries.
Intermediate IOL	Sketch an organization's enterprise information security architecture system.
Advanced IOL	Assess different authorization boundaries and identify key assets with potential Very High or High residual risks.
4. LO	**Explain how the potential impacts of threats are categorized**
Basic IOL	Give examples of how cyber threats and vulnerabilities could affect an organization's operations.
Intermediate IOL	Categorize the potential impact (low, moderate, and high) of cyber threats to an organization's assets.
Advanced IOL	Evaluate whether security categorization decisions align with an organization's mission.
5. LO	**Discuss risk remediation strategies.**
Basic IOL	Give examples of how to protect information systems from cyber threats on an ongoing basis.
Intermediate IOL	Analyze plans for remediating an identified risk.
Advanced IOL	Assess an organization's plans to implement security controls.
6. LO	**Describe the contents of an authorization package.**

Basic IOL	Describe the purpose of each item in an authorization package.
Intermediate IOL	Analyze an authorization package to confirm the level of risk is within an organization's acceptable limits.
Advanced IOL	Evaluate an authorization package to decide whether to issue an Authorization to Operate (ATO) based on organizational requirements.

Security Control Assessor (612)

Work Role Description in DCWF

Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST 800-37).

1. LO	**Discuss the key functions of the Security Control Assessor role.**
Basic IOL	Explain how Security Control Assessors determine if a security control adequately addresses a security issue based on the intent of the security control.
Intermediate IOL	Compare the types of tasks Security Control Assessors perform and the necessary skills.
Advanced IOL	Recommend when Security Control Assessors should assess and reassess controls.
2. LO	**Summarize key laws, regulations, policies, and ethics related to cybersecurity.**
Basic IOL	Summarize policy guidance related to assessing cybersecurity risk.
Intermediate IOL	Estimate the consequences of inadequate or inaccurate assessments.
Advanced IOL	Recommend policies that organizations should adopt to minimize the potential impact of an unethical assessment and enhance the cybersecurity of the organization.
3. LO	**Discuss different methodologies for assessing implemented controls.**
Basic IOL	Describe the qualities of an effective assessment plan.
Intermediate IOL	Create an assessment plan based on an organization's security plan.
Advanced IOL	Evaluate an assessment plan and suggest improvements, including potential policies to ensure effective assessments.
4. LO	**Explain the process for assessing implemented controls.**
Basic IOL	Explain the purpose of assessing implemented controls.
Intermediate IOL	Test whether an implemented control is operating as intended.
Advanced IOL	Evaluate the effectiveness of an implemented control.
5. LO	**Describe the purpose and contents of assessment reports.**
Basic IOL	Describe the qualities of an effective assessment report.
Intermediate IOL	Write an assessment report based on an organization's assessment findings and requirements.
Advanced IOL	Recommend how to respond to identified control deficiencies in an assessment report.
6. LO	**Discuss strategies for reassessing remediated security controls.**
Basic IOL	Give examples of how to monitor remediated security controls.
Intermediate IOL	Recommend qualifications to an organization's security plan after reassessing corrected security controls.
Advanced IOL	Identify residual risk levels based on organization's security assessment report.

Software Developer (621)

Work Role Description in DCWF
Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

1. LO	**Discuss the key functions of the Software Developer role.**
Basic IOL	Give examples of what Software Developers need to know about cybersecurity.
Intermediate IOL	Compare the types of tasks Software Developers perform and the necessary skills.
Advanced IOL	Recommend actions Software Developers can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Describe strategies for designing secure software and applications.**
Basic IOL	Give examples of how to reduce exploitation opportunities in software system designs.
Intermediate IOL	Modify a software system design to include security criteria.
Advanced IOL	Evaluate a software system design for cyber vulnerabilities and threats.
3. LO	**Describe secure coding techniques.**
Basic IOL	Identify common coding flaws.
Intermediate IOL	Solve a coding issue to mitigate risk.
Advanced IOL	Develop an application that can log and handle errors.
4. LO	**Discuss strategies for testing software security.**
Basic IOL	Describe root cause analysis techniques.
Intermediate IOL	Test software for vulnerabilities.
Advanced IOL	Develop software system testing and validation procedures.

Secure Software Assessor (622)

Work Role Description in DCWF
Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

1. LO	**Discuss the key functions of the Secure Software Assessor role.**
Basic IOL	Explain how Secure Software Assessors analyze the security of applications, software, and specialized utility programs.
Intermediate IOL	Compare the types of tasks Secure Software Assessors perform and the necessary skills.
Advanced IOL	Recommend actions Secure Software Assessors can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify the protection needs of information systems.**
Basic IOL	Give examples of security measures that must be taken when a product reaches its end of life.
Intermediate IOL	Analyze software attack surfaces to determine protection needs.
Advanced IOL	Propose application design elements based on security requirements.
3. LO	**Describe secure software testing procedures.**
Basic IOL	Summarize the software quality assurance process.
Intermediate IOL	Modify a secure test plan design according to an organization's requirements.
Advanced IOL	Develop secure software testing and validation procedures that meet an organization's requirements.
4. LO	**Identify strategies for testing the security of applications, software, and specialized utility programs.**
Basic IOL	Describe strategies for testing software security.
Intermediate IOL	Use security tools to test code.
Advanced IOL	Assess software for vulnerabilities.
5. LO	**Discuss potential countermeasures for identified security risks.**
Basic IOL	Give examples of technical countermeasures for identified security risks.
Intermediate IOL	Describe a software patch that would mitigate a risk identified with the software code.
Advanced IOL	Recommend risk management policies and requirements to address identified security risks.

Enterprise Architect (651)

Work Role Description in DCWF

Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

1. LO	**Discuss the key functions of the Enterprise Architect role.**
Basic IOL	Give examples of how Enterprise Architects support enterprise mission needs.
Intermediate IOL	Compare the types of tasks Enterprise Architects perform and the necessary skills.
Advanced IOL	Relate the Enterprise Architect's tasks to the systems engineering process.
2. LO	**Explain how architecture requirements are formed and prioritized.**
Basic IOL	Summarize information technology enterprise architecture concepts.
Intermediate IOL	Relate enterprise architecture requirements to critical business functions.
Advanced IOL	Evaluate enterprise architecture requirements based on organizational goals and objectives.
3. LO	**Describe how to build and implement an enterprise architecture.**
Basic IOL	Explain network security methodologies that are critical for building secure enterprise architectures.
Intermediate IOL	Demonstrate how implementation strategies affect the alignment of enterprise components.
Advanced IOL	Plan an enterprise architecture based on user needs and organizational requirements.
4. LO	**Identify strategies for evaluating enterprise architectures.**
Basic IOL	Summarize regulations, policies, and ethics related to data in transit.
Intermediate IOL	Compare the sketch of a system's architecture with the organization's cybersecurity architecture guidelines.
Advanced IOL	Recommend ways to align an enterprise architecture with an organization's cybersecurity architecture guidelines.

Security Architect (652)

Work Role Description in DCWF
Designs enterprise and systems security throughout the development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

1. LO	**Discuss the key functions of the Security Architect role.**
Basic IOL	Describe how Security Architects translate technology into security designs.
Intermediate IOL	Compare the types of tasks Security Architects perform and the necessary skills.
Advanced IOL	Hypothesize the environmental conditions that affect Security Architects' designs.
2. LO	**Identify the protection needs of systems and networks.**
Basic IOL	List systems security requirements that could apply to each phase in a system's development lifecycle.
Intermediate IOL	Interpret laws and regulations to identify the protection needs of an information system.
Advanced IOL	Write baseline security requirements for an architecture based on organizational goals and objectives.
3. LO	**Describe effective cybersecurity designs for systems and networks.**
Basic IOL	Describe cybersecurity methods that should be applied in a security design.
Intermediate IOL	Demonstrate how to employ secure configuration management processes.
Advanced IOL	Recommend security design elements for a system that processes data with multiple classification levels.
4. LO	**Discuss how to evaluate security architectures.**
Basic IOL	Explain how a security system should work.
Intermediate IOL	Analyze a security design and recommend improvements.
Advanced IOL	Create a security risk management plan based on identified risk.

Research & Development Specialist (661)

Work Role Description in DCWF

Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

1. LO	**Discuss the key functions of the Research & Development Specialist role.**
Basic IOL	Describe how Research & Development Specialists research and develop new capabilities.
Intermediate IOL	Compare the types of tasks Research & Development Specialists perform and the necessary skills, to include any domain expertise.
Advanced IOL	Recommend actions Research & Development Specialists can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify strategies for researching new and emerging cybersecurity technologies.**
Basic IOL	Identify strategies for researching new software systems technologies.
Intermediate IOL	Demonstrate how a new software systems technology meets customer requirements.
Advanced IOL	Evaluate a new technology for potential cybersecurity vulnerabilities.
3. LO	**Discuss best practices for creating new cyber capabilities.**
Basic IOL	Summarize system life cycle management principles.
Intermediate IOL	Illustrate how to apply the systems engineering life cycle process when developing a new capability.
Advanced IOL	Plan a new capability that meets an organization’s mission requirements.

Systems Requirements Planner (641)

Work Role Description in DCWF
Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

1. LO	**Discuss the key functions of the Systems Requirements Planner role.**
Basic IOL	Give examples of how Systems Requirements Planners translate functional requirements into technical solutions.
Intermediate IOL	Compare the types of tasks Systems Requirements Planners perform and the necessary skills.
Advanced IOL	Recommend actions Systems Requirements Planners can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify ways to analyze functional requirements.**
Basic IOL	Describe how functional requirements are determined and refined.
Intermediate IOL	Choose systems requirements based on organizational goals and objectives.
Advanced IOL	Evaluate systems requirements based on cybersecurity laws, regulations, policies, and ethics.
3. LO	**Describe strategies for translating requirements into technical solutions.**
Basic IOL	Explain how to apply security systems engineering principles into the design of a new system.
Intermediate IOL	Practice translating customer requirements into plans for new operational capabilities.
Advanced IOL	Plan or revise the scope and objectives of a project based on customer requirements.

System Testing and Evaluation Specialist (671)

Work Role Description in DCWF

Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

1. LO	**Discuss the key functions of the System Testing & Evaluation Specialist role.**
Basic IOL	Describe how System Testing & Evaluation Specialists assess system requirements, to include determining success criteria.
Intermediate IOL	Compare the types of tasks System Testing & Evaluation Specialists perform and the necessary skills.
Advanced IOL	Recommend actions System Testing & Evaluation Specialists can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Discuss how to collect, interpret, and validate test data.**
Basic IOL	Explain how levels of assurance are determined.
Intermediate IOL	Analyze test data.
Advanced IOL	Assess the validity of test data.
3. LO	**Describe strategies for testing systems.**
Basic IOL	Give examples of auditable evidence of security measures.
Intermediate IOL	Demonstrate how to perform operational testing.
Advanced IOL	Assess a system to determine compliance with specifications and requirements.
4. LO	**Explain how to write test plans.**
Basic IOL	Describe best practices for writing requirements in a test plan (e.g., including success criteria).
Intermediate IOL	Analyze operations-based testing scenarios.
Advanced IOL	Write a test plan.
5. LO	**Identify best practices for reporting test results.**
Basic IOL	Describe how to prepare test and evaluation reports.
Intermediate IOL	Illustrate key points using test data.
Advanced IOL	Recommend actions based on test results.

Information Systems Security Developer (631)

Work Role Description in DCWF
Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

1. LO	**Discuss the key functions of the Information Systems Security Developer role.**
Basic IOL	Give examples of how Information Systems Security Developers evaluate information system security throughout the systems development life cycle.
Intermediate IOL	Compare the types of tasks Information Systems Security Developers perform and the necessary skills.
Advanced IOL	Recommend actions Information Systems Security Developers can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Describe the protection needs of information systems.**
Basic IOL	Explain how cybersecurity principles figure into system requirements.
Intermediate IOL	Estimate the security requirements of a system through its life cycle.
Advanced IOL	Evaluate system requirements based on information technology security principles.
3. LO	**Discuss best practices for designing and developing cybersecurity-enabled products.**
Basic IOL	Describe the elements of an effective security design.
Intermediate IOL	Demonstrate how to incorporate cybersecurity solutions into a systems design.
Advanced IOL	Evaluate a security design based on system life cycle management principles.
4. LO	**Identify strategies for assessing the effectiveness of cybersecurity measures.**
Basic IOL	Explain how to perform a risk analysis.
Intermediate IOL	Use a tool to conduct a vulnerability scan on a system.
Advanced IOL	Evaluate a secure interface between information systems, physical systems, or embedded technologies.
5. LO	**Describe the documentation Information Systems Security Developers create and maintain.**
Basic IOL	Describe documentation related to Risk Management Framework processes.
Intermediate IOL	Modify a Disaster Recovery and Continuity of Operations plan for a system under development to comply with regulations.
Advanced IOL	Write documentation for component and interface specifications.
6. LO	**Describe common cybersecurity risk mitigation strategies.**
Basic IOL	Identify common technical problems with new systems.
Intermediate IOL	Choose the best risk mitigation strategies for identified security risks.
Advanced IOL	Design a countermeasure to an identified security risk.

Systems Developer (632)

Work Role Description in DCWF
Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

1. LO	**Discuss the key functions of the Systems Developer role.**
Basic IOL	Give examples of how Systems Developers test information systems throughout the systems development life cycle.
Intermediate IOL	Compare the types of tasks Systems Developers perform and the necessary skills.
Advanced IOL	Recommend actions Systems Developers can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Describe strategies for creating cybersecurity designs.**
Basic IOL	Summarize engineering principles related to information systems security.
Intermediate IOL	Modify a cybersecurity design so it meets an organization's operational needs and environmental factors.
Advanced IOL	Evaluate a design for an information system based on cybersecurity principles and organizational requirements.
3. LO	**Explain how to assess information systems.**
Basic IOL	Explain cybersecurity laws, regulations, or policies related to assessing information systems.
Intermediate IOL	Analyze an information system to detect cyber threats and vulnerabilities.
Advanced IOL	Evaluate an information system and recommend solutions to mitigate vulnerabilities.

Database Administrator (421)

Work Role Description in DCWF
Administers databases and/or data management systems that allow for the storage, query, and utilization of data.

1. LO	**Describe the Database Administrator role.**
Basic IOL	Explain how Database Administers configure data management systems.
Intermediate IOL	Compare the types of tasks Database Administrators perform and the necessary skills.
Advanced IOL	Recommend actions Database Administrators can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify strategies for monitoring and maintaining optimal database performance.**
Basic IOL	State a best practice for ensuring optimal database performance.
Intermediate IOL	Identify and resolve the root cause of a database malfunction.
Advanced IOL	Recommend changes to a database to optimize performance.
3. LO	**Explain strategies for performing backup and recovery of databases.**
Basic IOL	Give an example of when backup and recovery of a database are required to ensure data integrity.
Intermediate IOL	Compare full and incremental backups.
Advanced IOL	Evaluate a Data Administrator's actions to perform a full database backup and recovery.
4. LO	**Define data administration and management policies and standards.**
Basic IOL	Summarize policies related to data management.
Intermediate IOL	Categorize issues that could arise if an employee does not abide by data management standards.
Advanced IOL	Critique an organization's data administration standards and provide recommendations.

Data Analyst (422)

Work Role Description in DCWF

Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.

1. LO	**Discuss the key functions of the Data Analyst role.**
Basic IOL	Give an example of how Data Analysts examine data from multiple sources to provide new insights.
Intermediate IOL	Compare the types of tasks Data Analysts perform and the necessary skills.
Advanced IOL	Recommend actions Data Analysts can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify strategies for analyzing data requirements and specifications.**
Basic IOL	Identify a data set that complies with data requirements.
Intermediate IOL	Apply knowledge of approved data requirements and specifications to fix discrepancies within a data set.
Advanced IOL	Critique an organization's data requirements and specifications.
3. LO	**Discuss best practices for analyzing data sources based on data analysis and findings.**
Basic IOL	Give an example of a data source.
Intermediate IOL	Conduct a data quality assessment to validate source data.
Advanced IOL	Develop a recommendations report based on data findings.
4. LO	**Recall strategies for assessing the validity of metrics, source/trending data, and recommendations.**
Basic IOL	Identify outliers among a data set using a data analysis tool.
Intermediate IOL	Apply basic descriptive statistics and techniques to identify hidden patterns and/or relationships among two data sets.
Advanced IOL	Assess the validity of recommendations with the source data used to develop them.
5. LO	**List relevant data policies, standards, and procedures.**
Basic IOL	Provide an example of a data standard.
Intermediate IOL	Modify a data set to comply with approved data standards.
Advanced IOL	Assess an organization's data policy and provide recommendations for improvement.

Knowledge Manager (431)

Work Role Description in DCWF
Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

1. LO	**Describe the Knowledge Manager role.**
Basic IOL	Give an example of how Knowledge Managers administer access to intellectual capital and information content.
Intermediate IOL	Compare the types of tasks Knowledge Managers perform and the necessary skills.
Advanced IOL	Recommend actions Knowledge Managers can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Select appropriate knowledge management technologies based upon the needs of end-users.**
Basic IOL	List types of collaborative technologies.
Intermediate IOL	Interpret the needs of an organization's end-users.
Advanced IOL	Evaluate the strengths and limitations of various knowledge management technologies.
3. LO	**Describe strategies for designing a knowledge management framework.**
Basic IOL	Explain the value of a knowledge management framework to an organization.
Intermediate IOL	Estimate the potential challenges of implementing a new knowledge management framework.
Advanced IOL	Evaluate an organization's knowledge management framework.
4. LO	**Discuss best practices for managing and monitoring knowledge management assets and resources.**
Basic IOL	Give an example of how the wrong individual may be given access to explicit organizational knowledge.
Intermediate IOL	Sketch how a knowledge management system can link together libraries of information.
Advanced IOL	Hypothesize the security issues that could arise if an organization disregards PII data security standards.
5. LO	**Identify strategies for constructing access paths to suites of information.**
Basic IOL	Identify examples of access paths.
Intermediate IOL	Outline the steps for creating a link to a page.
Advanced IOL	Hypothesize the root cause of a malfunctioning access path.

Technical Support Specialist (411)

Work Role Description in DCWF

Provides technical support to customers who need assistance utilizing client level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).

1. LO	**Describe the Technical Support Specialist role.**
Basic IOL	Explain how Technical Support Specialists assist customers with hardware and software issues.
Intermediate IOL	Compare the types of tasks Technical Support Specialists perform and the necessary skills.
Advanced IOL	Recommend actions Technical Support Specialists can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Discuss how to create help desk tickets.**
Basic IOL	State the purpose of a ticketing system.
Intermediate IOL	Complete and submit a help desk ticket in a ticketing system.
Advanced IOL	Critique a Technical Support Specialist's actions to resolve a ticket.
3. LO	**Recall best practices for resolving customer reported incidents.**
Basic IOL	Identify the proper solution to a hardware issue.
Intermediate IOL	Analyze complex system problems to identify solutions.
Advanced IOL	Justify a Technical Support Specialist's actions to diagnose and resolve an issue caused by unapproved software.
4. LO	**Describe strategies for configuring and maintaining approved computer related equipment and systems.**
Basic IOL	Discuss how to install hardware, software, and peripheral equipment according to organizational standards.
Intermediate IOL	Analyze the configuration of a network work station to see if it complies with approved standards.
Advanced IOL	Recommend changes to a network's configuration to comply with organizational security policies.
5. LO	**List best practices for administering accounts, network rights, and access to systems and equipment.**
Basic IOL	List the steps for granting an individual access to a SharePoint site.
Intermediate IOL	Demonstrate how to administer network rights to different user roles.
Advanced IOL	Hypothesize the issues that could arise if an organization does not properly manage access to secure systems and equipment.
6. LO	**Assess system performance.**
Basic IOL	List causes of system performance degradation.
Intermediate IOL	Use measures of system performance to identify and resolve a performance issue.
Advanced IOL	Critique a Technical Support Specialist's actions to mitigate a system performance degradation.

Network Operations Specialist (441)

Work Role Description in DCWF
Plans, implements, and operates network services/systems, to include hardware and virtual environments.

1. LO	**Describe the Network Operations Specialist role.**
Basic IOL	Explain how Network Operations Specialists implement new networks within organizations.
Intermediate IOL	Compare the types of tasks Network Operations Specialists perform and the necessary skills.
Advanced IOL	Recommend actions Network Operations Specialists can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Discuss strategies for managing and maintaining network infrastructure.**
Basic IOL	List different types of network commands and functionality.
Intermediate IOL	Install a new network device, making sure that no connectivity issues occur when it is tested.
Advanced IOL	Given a scenario where a LAN/WAN is functioning improperly, reconstruct the network infrastructure to correct the identified malfunction(s).
3. LO	**Identify and resolve network vulnerabilities to safeguard information from threats.**
Basic IOL	Describe STIGs and network vulnerabilities that can be attacked by an outside entity.
Intermediate IOL	Patch a network vulnerability.
Advanced IOL	Design and develop a customized patch for a specialized network.
4. LO	**Identify strategies for monitoring and maintaining network operations (e.g., traffic, capacity, performance, and connectivity issues).**
Basic IOL	List possible measures, methodologies, or indicators of network performance.
Intermediate IOL	Diagnose a network connectivity issue.
Advanced IOL	Given a case study, develop recommendations for how an organization can improve network performance.
5. LO	**Design and develop network backup and recovery procedures.**
Basic IOL	Explain how network infrastructure contingency could be tested.
Intermediate IOL	Leverage industry best practices to write a network and recovery procedure.
Advanced IOL	Critique a network backup and recovery procedure for an organization.

System Administrator (451)

Work Role Description in DCWF
Installs, configures, troubleshoots, and maintains hardware, software, and administers system accounts.

1. LO	**Describe the System Administrator role.**
Basic IOL	Give an example of how System Administrators maintain hardware and software.
Intermediate IOL	Compare the types of tasks System Administrators perform and the necessary skills.
Advanced IOL	Recommend actions System Administrators can take to help mitigate cyber threats and vulnerabilities.
2. LO	**List organizational policies and procedures pertaining to system administration.**
Basic IOL	Explain the importance of standard operating procedures.
Intermediate IOL	Hypothesize the issues that could arise if an organization disregards systems administration standard operating procedures.
Advanced IOL	Evaluate a system administration standard operating procedure and recommend changes to improve it.
3. LO	**Identify strategies for resolving system/server performance issues.**
Basic IOL	Describe a technical problem that can negatively impact system performance.
Intermediate IOL	Diagnose and resolve a software issue.
Advanced IOL	Evaluate a failed server, including the root cause and recommended future action(s).
4. LO	**Recall best practices for managing accounts (e.g., systems, users).**
Basic IOL	List types of user accounts.
Intermediate IOL	Illustrate the protocol for revoking a user account.
Advanced IOL	Modify the privileges of a user who has become an account administrator.
5. LO	**Discuss strategies for managing network rights and access to systems and equipment.**
Basic IOL	Name a type of user who should not be granted access to a secure network.
Intermediate IOL	Write the process for issuing network rights to a new user.
Advanced IOL	Evaluate a process for granting administrative rights to a secure system based on industry best practices.

Systems Security Analyst (461)

Work Role Description in DCWF
Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

1. LO	**Describe the Systems Security Analyst role.**
Basic IOL	Give an example of how Systems Security Analysts integrate systems security.
Intermediate IOL	Compare the types of tasks Systems Security Analysts perform and the necessary skills.
Advanced IOL	Recommend actions Systems Security Analysts can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Discuss organizational and system security posture trends.**
Basic IOL	List possible organizational security posture trends.
Intermediate IOL	Hypothesize how system security posture trends could affect an organization.
Advanced IOL	Appraise an organization's system security posture and provide recommendations for improvement.
3. LO	**Describe methodologies for creating security measures.**
Basic IOL	List types of security measures.
Intermediate IOL	Summarize the types of organizational security measures and the vulnerabilities they can address.
Advanced IOL	Propose an action plan with security measures to stop a recurring security breech.
4. LO	**Explain how to assess configuration management processes and security controls.**
Basic IOL	Define security controls and provide an example.
Intermediate IOL	Compare the types of organizational security controls.
Advanced IOL	Recommend improvements to an organization's configuration and security management process.
5. LO	**Identify relevant cybersecurity requirements, standards, and policies.**
Basic IOL	Provide examples of how cybersecurity requirements and standards safeguard a system against threats.
Intermediate IOL	Analyze cybersecurity policies that can effectively protect an organization from threats.
Advanced IOL	Compare an organization's cybersecurity policies against requirements.
6. LO	**Identify best practices for assessing system security deficiencies.**
Basic IOL	Describe a common security deficiency.
Intermediate IOL	Apply knowledge of security system design tools, methods, and techniques to correct a security deficiency identified during testing.
Advanced IOL	Assess the security of a system.

Cyber Legal Advisor (731)

Work Role Description in DCWF
Provides legal advice and recommendations on relevant topics related to cyber law.

1. LO	**Discuss the key functions of the Cyber Legal Advisor role.**
Basic IOL	Identify who Cyber Legal Advisors counsel.
Intermediate IOL	Compare the types of tasks Cyber Legal Advisors perform and the necessary skills.
Advanced IOL	Explain how Cyber Legal Advisors assist with risk management.
2. LO	**Discuss laws related to cybersecurity.**
Basic IOL	Describe international laws related to cybersecurity.
Intermediate IOL	Interpret laws or regulations to address specific cyber issues.
Advanced IOL	Assess business or military operation plans in terms of applicable cybersecurity laws.

Privacy Compliance Manager (732)

Work Role Description in DCWF
Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

1. LO	**Discuss the key functions of the Privacy Compliance Manager role.**
Basic IOL	Give examples of the guidance that Privacy Compliance Managers provide to senior management.
Intermediate IOL	Compare the types of tasks Privacy Compliance Managers perform and the necessary skills.
Advanced IOL	Summarize key federal privacy laws.
2. LO	**Give examples of who Privacy Compliance Managers collaborate with and why.**
Basic IOL	Describe how Privacy Compliance Managers assist legal counsel.
Intermediate IOL	Illustrate how an organization coordinates efforts to respond to privacy incidents and breaches.
Advanced IOL	Devise a plan for evaluating cyber privacy and security policies and procedures with stakeholders.
3. LO	**Describe the procedures, processes, and programs Privacy Compliance Managers create.**
Basic IOL	Describe the components of an effective internal privacy audit program.
Intermediate IOL	Compare the types of procedures Privacy Compliance Managers develop and manage.
Advanced IOL	Evaluate an organization's process for developing and managing personal acknowledgements from all employees regarding their responsibility to protect PII.
4. LO	**Discuss how Privacy Compliance Managers monitor compliance.**
Basic IOL	Explain how to conduct a Privacy Impact Assessment.
Intermediate IOL	Analyze whether a security incident violates a privacy principle or legal standard and requires specific legal action.
Advanced IOL	Hypothesize how patterns of non-compliance with privacy requirements can impact the security of an organization's cybersecurity program.
5. LO	**Describe how Privacy Compliance Managers mitigate or resolve issues.**
Basic IOL	Describe best practices for preparing audit reports.
Intermediate IOL	Analyze possible sanctions for failure to comply with corporate privacy policies and procedures.
Advanced IOL	Write a corporate privacy policy to resolve an allegation of non-compliance.

Cyber Instructional Curriculum Developer (711)

Work Role Description in DCWF

Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.

1. LO	**Discuss the key functions of the Cyber Instructional Curriculum Developer role.**
Basic IOL	Give examples of training policies and protocols Cyber Instructional Curriculum Developers help craft.
Intermediate IOL	Compare the types of tasks Cyber Instructional Curriculum Developers perform and the necessary skills.
Advanced IOL	Generate a flow chart that illustrates the role of the Cyber Instructional Curriculum Developer throughout the curriculum development process.
2. LO	**Describe best practices for designing and developing cyber training/education courses.**
Basic IOL	Explain how to conduct a learning needs assessment.
Intermediate IOL	Demonstrate how to convert a paper-based cyber scenario into an online activity.
Advanced IOL	Write a cyber-related exercise scenario.
3. LO	**Discuss strategies for evaluating cyber training.**
Basic IOL	Describe methods for measuring the effectiveness of cyber training and education.
Intermediate IOL	Practice reviewing cyber course content and assessments for alignment with training objectives.
Advanced IOL	Create evaluation metrics that tie training outcomes to mission goals.

Cyber Instructor (712)

Work Role Description in DCWF
Develops and conducts training or education of personnel within cyber domain.

1. LO	**Discuss the key functions of the Cyber Instructor role.**
Basic IOL	Give examples of how Cyber Instructors serve as internal consultants and advisors in their own area of expertise
Intermediate IOL	Compare the types of tasks Cyber Instructors perform and the necessary skills.
Advanced IOL	Generate a flow chart that illustrates the role of the Cyber Instructor throughout the curriculum development process.
2. LO	**Describe strategies for designing and developing instructor-led cyber training.**
Basic IOL	Give examples of how to modify cyber training to suit different learning styles.
Intermediate IOL	Modify a cyber curriculum to meet the needs of a target audience.
Advanced IOL	Design a cyber-related exercise scenario.
3. LO	**Identify best practices for conducting cyber training.**
Basic IOL	Identify methods for gauging learner understanding.
Intermediate IOL	Illustrate a complex cyber concept.
Advanced IOL	Compose clear responses to technical cyber questions.
4. LO	**Discuss strategies for evaluating cyber training.**
Basic IOL	Give examples of how to evaluate the effectiveness of cyber training programs.
Intermediate IOL	Analyze whether a lesson plan meets an organization’s goals for cybersecurity training.
Advanced IOL	Evaluate the comprehensiveness of a cybersecurity training program based on an organization’s mission.

Information Systems Security Manager (722)

Work Role Description in DCWF
Responsible for the cybersecurity of a program, organization, system, or enclave.

1. LO	**Discuss the key functions of the Information Systems Security Manager role.**
Basic IOL	Give examples of how Information Systems Security Managers help an organization maintain its security posture.
Intermediate IOL	Compare the types of tasks Information Systems Security Managers perform and the necessary skills.
Advanced IOL	Justify the resources an organization needs to support its IT security goals and objectives and reduce overall risk.
2. LO	**Describe methods for managing policy compliance.**
Basic IOL	Summarize laws, statutes, and policies related to cybersecurity compliance.
Intermediate IOL	Modify an organization's IT policy, plans, instructions, guidance, or standard operating procedures to align it with the organization's mission and goals.
Advanced IOL	Evaluate an organization's method for monitoring policy compliance.
3. LO	**Describe strategies for evaluating system development efforts.**
Basic IOL	Describe strategies for coordinating cybersecurity inspections, tests, and reviews.
Intermediate IOL	Estimate the security implications of a new technology upgrade.
Advanced IOL	Evaluate a development effort to ensure the proper installation of baseline security safeguards.
4. LO	**Discuss systems security requirements.**
Basic IOL	Describe how security requirements for an IT system change through the system's life cycle.
Intermediate IOL	Analyze the cybersecurity requirements listed in an organization's procurement documentation.
Advanced IOL	Choose the best information security strategy to meet an organization's security objective.
5. LO	**Describe techniques for managing security improvement actions.**
Basic IOL	Summarize incident handling methodologies.
Intermediate IOL	Analyze an organization's continuity plans to ensure the integration of cybersecurity requirements.
Advanced IOL	Assess an organization's plan for tracking audit findings and implementing risk mitigation recommendations.

COMSEC Manager (723)

Work Role Description in DCWF
Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI No. 4009).

1. LO	**Discuss the key functions, roles, and responsibilities of the COMSEC Manager role.**
Basic IOL	Give examples of how COMSEC Managers manage the COMSEC resources of an organization.
Intermediate IOL	Compare the types of tasks COMSEC Managers perform and the necessary skills.
Advanced IOL	Propose actions COMSEC Managers can take to help senior leaders manage risk.
2. LO	**Identify methods for managing and safeguarding COMSEC material.**
Basic IOL	Summarize laws, policies, procedures, or governance related to critical infrastructure.
Intermediate IOL	Analyze an organization's process for implementing security improvement actions.
Advanced IOL	Create an EISA for an organization based on its security strategy.
3. LO	**Describe strategies for handling COMSEC security violations and incidents.**
Basic IOL	Give examples of COMSEC security violations.
Intermediate IOL	Analyze an organization's procedures for handling information compromise.
Advanced IOL	Evaluate an organization's continuity of operations strategy.

Cyber Workforce Developer and Manager (751)

Work Role Description in DCWF

Develop 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.

1. LO	**Discuss the key functions of the Cyber Workforce Developer and Manager role.**
Basic IOL	Give examples of how Cyber Workforce Developers and Managers address cyber workforce planning issues.
Intermediate IOL	Compare the types of tasks Cyber Workforce Developers and Managers perform and the necessary skills.
Advanced IOL	Recommend cyber workforce planning strategies based on organizational requirements and workforce trend data.
2. LO	**Describe strategies for closing cybersecurity workforce gaps.**
Basic IOL	Identify ways to assess and forecast manpower requirements.
Intermediate IOL	Compare methods for collecting metrics to monitor cyber workforce readiness.
Advanced IOL	Assess and forecast manpower requirements based on organizational objectives.
3. LO	**Discuss how to develop workforce and position qualification standards.**
Basic IOL	Give examples of workforce and position qualification standards.
Intermediate IOL	Write position descriptions based on established cyber work roles.
Advanced IOL	Create a cyber career field classification structure based on organizational functional requirements and industry standards.
4. LO	**Describe best practices for retaining a cyber workforce.**
Basic IOL	Explain how cyber career paths promote retention.
Intermediate IOL	Sketch a cyber career path that includes career field qualification standards.
Advanced IOL	Justify funding for cyber training resources based on organizational requirements and workforce trend data.
5. LO	**Discuss how to promote organizational cyber workforce compliance required by cyber policies, principles, and practices.**
Basic IOL	Give examples of qualification requirements based on policy to promote organizational compliance.
Intermediate IOL	Identify strategies for coordinating with internal and external subject matter experts to ensure existing qualification standards reflect organizational requirements and industry standards.
Advanced IOL	Recommend a new policy, plan, or strategy to ensure compliance with laws, regulations, policies, and standards in support of organizational cyber activities.

Cyber Policy and Strategy Planner (752)

Work Role Description in DCWF

Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

1. LO	**Discuss the key functions of the Cyber Policy and Strategy Planner role.**
Basic IOL	Give examples of key cyber laws and regulations that Cyber Policy and Strategy Planners need to know.
Intermediate IOL	Compare the types of tasks Cyber Policy and Strategy Planners perform and the necessary skills.
Advanced IOL	Explain how Cyber Policy and Strategy Planners promote awareness of cyber strategies and policies.
2. LO	**Describe best practices for creating cyber strategies.**
Basic IOL	Discuss key points about strategic theory and practice related to cybersecurity.
Intermediate IOL	Analyze how an organization's cyber strategy complies with applicable laws.
Advanced IOL	Create a cyber strategy for an organization that integrates with its vision, mission, and goals.
3. LO	**Identify methods for developing cyber policies.**
Basic IOL	Give examples of how stakeholders assist with cyber policy creation.
Intermediate IOL	Estimate emerging threats that could warrant new cyber policies.
Advanced IOL	Develop a policy that meets an organization's cyber mission and complies with cyber laws.
4. LO	**Identify methods for evaluating cyber programs and policies.**
Basic IOL	Describe ways to monitor how well cyber policies are being followed.
Intermediate IOL	Analyze an organization's process for auditing cyber programs.
Advanced IOL	Hypothesize when a policy needs to be revised or replaced.

Program Manager (801)

Work Role Description in DCWF
Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

1. LO	**Describe the Program Manager role.**
Basic IOL	Explain how Program Managers ensure program alignment with critical agency priorities.
Intermediate IOL	Compare the types of tasks Program Managers perform and the necessary skills.
Advanced IOL	Summarize the role Program Managers serve in the risk management process.
2. LO	**Identify strategies for ensuring supply management efforts address information security requirements.**
Basic IOL	Select the approved methods for acquisition from a list of terms.
Intermediate IOL	Relate procurement efforts to outsourcing efforts.
Advanced IOL	Propose next steps if information security requirements are not addressed during acquisition and procurement activities.
3. LO	**Discuss program management best practices.**
Basic IOL	List the steps to conduct a needs analysis.
Intermediate IOL	Practice balancing an organization's budget using applicable tools and best practices.
Advanced IOL	Recommend actions an IT program manager could take to improve program performance.
4. LO	**Identify methods for managing risk.**
Basic IOL	List risk mitigation strategies for IT programs.
Intermediate IOL	Outline issues that might occur with an IT program if risk is not properly managed.
Advanced IOL	Assess enterprise cybersecurity management guidance in terms of risk.

IT Project Manager (802)

Work Role Description in DCWF
Work that involves directly managing information technology projects to provide a unique service or product.

1. LO	**Describe the IT Project Manager role.**
Basic IOL	Explain how IT Project Managers ensure the delivery of IT projects.
Intermediate IOL	Compare the types of tasks IT Project Managers perform and the necessary skills.
Advanced IOL	Recommend actions IT Project Managers can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Discuss methods for ensuring contracts address security requirements.**
Basic IOL	Provide an example of a security requirement.
Intermediate IOL	Modify draft contract language to ensure it clearly outlines and addresses all system requirements.
Advanced IOL	Critique a service-level agreement (SLA) for how well it defines measures for monitoring a service.
3. LO	**Identify strategies for ensuring supply management efforts address information security requirements.**
Basic IOL	Illustrate the acquisition/procurement lifecycle process.
Intermediate IOL	Categorize potential challenges/issues that might arise if information security requirements are not properly addressed during acquisition and procurement activities.
Advanced IOL	Critique an IT project manager's actions to procure services from an outside vendor against security requirements.
4. LO	**Discuss best practices for managing IT projects.**
Basic IOL	Explain the benefits of conducting a Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis.
Intermediate IOL	Apply resource management principles to modify a project plan created to improve a business process.
Advanced IOL	Design and develop recommendations to minimize risk by leveraging project management best practices.
5. LO	**Discuss strategies for measuring and mitigating security risk.**
Basic IOL	List methods for measuring information security risk.
Intermediate IOL	Practice modifying a system with vulnerabilities using findings from an IT audit.
Advanced IOL	Design upgrades to an IT program that could improve defense against cyber threats.
6. LO	**Describe strategies for delivering services to customers.**
Basic IOL	List techniques for gathering customer feedback.
Intermediate IOL	Differentiate the needs of customers from other stakeholders.
Advanced IOL	Appraise an operating level agreement (OLA) and provide recommendations for improvement.

Product Support Manager (803)

Work Role Description in DCWF
Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

1. LO	**Describe the Product Support Manager role.**
Basic IOL	Explain how Product Support Managers maintain the readiness of systems and components.
Intermediate IOL	Compare the types of tasks Product Support Managers perform and the necessary skills.
Advanced IOL	Summarize the role Product Support Managers serve in the risk management process.
2. LO	**Assess IT programs, projects, and technical systems for vulnerabilities.**
Basic IOL	Identify measures of system performance.
Intermediate IOL	Practice interpreting the findings from an IT program audit and identifying the risks of inaction.
Advanced IOL	Recommend system improvements and/or upgrades that could resolve vulnerabilities.
3. LO	**Identify relevant cybersecurity and risk management policies, requirements, and procedures.**
Basic IOL	Match the risk management policy to the correct description.
Intermediate IOL	Modify a draft supply chain security requirement to mitigate risk.
Advanced IOL	Appraise a set of cybersecurity requirements.
4. LO	**Describe strategies for managing support functions.**
Basic IOL	Recall best practices for managing support functions.
Intermediate IOL	Practice analyzing a budget to identify cost-savings.
Advanced IOL	Design and develop a project plan for implementing an IT system to address administrative and operational needs, such as project scope, cost, and staffing.
5. LO	**Discuss best practices for designing and developing contracts and supporting documentation.**
Basic IOL	Define what a Service Level Agreement (SLA) is and describe how it pertains to contracts.
Intermediate IOL	Modify a section of a contract to address network security.
Advanced IOL	Critique an SLA, identifying weaknesses and areas for improvement.

IT Investment/Portfolio Manager (804)

Work Role Description in DCWF
Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.

1. LO	**Describe the IT Investment/Portfolio Manager role.**
Basic IOL	Explain how IT Investment/Portfolio Managers align a portfolio of IT capabilities with business enterprise priorities.
Intermediate IOL	Compare the types of tasks IT Investment/Portfolio Managers perform and the necessary skills.
Advanced IOL	Recommend actions IT Investment/Portfolio Managers can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify strategies for ensuring supply management efforts address information security requirements.**
Basic IOL	Describe the Federal Acquisition Lifecycle.
Intermediate IOL	Differentiate acquisition activities from procurement activities.
Advanced IOL	Appraise a contract with an external vendor for compliance with information security requirements.
3. LO	**Discuss methods for ensuring that contract language addresses all requirements.**
Basic IOL	Define the sections of a request for proposal (RFP).
Intermediate IOL	Categorize issues that could arise if a contract does not clearly outline system requirements.
Advanced IOL	Evaluate draft language for the performance section of an RFP and offer suggestions for improvement.

IT Program Auditor (805)

Work Role Description in DCWF
Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

1. LO	**Describe the IT Program Auditor role.**
Basic IOL	Explain how IT Program Auditors evaluate IT programs to determine compliance with published standards.
Intermediate IOL	Compare the types of tasks IT Program Auditors perform and the necessary skills.
Advanced IOL	Recommend actions IT Program Auditors can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Discuss strategies for assessing IT programs, projects, and systems for cybersecurity threats.**
Basic IOL	Distinguish between import and export reviews.
Intermediate IOL	Examine a service performance report for potential issues or variances.
Advanced IOL	Review a draft IT program audit report and recommend improvements to strengthen the findings and recommendations.

Cyber Defense Analyst (511)

Work Role Description in DCWF
Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats.

1. LO	**Discuss the key functions of the Cyber Defense Analyst role.**
Basic IOL	Describe how Cyber Defense Analysts adhere to applicable policies, procedures, laws, and regulations.
Intermediate IOL	Compare the types of tasks Cyber Defense Analysts perform and the necessary skills.
Advanced IOL	Formulate actions that can help identify and mitigate cyber threats and vulnerabilities.
2. LO	**Describe cyber defense and vulnerability assessment tools and methodologies.**
Basic IOL	Identify strategies for collecting data from cyber defense resources.
Intermediate IOL	Use network and host-based analysis tools to identify malicious activities.
Advanced IOL	Develop, execute, and evaluate intrusion detection methodologies for detecting network-based intrusions.
3. LO	**Identify methods for analyzing network traffic.**
Basic IOL	Describe the characteristics of a network attack.
Intermediate IOL	Analyze network traffic to identify anomalous, malicious, and benign activity.
Advanced IOL	Reconstruct a network attack to identify exploited vulnerabilities and compare the malicious activity to the benign.
4. LO	**Describe strategies for identifying and evaluating incidents.**
Basic IOL	Identify the steps to evaluate a cyber incident.
Intermediate IOL	Analyze and recommend ways to distinguish malicious incidents from benign activity.
Advanced IOL	Monitor an operational environment and report on adversarial activities that fulfill leadership's priority information requirements.

Cyber Defense Infrastructure Support Specialist (521)

Work Role Description in DCWF
Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

1. LO	**Discuss the key functions of the Cyber Defense Infrastructure Support Specialist role.**
Basic IOL	Give examples of how Cyber Defense Infrastructure Support Specialists maintain infrastructures.
Intermediate IOL	Compare the types of tasks Cyber Defense Infrastructure Support Specialists perform and the necessary skills.
Advanced IOL	Develop an action plan that Cyber Defense Infrastructure Support Specialists can use to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify the protection needs of a cyber environment.**
Basic IOL	Describe the protection needs of an organization's infrastructure.
Intermediate IOL	Analyze the layers and components of an organization's cyber defense infrastructure.
Advanced IOL	Assess an organization's network protection components to develop a secure environment that aligns with the organization's risk posture.
3. LO	**Describe ways to test infrastructure security.**
Basic IOL	Give examples of tools that enhance cybersecurity environments.
Intermediate IOL	Demonstrate how to evaluate cyber defenses.
Advanced IOL	Synthesize cybersecurity assessment results to recommend security enhancements to an organization's infrastructure.
4. LO	**Describe methods for identifying and reporting infrastructure incidents.**
Basic IOL	Give examples of infrastructure ports and associated protocols.
Intermediate IOL	Analyze an organization's access control mechanisms for network security.
Advanced IOL	Evaluate identified vulnerabilities and risk to develop infrastructure security enhancements.

Cyber Defense Incident Responder (531)

Work Role Description in DCWF
Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

1. LO	**Discuss the key functions of the Cyber Defense Incident Responder role.**
Basic IOL	Give examples of how Cyber Defense Incident Responders analyze cyber incidents.
Intermediate IOL	Compare the types of tasks Cyber Defense Incident Responders perform and the necessary skills.
Advanced IOL	Recommend actions that can help identify and mitigate cyber threats and vulnerabilities.
2. LO	**Identify strategies for analyzing incidents.**
Basic IOL	Describe different types of cyber alerts.
Intermediate IOL	Use a cyber analysis tool or capability to analyze an incident.
Advanced IOL	Assess cyber alert and analysis data to determine the extent of a compromise.
3. LO	**Describe strategies for collecting intrusion artifacts.**
Basic IOL	Give examples of intrusion artifacts.
Intermediate IOL	Demonstrate how to collect and preserve evidence according to standard operating procedures or national standards.
Advanced IOL	Assess forensics data for initial infection vectors, indicators of compromise, and mitigation strategies.
4. LO	**Summarize incident response and handling methodologies.**
Basic IOL	Compare the roles and responsibilities of Incident Responders and Incident Handlers.
Intermediate IOL	Analyze strategies for coordinating incident response functions.
Advanced IOL	Develop mitigation strategies for an incident in an after action review.

Vulnerability Assessment Analyst (541)

Work Role Description in DCWF

Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

1. LO	**Discuss the key functions of the Vulnerability Assessment Analyst role.**
Basic IOL	Give examples of how Vulnerability Assessment Analysts measure the effectiveness of defense-in-depth architecture.
Intermediate IOL	Compare the types of tasks Vulnerability Assessment Analysts perform and the necessary skills.
Advanced IOL	Explain the pros and cons of conducting vulnerability assessments from within and outside a network.
2. LO	**Describe methods for conducting technical and nontechnical risk assessments.**
Basic IOL	Describe the focus areas of vulnerability assessments.
Intermediate IOL	Demonstrate how to use an analysis scanning tool to identify vulnerabilities.
Advanced IOL	Assess and classify the vulnerabilities in an application or system.
3. LO	**Discuss strategies for evaluating systems for compliance.**
Basic IOL	Identify key cyber defense auditing policies.
Intermediate IOL	Analyze an application, system, or network for compliance with an organization’s cyber defense policy.
Advanced IOL	Synthesize analysis results from assessments to develop a site’s risk posture.

Warning Analyst (141)

Work Role Description in DCWF
Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

1. LO	**Discuss the key functions of the Warning Analyst role.**
Basic IOL	Give examples of critical target elements in the cyber domain.
Intermediate IOL	Compare the types of tasks Warning Analysts perform and the necessary skills.
Advanced IOL	Evaluate collection plans based on intelligence requirements.
2. LO	**Give examples of how modern technologies, systems, and networks impact cyber operations.**
Basic IOL	Describe the security of different virtualization products.
Intermediate IOL	Estimate how modern digital and wireless communications systems impact cyber operations.
Advanced IOL	Rate the impact of various modern technologies, systems, and networks on cyber operations.
3. LO	**Identify ways to analyze threats.**
Basic IOL	Explain how encryption algorithms work.
Intermediate IOL	Identify threats to Blue Force vulnerabilities and probabilities of exploitation.
Advanced IOL	Evaluate information for reliability, validity, and relevance.

Exploitation Analyst (121)

Work Role Description in DCWF

Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

1. LO	**Discuss the key functions of the Exploitation Analyst role.**
Basic IOL	Summarize national and international laws related to cyber exploitation.
Intermediate IOL	Compare the types of tasks Exploitation Analysts perform and the necessary skills.
Advanced IOL	Create a diagram showing the technical elements of a network that can be penetrated.
2. LO	**Describe how to profile target vulnerabilities.**
Basic IOL	Identify techniques for exploiting targets.
Intermediate IOL	Demonstrate how to profile a network or system administrator's activities.
Advanced IOL	Evaluate technical information to determine whether it could be used to enable remote operations.
3. LO	**Give examples of exploitation strategies.**
Basic IOL	Describe technical or operational vulnerabilities that can be exploited.
Intermediate IOL	Demonstrate how to exploit a vulnerability.
Advanced IOL	Create a strategy that exploits a technical or operational vulnerability.

All-Source Analyst (111)

Work Role Description in DCWF
Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

1. LO	**Discuss the key functions of the All-Source Analyst role.**
Basic IOL	Describe how to accurately and completely source all data used in intelligence, assessment and/or planning products.
Intermediate IOL	Compare the types of tasks All-Source Analysts perform and the necessary skills.
Advanced IOL	Plan and present an intelligence brief in support of a cyberspace operation.
2. LO	**Describe best practices for generating and responding to cyber-related requests for information.**
Basic IOL	Give examples of cyber-related requests for information and collection requirements that apply to All-Source Analysts.
Intermediate IOL	Analyze an organization's cyber-related request for information for clarity, classification, and control marking standards.
Advanced IOL	Create a cyber-related request for information, including research questions and data tracking variables.
3. LO	**Identify strategies for analyzing potential cyber threats and vulnerabilities.**
Basic IOL	Describe common cyber attack methods and techniques.
Intermediate IOL	Use an analytic tool to identify a potential cyber threat.
Advanced IOL	Evaluate data for reliability, validity, and relevance.

Mission Assessment Specialist (112)

Work Role Description in DCWF

Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

1. LO	**Discuss the key functions of the Mission Assessment Specialist role.**
Basic IOL	Identify strategies for monitoring and reporting on threat dispositions and adversarial activities.
Intermediate IOL	Compare the types of tasks Mission Assessment Specialists perform and the necessary skills.
Advanced IOL	Assess the role Mission Assessment Specialists play in risk management.
2. LO	**Describe threats to cyber operations.**
Basic IOL	Give examples of cyber threats and vulnerabilities.
Intermediate IOL	Identify a cyber threat on a network.
Advanced IOL	Hypothesize the operational impacts of cybersecurity lapses on a network.
3. LO	**Discuss strategies for measuring the operational effectiveness of systems.**
Basic IOL	Describe how to extract, analyze, and use metadata.
Intermediate IOL	Conduct a nodal analysis.
Advanced IOL	Create measures of effectiveness to test a system.

Target Developer (131)

Work Role Description in DCWF

Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

1. LO	**Discuss the key functions of the Target Developer role.**
Basic IOL	Give examples of how to characterize targets.
Intermediate IOL	Compare the types of tasks Target Developers perform and the necessary skills.
Advanced IOL	Assess the cybersecurity laws related to the Target Developer role.
2. LO	**Describe strategies for analyzing target systems.**
Basic IOL	Describe critical target elements in the cyber domain.
Intermediate IOL	Analyze target systems.
Advanced IOL	Assess the validity of metadata.

Target Network Analyst (132)

Work Role Description in DCWF

Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

1. LO	**Discuss the key functions of the Target Network Analyst role.**
Basic IOL	Give examples of the physical and logical network devices and infrastructures Target Network Analysts analyze.
Intermediate IOL	Compare the types of tasks Target Network Analysts perform and the necessary skills.
Advanced IOL	Hypothesize how emerging technologies will affect the Target Network Analyst role.
2. LO	**Describe how to identify target threats and vulnerabilities.**
Basic IOL	Describe strategies for gathering information about target networks.
Intermediate IOL	Analyze target vulnerabilities.
Advanced IOL	Assess the validity of metadata.

Target Reporter (133)

Work Role Description in DCWF

Provides synthesized products to customers by researching, analyzing, and reporting in response to customer requirements and in accordance with organization cyber objectives. Collaborates on target-related information and provides feedback to customers as appropriate to relay developments, trends, and/or situational awareness regarding specific targets.

1. LO	**Discuss the key functions of the Target Reporter role.**
Basic IOL	Categorize the physical and logical network devices and infrastructure Target Reporters analyze.
Intermediate IOL	Compare the types of tasks Target Reporters perform and the necessary skills.
Advanced IOL	Hypothesize how modern and emerging technologies could impact cybersecurity.
2. LO	**Give examples of analytic approaches to meeting cyber objectives.**
Basic IOL	Describe how to extract, analyze, and use metadata.
Intermediate IOL	Analyze network data (e.g., router configuration files, routing protocols).
Advanced IOL	Recommend analytic approaches for situations in which information is incomplete.
3. LO	**Discuss target reporting requirements related to cybersecurity.**
Basic IOL	Discuss international laws, regulations, policies, and ethics as they relate to cybersecurity.
Intermediate IOL	Diagram a network in a report format.
Advanced IOL	Evaluate a target report in terms of cyber operation objectives, policies, and legalities.

Multi-Disciplined Language Analyst (151)

Work Role Description in DCWF

Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

1. LO	**Discuss the key functions of the Multi-Disciplined Language Analyst role.**
Basic IOL	Give examples of what Multi-Disciplined Language Analysts transcribe and translate to support cyber action.
Intermediate IOL	Compare the types of tasks Multi-Disciplined Language Analysts perform and the necessary skills.
Advanced IOL	Assess the cyber laws, regulations, and policies that pertain to the Multi-Disciplined Language Analyst role.
2. LO	**Explain networking concepts and protocols.**
Basic IOL	Discuss networking and internet communications fundamentals.
Intermediate IOL	Sketch the architecture of a modern digital network.
Advanced IOL	Create a map of a target network.
3. LO	**Describe threats to cyber operations.**
Basic IOL	Give examples of cyber threats and vulnerabilities.
Intermediate IOL	Analyze metadata for anomalies.
Advanced IOL	Hypothesize the operational impacts of cybersecurity lapses.

All-Source Collection Manager (311)

Work Role Description in DCWF
Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

1. LO	**Discuss the key functions of the All-Source Collection Manager role.**
Basic IOL	Explain how All-Source Collection Managers develop collection plans.
Intermediate IOL	Compare the types of tasks All-Source Collection Managers perform and the necessary skills.
Advanced IOL	Recommend actions All-Source Collection Managers can take to help mitigate cyber threats and vulnerabilities.
2. LO	**State best practices for managing operational planning processes.**
Basic IOL	Give examples of collection management requirements.
Intermediate IOL	Diagnose threats that can arise during the operational planning process if environmental factors and risks are not properly assessed.
Advanced IOL	Evaluate the feasibility of implementing a collection plan based on provided capabilities and limitations.
3. LO	**Identify strategies for determining proper allocation of assets.**
Basic IOL	List factors that an All-Source Collection Manager must consider when allocating collection assets.
Intermediate IOL	Execute resource allocation of collection assets against prioritized collection requirements.
Advanced IOL	Evaluate the allocation of collection assets for effectiveness and efficiency.
4. LO	**Select collaboration tools and forums based on the needs of stakeholders.**
Basic IOL	Give examples of collection forums.
Intermediate IOL	Outline breakdowns in communication that might occur during the coordinating process if collaborative forums are not utilized.
Advanced IOL	Critique two collaboration tools, weighing the strengths and weaknesses of each.
5. LO	**Discuss methodologies for documenting processing, exploitation, and dissemination management activities.**
Basic IOL	List the steps to document exploitation activities.
Intermediate IOL	Write a report outlining processing management activities.
Advanced IOL	Evaluate a report outlining dissemination management activities.

All-Source Collection Requirements Manager (312)

Work Role Description in DCWF

Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

1. LO	**Discuss the All-Source Collection Requirements Manager role.**
Basic IOL	Explain how All-Source Collection Requirements Managers develop effects-based collection requirements strategies.
Intermediate IOL	Compare the types of tasks All-Source Collection Requirements Managers perform and the necessary skills.
Advanced IOL	Recommend actions All-Source Collection Requirements Manager can take to assist with risk management.
2. LO	**Describe strategies for defining collection requirements.**
Basic IOL	Give an example of a collection requirement.
Intermediate IOL	Compare collection requests against collection requirements.
Advanced IOL	Critique a set of collection requirements against intelligence community best practices.
3. LO	**Identify methods for validating collection requirements.**
Basic IOL	Explain the importance of identifying information gaps.
Intermediate IOL	Based on the results of a collection report, modify a collection product to meet requirements.
Advanced IOL	Assess a collection report against outstanding requirements to identify information gaps.

Cyber Intelligence Planner (331)

Work Role Description in DCWF

Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

1. LO	**Discuss the key functions of the Cyber Intelligence Planner role.**
Basic IOL	Give examples of how Cyber Intelligence Planners assist with the Joint Operation Planning Process.
Intermediate IOL	Compare the types of tasks Cyber Intelligence Planners perform and the necessary skills.
Advanced IOL	Propose how Cyber Intelligence Planners can help mitigate potential vulnerabilities in the physical, logical, and cyber-persona layers of networks.
2. LO	**Identify strategies for developing and evaluating a cyber course of action (COA).**
Basic IOL	Describe who Cyber Intelligence Planners work with to analyze the mission, identify requirements, and determine a COA.
Intermediate IOL	Write cyber intelligence requirements based on an organization's leadership and cyber operational objectives.
Advanced IOL	Recommend a COA after comparing several COAs designed to provide intelligence support to an organization's cyber operations.
3. LO	**Describe methods for developing, reviewing, and presenting intelligence plans and products.**
Basic IOL	Give examples of how to measure the effectiveness of cyber intelligence plans and products.
Intermediate IOL	Modify an organization's cyber intelligence plans based on intelligence requirements, operational objectives, and threat factors.
Advanced IOL	Defend a cyber intelligence plan or product.

Cyber Operations Planner (332)

Work Role Description in DCWF

Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

1. LO	**Discuss the key functions of the Cyber Operations Planner role.**
Basic IOL	Identify issues that could affect cyber operations planning strategies and policies.
Intermediate IOL	Compare the types of tasks Cyber Operations Planners perform and the necessary skills.
Advanced IOL	Summarize how targeting selection, validation, and synchronization influence cyber operations planning.
2. LO	**Identify best practices in cyber operations planning.**
Basic IOL	Describe how Cyber Operations Planners incorporate organization objectives, leadership priorities, and decision-making risks into cyber operations plans.
Intermediate IOL	Analyze strategies for evaluating an organization's cyber operations plans.
Advanced IOL	Modify an organization's operations plans based on measures of effectiveness.
3. LO	**Describe strategies for integrating internal and external partners into cyber operations planning.**
Basic IOL	Give examples of how Cyber Operations Planners assist external partners.
Intermediate IOL	Identify decision points in which cyber operations planning must be synchronized and integrated with internal and external partners.
Advanced IOL	Recommend best practices for integrating cyber planning efforts with other organizations.

Partner Integration Planner (333)

Work Role Description in DCWF

Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

1. LO	**Discuss the key functions of the Partner Integration Planner role.**
Basic IOL	Give examples of how Partner Integration Planners assist with the Joint Operation Planning Process.
Intermediate IOL	Compare the types of tasks Partner Integration Planners perform and the necessary skills.
Advanced IOL	Propose how Partner Integration Planners can help mitigate potential vulnerabilities in the physical, logical, and cyber-persona layers of networks.
2. LO	**Identify cybersecurity laws, regulations, policies, and guidance that affect Partner Integration Planners.**
Basic IOL	Explain how a specific law or regulation applies to an organization's cyber objectives.
Intermediate IOL	Compare international cybersecurity laws related to an organization's cyber operations with international partners.
Advanced IOL	Review and defend or modify an organization's staffing policy.
3. LO	**Discuss best practices for building integrated cyber teams.**
Basic IOL	Explain how Partner Integration Planners assist with building integrated cyber teams.
Intermediate IOL	Compare and select external partners for an organization's cyber team based on operational objectives, partner resources and capabilities, and common cyber operations interests.
Advanced IOL	Create a strategy for building an integrated cyber team based on an organization's cyber operations objectives.

Access Network Operator (321)

Work Role Description in DCWF

Conducts access collection, processing, and/or geolocation of wired or wireless computer and digital networks in order to exploit, locate, and/or track targets of interest.

1. LO	**Discuss the key functions of the Access Network Operator role.**
Basic IOL	Explain how Access Network Operators leverage access collection to monitor targets of interest.
Intermediate IOL	Compare the types of tasks Access Network Operators perform and the necessary skills.
Advanced IOL	Recommend actions Access Network Operators can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Describe strategies for infiltrating and exploiting target networks (i.e., wire, wireless, or digital).**
Basic IOL	Give examples of how network devices can be exploited.
Intermediate IOL	Construct a plan to exploit a target's wireless network.
Advanced IOL	Use tools to test a digital network's ability to be exploited.
3. LO	**Identify vulnerabilities within a network.**
Basic IOL	Describe how wireless access points can be vulnerable to cyber attacks.
Intermediate IOL	Diagnose vulnerabilities in a digital network.
Advanced IOL	Recommend actions that could be taken to strengthen a network against vulnerabilities.
4. LO	**Discuss best practices for gaining access to target systems and technologies.**
Basic IOL	List common tools used to gain access to target systems.
Intermediate IOL	Diagnose the access points to a target operational architecture.
Advanced IOL	Recommend an automated system for gaining access to a specific target's system.
5. LO	**Recall strategies for collecting open source data.**
Basic IOL	List limitations to collection management.
Intermediate IOL	Compare common online tools used to conduct open source data collection.
Advanced IOL	Propose a plan for collecting open source data on a designated target.

Interactive Operator (322)

Work Role Description in DCWF
Performs network navigation, tactical forensic analysis, collection of intelligence information, and, when directed, executing on-net operations.

1. LO	**Discuss the key functions of the Interactive Operator role.**
Basic IOL	Explain how Interactive Operators perform tactical forensic analysis.
Intermediate IOL	Compare the types of tasks Interactive Operators perform and the necessary skills.
Advanced IOL	Recommend actions Interactive Operators can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Summarize best practices for monitoring networks and identifying vulnerabilities.**
Basic IOL	Explain how vulnerabilities within a network are identified.
Intermediate IOL	Use a cyber tool to diagnose the root cause of a network vulnerability.
Advanced IOL	Recommend specific tools, techniques, or procedures for analyzing and exploiting identified vulnerabilities.
3. LO	**List strategies for monitoring operational architecture.**
Basic IOL	Define operational architecture.
Intermediate IOL	Diagnose access points in a target operational architecture.
Advanced IOL	Design and develop a methodology for identifying access points within an operational architecture.
4. LO	**Describe methodologies for writing and editing simple scripts.**
Basic IOL	Identify the programming language used in a script.
Intermediate IOL	Modify a script so that it functions properly.
Advanced IOL	Create a simple script for processing a specified data set.
5. LO	**Give examples of how on-net and off-net activities are used to control and exfiltrate data from deployed technologies.**
Basic IOL	Identify off-net activities.
Intermediate IOL	Compare on-net and off-net activities as they relate to exfiltrating data from deployed technologies.
Advanced IOL	Assess security and risk-based concerns related to accessing and controlling on-net systems and exfiltrating target data.

Cyber Crime Investigator (221)

Work Role Description in DCWF
Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

1. LO	**Discuss the key functions of the Cyber Crime Investigator role.**
Basic IOL	Give examples of how Cyber Crime Investigators collect digital evidence.
Intermediate IOL	Compare the types of tasks Cyber Crime Investigators perform with other investigative roles.
Advanced IOL	Categorize the tools and equipment Cyber Crime Investigators use to catalog, document, extract, collect, package, and preserve digital evidence.
2. LO	**Identify strategies for collecting and preserving evidence used to prosecute computer crimes.**
Basic IOL	State the procedure for establishing chain of custody for digital evidence.
Intermediate IOL	Practice preserving digital evidence.
Advanced IOL	Evaluate an investigator's handling of digital evidence based on laws and guidelines.
3. LO	**Describe methods for investigating network intrusions.**
Basic IOL	Discuss best methods for identifying the perpetrator(s) of a network intrusion.
Intermediate IOL	Analyze evidence to identify the perpetrator(s) of a network intrusion.
Advanced IOL	Assess the evidentiary value of data collected from a network intrusion.
4. LO	**Describe methods for analyzing cyber crimes.**
Basic IOL	Identify elements of proof of a cybersecurity crime.
Intermediate IOL	Analyze evidence to identify the perpetrator(s) of a cyber crime.
Advanced IOL	Assess recovered data for information about a potential threat.

Forensics Analyst (211)

Work Role Description in DCWF
Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

1. LO	**Discuss the key functions of the Forensics Analyst role.**
Basic IOL	Give examples of key laws that apply to forensics analysis.
Intermediate IOL	Compare the types of tasks Forensics Analysts perform with other investigative roles.
Advanced IOL	Recommend actions Forensics Analysts can take to help mitigate cyber threats and vulnerabilities.
2. LO	**Identify best practices for handling and preserving evidence.**
Basic IOL	Illustrate how to collect, package, transport, and store electronic evidence.
Intermediate IOL	Use equipment to extract digital evidence.
Advanced IOL	Create a forensically sound duplicate of evidence.
3. LO	**Describe methods for analyzing network intrusions.**
Basic IOL	Explain how to analyze different parts of a system (e.g., memory, log files, etc.) to identify perpetrator(s) of a network intrusion.
Intermediate IOL	Analyze a forensic image or other data source for recovery of potentially relevant information.
Advanced IOL	Assess a network intrusion by performing multiple analyses.

Cyber Defense Forensics Analyst (212)

Work Role Description in DCWF

Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

1. LO	**Discuss the key functions of the Cyber Defense Forensics Analyst role.**
Basic IOL	Give examples of how Cyber Defense Forensics Analysts investigate computer security incidents.
Intermediate IOL	Compare the types of tasks Cyber Defense Forensics Analysts perform with other investigative roles.
Advanced IOL	Recommend best practices Cyber Defense Forensics Analysts can leverage to capture and preserve evidence.
2. LO	**Describe tools used to capture intrusion data.**
Basic IOL	Describe data carving tools and techniques.
Intermediate IOL	Use a binary analysis tool to test application security.
Advanced IOL	Investigate an intrusion using a forensic tool suite.
3. LO	**Identify methods for analyzing data.**
Basic IOL	Describe how and when to conduct a bit-level analysis.
Intermediate IOL	Analyze a memory dump to extract information.
Advanced IOL	Evaluate strategies for conducting forensic analyses in multiple operating system environments.

Appendices

1 Acronym List

ARCYBER	Army Cyber Command
CIO	Chief Information Officer
DC3	Department of Defense Cyber Crime Center
DCTA	DC3 Cyber Training Academy
DCWF	DoD Cyber Workforce Framework
DISA	Defense Information Systems Agency
DoD	Department of Defense
IOL	Indicator of Learning
KSA	Knowledge, Skill, and Ability
NIST	National Institute of Standards and Technology
NSA	National Security Agency
TLO	Terminal Learning Objective

DoD Components

Members of the DoD Enterprise, to include but not limited to: the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Department of Defense Agencies, field activities, and all other organizational entities in the Department of Defense.

Work Roles

Describes a distinct set of activities and attributes needed for the successful execution of work. A person may perform one or more work roles within their assigned position, billet, or contracted service requirement.

Knowledge, Skills, and Abilities (KSAs)

Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training.

Knowledge is a body of information applied directly to the performance of a function. Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual. Ability is competence to perform an observable behavior or a behavior that results in an observable product.

Tasks

A Task is a specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role.

Terminal Learning Objectives (TLOs)

A terminal learning objective identifies a broad learning outcome that learners will be able to demonstrate upon the completion of training. Terminal learning objectives must be achievable and realistic. TLOs will establish Enterprise, baseline standards for cyber training across the DoD. Terminal learning objectives were designed and developed for each of the 53 roles within the DCWF. There is a minimum of one learning objective and a maximum of six learning objectives per work role. The variation of learning objectives was dependent upon the core Tasks and KSAs for each role

Indicators of Learning (IOLs)

An indicator of learning identifies a specific learning outcome that is derived from the terminal learning objective. IOLs signal that a learner is tracking progress toward a particular TLO.

Each terminal learning objective has three corresponding indicators of learning, which are leveled at three proficiency levels: 1) Basic, 2) Intermediate, and 3) Advanced. The indicators of learning are meant to serve only as examples for Components to leverage when developing/updating their own courses to meet the terminal learning objectives

Proficiency Levels

A proficiency level Illustrates a learner's performance expectations and competency, whether basic, intermediate, or advanced:

- Basic - At this level, the role requires an individual to have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance.
- Intermediate - At this level, the role requires an individual to have extensive knowledge of basic concepts and processes and experience applying these with only periodic high-level guidance. An individual must be able to perform successfully in non-routine and sometimes complicated situations.
- Advanced - At this level, the role requires an individual to have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance. An individual must be able to serve as a resource and provide guidance to other.

3 Bloom's Revised Taxonomy of Learning

The levels of Bloom's Revised Taxonomy of Learning are as follows:

Level	Description
1. Remember	Recognizing or recalling knowledge from memory. Remembering is when memory is used to produce or retrieve definitions, facts, or lists, or to recite previously learned information.
2. Understand	Constructing meaning from different types of functions be they written or graphic messages or activities like interpreting, exemplifying, classifying, summarizing, inferring, comparing, or explaining.
3. Apply	Carrying out or using a procedure through executing or implementing. *Applying* relates to or refers to situations where learned material is used through products like models, presentations, interviews or simulations.
4. Analyze	Breaking materials or concepts into parts, determining how the parts relate to one another or how they interrelate, or how the parts relate to an overall structure or purpose. Mental actions included in this function are *differentiating, organizing, and attributing,* as well as *being able to distinguish between* the components or parts. When one is analyzing, he/she can illustrate this mental function by creating spreadsheets, surveys, charts, or diagrams, or graphic representations.
5. Evaluate	Making judgments based on criteria and standards through checking and critiquing. Critiques, recommendations, and reports are some of the products that can be created to demonstrate the processes of evaluation. In the newer taxonomy, *evaluating* comes before creating as it is often a necessary part of the precursory behavior before one creates something.
6. Create	Putting elements together to form a coherent or functional whole; reorganizing elements into a new pattern or structure through generating, planning, or producing. Creating requires users to put parts together in a new way or synthesize parts into something new and different creating a new form or product. This process is the most difficult mental function in the new taxonomy.

4 Reference List

- Anderson, L.W., Krathwohl, D.R., Airasian, P.W., Cruikshank, K.A., Mayer, R.E., Pintrich, P.R., Raths, J., Wittrock, M.C. (2001). *A Taxonomy for Learning, Teaching, and Assessing: A revision of Bloom's Taxonomy of Educational Objectives*. New York: Pearson, Allyn & Bacon.
- Department of Defense. (2018). Summary: Department of Defense Cyber Framework 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
- Executive Office of the President of the United States. (2018, September). National Cyber Strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- National Institute of Standards and Technology – U.S. Department of Commerce. Newhouse, W.; Keith, S.; Scribner, B.; & Witte, G. (2017, August). National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication 800-181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
- Anderson, L.W., Krathwohl, D.R., Airasian, P.W., Cruikshank, K.A., Mayer, R.E., Pintrich, P.R., Raths, J., Wittrock, M.C. (2001). *A Taxonomy for Learning, Teaching, and Assessing: A revision of Bloom's Taxonomy of Educational Objectives*. New York: Pearson, Allyn & Bacon.