DoD 8140 Cyber Workforce Qualification Program

Approval Process for Certifications and Training

Version 1.1
issued on 31 October, 2023

Prepared by
The Office of the DoD Deputy Chief Information Officer for Resources & Analysis,
Workforce Innovation Directorate

Table of Contents

Governance

Pursuant to the Department of Defense Manual (DoDM) 8140.03, "Cyberspace Workforce Qualification and Management Program," this Certification or Training Approval Process describes formal mechanisms to advance the DoD 8140 Cyber Workforce Qualification Program.

The Cyber Workforce Management Board (CWMB), Tri-Chaired by the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)), the DoD Principal Cyber Adviser (PCA) and the DoD Chief Information Officer (CIO), serves as the principal governance body to manage the DoD Cyber Workforce.

To learn more about the DoD 8140 Policy Series, visit us on the DoD Cyber Exchange at:

https://public.cyber.mil/wid/cwmp/

In accordance with the DoD Directive (DoDD) 8140.01, "Cyberspace Workforce Management," the Office of Primary Responsibility (OPR) for each DoD Component should evaluate and recommend requirements for any undefined areas or content. The DoD CIO serves as the impartial facilitator of the DoD 8140 Program by avoiding any direct influence on the evaluation and validation activities.

Introduction

The DoD CIO Workforce Innovation Directorate (WID) serves as the CWMB Secretariate and with the other members of the CWMB, manages and oversees the DoD 8140 Qualification Process for the DoD cyber workforce elements including: information technology (IT) (cyber), cybersecurity, cyber enablers, cyber effects, cyber (intel), data/artificial intelligence (AI) and software engineering.

The CWMB has established an open and continuous process available for interested certification and training providers supporting elements of the DoD Cyber Workforce. The online application process for nominating certification or training consists of four progressive parts. Each part captures key information about the Provider and their offerings. The automated assessment step is advanced by artificial intelligence (AI) applied to input and data and includes opportunities for the provider to add self-evaluation and comments. Once the completed application is submitted, the DoD CIO WID reviews the report findings, and releases a verdict of "accepted" or "declined" along with next steps.

Throughout the process, text and email notifications will inform the provider with status updates to the contacts specified and will be available on the online DoD 8140 Marketplace.

Online resources that can help provide an understanding of the requirements needed to achieve an approved certification or training for use by the DoD cyber workforce in accordance with DoDM 8140.03 are listed below:

- *DoDD 8140.01, "Cyberspace Workforce Management"*
  https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf?ver=2019-06-06-120639-863

- *DoDM 8140.03, "Cyberspace Workforce Qualification and Management Program"*
  https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/814003p.PDF?ver=Yi_dR4VeVd7-yxrty2REFQ%3D%3D

- *DoD Cyber Workforce Framework (DCWF)*
  https://public.cyber.mil/cw/dcwf/
  https://dl.dod.cyber.mil/wp-content/uploads/trn/online/dcwf-overview/story.html

- *Carnegie Mellon, Eberly Center Teaching Excellence & Educational Innovation Version of Bloom's Taxonomy*
  https://www.cmu.edu/teaching/designteach/design/bloomsTaxonomy.html

- *DoD 8140 Qualification Approval Process Information and Registration Page*
  https://www.dodemergingtech.com/dod-cyber-workforce-qualification-program/

- *DoD 8140 Marketplace*
  https://www.avuedigitalservices.com/casting/aisearch/control/cyberWorkforceProviderMarketPlace

Guidelines for Assessing Exam Proficiency and Course Content against DCWF Work Roles and Core KSATs

Prior to the decision to nominate a certification or training for consideration for the DoD Cyber Workforce, the provider should analyze and compare the certification and/or training exam proficiency level to the DCWF knowledge, skills, abilities, and tasks (KSATs) that are designated as "core" for that DCWF work role. The provider should ensure that the certification or training exam assesses proficiency in at least 70% of the core KSATs. For each DCWF work role aligned to the certification or training offering, the offering must achieve a score of 70% or better to be approved for use in accordance with DoDM 8140.03.

If the certification or training offering does not achieve proficiency in at least 70% of the core KSATs for the DCWF work role, the offering is not ready and will require modification prior to approval for use. A certification or training offering may be used in tandem with another certification or training offering to achieve proficiency in at least 70% of the core KSATs for the given DCWF work role.

A nominated certificate/training program must directly train towards the DCWF work role(s) (not 2% training towards DCWF work role and 98% training towards unrelated topics.

In addition to the core KSATs for each DCWF work role, there are other, non-core KSATs which are beneficial but not included in the calculation to achieve proficiency in at least 70% of the core KSATs for a DCWF work role. To perform the initial self-assessment of the certification and/or exam proficiency against the DCWF work roles and core KSATs, it is recommended that the provider follow these steps:

For this document, "suitability" means that each of the core requirements needed to perform the DCWF work role as defined by the core KSATS are directly and adequately addressed by the certification or training offering.

1. Identify the DCWF work role that best aligns to the certification or training offering. The certification or training offering must demonstrate alignment with at least one DCWF work role. Compare the certification or training exam information against the relevant DCWF categories, work roles and their core KSATs to determine if the certification or training offering sufficiently aligns to the DCWF work role to achieve a 70% alignment score of the KSATs.
2. For the chosen DCWF work role(s) that align to the certification or training offering, determine whether each of the DCWF work role's core KSATs are suitable for the certification or training offering. For example, it may not be realistic to expect a cyber certification exam or course objectives to address a DCWF work role's core KSAT that requires the ability to "lead a team." A specific core KSAT should be excluded from the set of KSATs for the

aligned certification or training offering if the DCWF work role core KSAT is outside the scope of the certification or training offering. The DCWF work role KSAT that is outside the scope of the certification or training offering (i.e., "lead a team"), would need to be met through a separate qualification method (e.g., certification, training, or experience). Alternately, the KSAT not met by the certification or training offering may be assumed part of the 30% score that will not achieve the 70% approval. The suitability analysis step should be completed for each KSAT within the DCWF work roles aligned to the certification or training offering.

3. For each of the core KSATs, determine the degree to which the core KSAT is fully or partially covered by one or more of the certification and training exam proficiency objectives (i.e., specific proficiency objectives). Map the evaluation of how each core KSAT for a specific DCWF work role is addressed by which exam or course questions and objectives.
4. A single core KSAT can be covered by one or more exam objectives, and an exam objective can be used to address multiple core KSATs.
5. Assess, and if necessary, extrapolate details using the available exam or course content to determine whether the description of a specific objective could reasonably be expected to satisfy a given core KSAT.
6. Consider the exam objectives that correlate to a skill or task in the DCWF work role description:
    a. Whether the experience and knowledge required of a person is sufficient to correctly and adequately satisfy the exam objectives; and
    b. Whether the exam objectives provide and/or enhance the person's understanding and comprehension such that they would be better able to identify, apply, analyze, demonstrate, and evaluate situations related to carrying out the core KSATs required for the DCWF work role.
7. Consider "prerequisite" knowledge required and determine whether prerequisites are needed prior to achieving a certification or training. For advanced level cyber certifications in particular, the exams or course objectives often do not explicitly address fundamental core KSATs that are either assumed or not directly applicable to specialized skill sets. For instance, forensics analysts or penetration testing certification offerings may not explicitly address core KSATs pertaining to cyber defense in-depth concepts or basic computer protocols, but it may be reasonable to expect an individual holding such a certification to have that knowledge or proficiency.
8. Document and tabulate the core KSATs that are covered by the exam information material.
9. The overall evaluation score is calculated as a ratio of the number of core KSATs that are covered by the exam proficiency to the total number of core KSATs. In accordance with DoD 8140.03, to achieve approval, the overall evaluation must meet or exceed 70% proficiency of the core KSATs for a DCWF work role

Online Certification or Training Approval Process Part 1: Getting Started

Figure 1: Cyber Workforce Qualification Program Screenshot

The Provider will be asked to submit the following details about the certification or training offering:

a. Basic information about Provider's organization including Data Universal Numbering System (DUNS)/Unique Entity ID (UEI), Employer Identification Number (EIN), socio-economic status, points of contact, and other identifying data.
b. Any mapping of the Provider's offering to the DoD Cyber Workforce Framework (DCWF) and alignment with DoDM 8140.03, "Cyberspace Workforce Qualification and Management Program." This will include a detailed analysis of the core KSATs by DCWF work role.
c. Narrative descriptions of the Provider's offering.
d. Terminal Learning Objectives (TLOs), Enabling Learning Objectives (ELOs), exam objectives, and proficiency levels. DoD uses the Carnegie Mellon, Eberly Center Teaching Excellence & Educational Innovation version of Bloom's taxonomy.
e. Providers that return to submit additional certification or training offerings may search and update the organization's and subject matter expert's (SMEs) detailed information for each submission.

Any commercial organization that provisions personnel credentials (the Provider) can submit a certification or training offering for evaluation against the DoD Cyber Workforce Framework (DCWF) if the Provider and the candidate certification or training offering meet the following criteria:

a. The Provider, as the certification body, is a legal entity and accredited to the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 17024 standard "Conformity Assessment - General Requirements for Bodies Operating Certification of Persons." Federal agencies are considered legal entities.

b. The DoD 8140-candidate certification/assessment is accredited to the ISO/IEC 17024 standard. Accreditors of personnel certification programs are accreditation bodies recognized by the DoD.

c. The DoD 8140-candidate training offering is accredited to the ISO/IEC 17011 standard. Accreditors of training programs are accreditation bodies recognized by the DoD.

d. The certification or training offering is likely to be a good match for one or more of the DCWF work roles and at the basic, intermediate, or advanced proficiency levels.

DoD Component sponsorship of a candidate certification or training offering is no longer required for the qualification process. DoD Components interested in tracking the status of a specific certification or training offering may flag the application to receive status updates.

How to Apply:

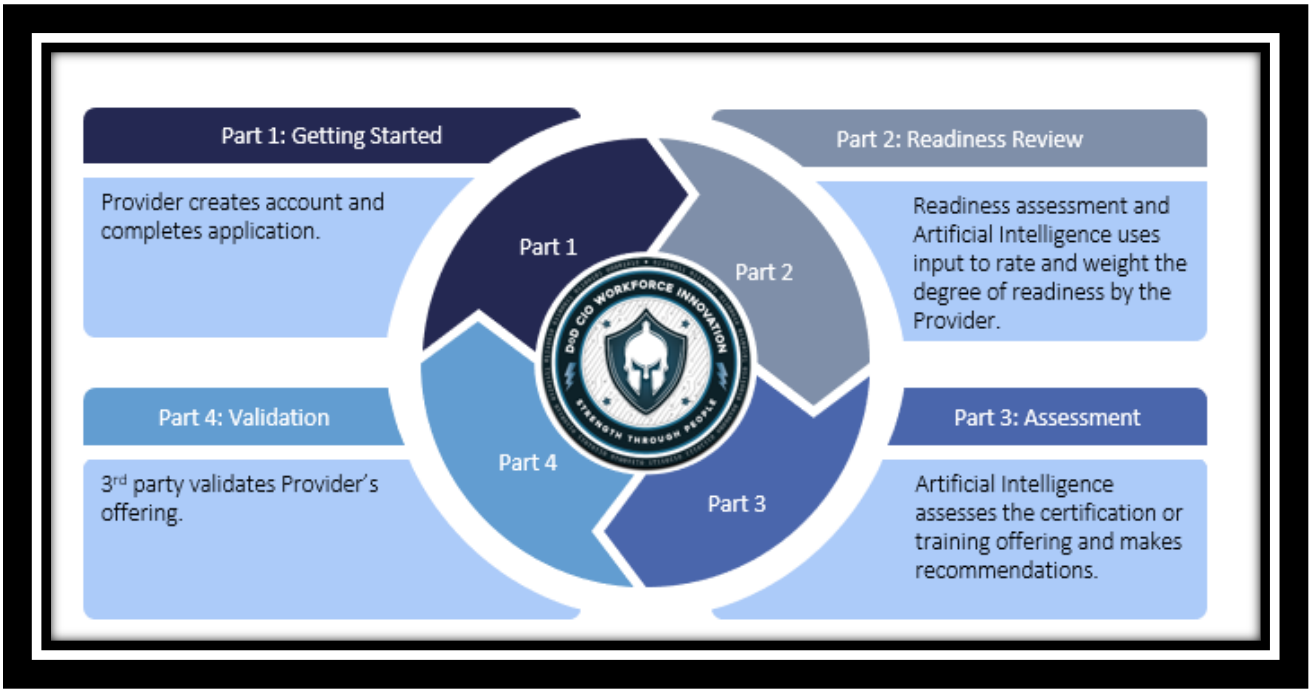

Figure 2: Online Certification or Training Approval Process

1. The Provider may express interest in applying by completing the application at the following link: *https://www.dodemergingtech.com/dod-cyber-workforce-qualification-program/*

   Scroll down the page to the "I'M INTERESTED" button to start the application process. There are also links to additional resources on the same page.

Figure 3: I'm Interested button

2. Sign up for a DoD 8140 Cyber Workforce Qualification Program Application account. The applicant will create a UserID and Password on the New Registration screen, plus choose a Verification Question and Verification Answer for account recovery, if needed. After the applicant submits the registration information, they are routed to the Home Screen.

Figure 4: Account Registration Screen

1. The online application process consists of three progressive parts. Each part captures information about the applicant's organization, program, and training course(s), certification(s), and degree program(s).

2. Click "Start My Application" to begin Part 1: Statement of Interest.

3. On this screen, the applicant provides information about the organization. Questions requiring a mandatory response are marked by an asterisk (*) and the font in red color. If the applicant attempts to move on to Part 2 without answering a question requiring a mandatory response will receive an on-screen prompt alerting them that all questions have not been answered.

4. Should the applicant have any questions regarding the application, there is a red Live Chat button on the right side of the browser screen. Clicking this will connect you with an online agent who will answer questions or determine whether to escalate issues for resolution.

5. After completion of Part 1, the applicant can click "Save and Continue" to move on to Part 2: Readiness Assessment.

Online Certification or Training Approval Process Part 2: Readiness Review

The readiness review will help determine the Provider's readiness for the Certification or Training Approval Process in accordance with DoDM 8140.03. The readiness review is an automated step supported by AI that uses input to weight and rate the degree to which the Provider is ready to submit a complete application.

Part 2 will run the Provider's submitted application against predefined requirements to generate a readiness score that assesses the Provider's organizational capability to deliver a quality and enduring certification or training offering for use by the DoD. The readiness score will be used to ensure a standardized, consistent, transparent, and timely review using multiple variables, conditions, and criteria across numerous certification and training offerings and DCWF work roles.

Key elements that will be considered are:

1. Previously approved certifications or trainings that indicate an in-depth understanding of the Certification or Training Approval Process.

    - How the offering Provider's organization has been validated as a credentialing body. In addition to providing documentation of the credentialing organization's validation, the Provider can demonstrate the type of validation data collected and the type of validation reports generated for DoD.
    - The Provider's submitted method used to evaluate the validation as a credentialing body must include example documentation and demonstration spanning the last three years. The offering must have been in existence for at least three consecutive years with data for at least one year of graduates or participants that have completed the Provider's program.
    - The 3rd party validator will validate the evaluation of the credentialing body.

2. The Provider's self-assessed mapping to the DCWF categories, work roles, and core KSATs.

    - It is highly recommended that detailed exam and associated course information be submitted with the offering to assess against DCWF core KSAT requirements. If included with the submission, the exam information would be considered the primary source and any course curriculum content would be considered the secondary source for general reference.

3. Information about the Provider's offering to include methods and status of accreditation and validation.

    - Be prepared to provide supplemental information such as the resumes or cover letters of subject matter experts used and sample report data.

Informal feedback may be provided to the Provider, when feasible, during the step to evaluate and validate the credentialing body. Informal feedback will be provided to the Provider after the validation step of the credentialing body's evaluation has concluded. Informal feedback will only focus on missing criteria and/or deficiencies within the nominated certification or training offering.

Upon completion of the readiness review step of the Certification or Training Approval Process, the Provider may be advised that the application is not ready to proceed to Part 3, and if so, the Provider may receive feedback via text and/or email describing the criteria that was missing or why the offering was not approved.

If the AI determines that the application is not ready, the application will remain in "Readiness Review" status but will not be disqualified and archived. The Provider may update the readiness review step at any time for the next three months. However, the Provider may not resubmit the readiness review for another review for six months from the date a decision not to approve is rendered.

If the account has been inactive for over three months, it will be deactivated and the Provider, and its status, will be removed from the DoD 8140 Marketplace. A return user may reactivate an account at any time; however, if the process changes, the return user may have to re-start the application from Part 1.

Success Tips:

Rigorously study, analyze, review, and map the offering to the DCWF work roles and core KSATs.

Attach the data that proves the terminal learning objectives and Bloom's taxonomy of verbs are validated.

Online Certification or Training Approval Process Part 3: Assessment

When the readiness review unlocks Part 3, the status is automatically set to "In Assessment" within the DoD 8140 Marketplace. Part 3 is the most complex and will require an in-depth understanding of how the DCWF work roles align to the Provider's offering.

Part 3 will assess how the Provider's offering:

- Maps to the DCWF and DoD 8140 policies,
- Shows how the TLOs and ELOs fulfill the core KSATs within the DCWF workrole, and
- Meets the 70% approval threshold to be approved for use in accordance with DoDM 8140.03 for each applicable DCWF work role.

Part 3 is supported by AI to assess the certification or training offering against the relevant DCWF categories, work roles, and core KSATs and makes recommendations based on the assessment. The Provider will be asked to provide a self-assessment and be given opportunities to make edits and adjustments based on the AI-generated recommendations.

For the purposes of this document, certification or training offerings that are DoD 8140 Approved for Use indicates that the offering can be used by an individual to become qualified to the DoD 8140 Program.

The certification or training offering must demonstrate alignment with at least one DCWF work role. Within the DCWF work roles aligned to the certification or training offering, the offering must meet a minimum threshold score of 70% to be approved for use in accordance with DoDM 8140.03 for each applicable DCWF work role.

If the certification or training offering does not achieve a 70% score, the AI will determine the offering is not ready, and the submitted offering will go back to "Readiness Review" status.

Online Certification or Training Approval Process Part 4: Validation

The automated assessment results from Part 3 are forwarded to the 3rd party validator for review, adjudication, and will provide a recommendation to approve or reject for specific applicable DCWF work roles. The evaluation process is often inherently subjective. The level of granularity of available exam or course content often leaves significant details for the analyst to extrapolate or assess to determine whether the description of a specific objective could reasonably be expected to satisfy a given core KSAT. Validation results that differ from the automated assessment will undergo additional scrutiny including repeating the automated assessment, reviewing the exam data, reviewing the Provider's self-assessment, and meeting with the Provider, if warranted.

If the results of the validation align with the automated assessment, the certification or training offering will be approved for use in accordance with DoDM 8140.03 for each applicable DCWF work role.

If the DoD CIO WID determines that more information is needed from the Provider, the Provider will be notified via text and/or email. Once any supplemental information is received and any additional review is complete, a final decision will be rendered on the offering. If a negative decision is rendered, the reasons for the negative decision will be documented.

The Provider's status will be set to "*DoD 8140 Approved for Use*" based on a final decision to approve.

If the offering does not receive approval, the application's status will be set back to "Readiness Review," but the offering will not automatically be disqualified. The Provider may update the application at any time within the first 3 months. However, the Provider may not resubmit the application for another review for six months from the date a decision not to approve is rendered.

This process will compile a case file and archive all related documents and correspondence pertaining to each offering submission.

If the Provider's account has been inactive for over three months, it will be deactivated. The Provider's organization that submitted the offering and its status will be removed from the DoD 8140 Marketplace. The Provider may reactivate the account at any time; however, if the process changes, the Provider may have to re-start from Part 1.

Process Flow

The steps of assessing and approving the offering in accordance with DoDM 8140.03 includes the 3rd party validation step.

There are three roles in the Certification or Training Approval Process:

- *Provider*: The submitting organization that provides the certification or training offering.
- *AI*: This stream shows where and how AI will be used in the application and assessment steps.
- *3rd Party Validator:* On behalf of the CWMB, the 3rd party validator will validate the automated assessment supported by AI and approve the Provider's offering in accordance with DoDM 8140.03.

The data collected in all four parts of the Certification or Training Approval Process will be used to assess the Provider's application. The status of the Provider Organization's submission will be updated automatically as the application proceeds through the steps of process as the submission, assessment, validation, and approval are completed. The Provider's designated points of contact may receive status updated via text and/or email as well as on the DoD 8140 Marketplace site.

Figure 5: DoD 8140 Qualification Approval Process: Process Flow

Statuses

As the application moves through the process, the Provider's status will be automatically updated. The Certification or Training Approval Process Statuses are:

- *In Development:* Submission not ready.
- *Readiness Review:* Submission not ready.
- *In Assessment:* Submission pending assessment.
- *3rd Party Validation:* Submission pending validation and approval
- *DoD 8140 Approved for Use:* Submission completed and approved for use to justify a person is qualified for a DCWF work role in accordance with DoDM 8140.03.

Once the 3rd party validator reviews the assessment, and approves the certification or training offering, the offering will be assigned the status *DoD 8140 Approved for Use,* defined for the purposes of this process and document as: *Has successfully completed DoD 8140 approval process and, in addition, has test data and/or proven performance-based assessments of core KSAT fulfillment in accordance with DoDM 8140.03.*

General Information

The Provider may start and stop on an application at any time to continue updating it until the application is submitted. Once the information is submitted, whether it is submitted for Part 1, 2,3, or 4, the Provider will only have read-only access.

The Provider may submit multiple offerings under the Provider organization's umbrella account when in Part 2. Parts 1 is for global information.

If further assistance is required, click the LiveChat tab or link within the application page to chat with our help desk about accounts, password resets, and other matters related to use and navigation.

Other information may be sent to the points of contact linked to the Provider organization's account. Please ensure the point of contacts set spam or junk mail to mark the source as safe or not junk mail.

The DoD CIO WID will update the appropriate public and private DoD 8140 Cyber Workforce Qualification Program online portals and databases regarding final decisions. Meeting minutes documenting any official decisions will count as official correspondence.

Please note the posting of the training vendor or credentialing agency's offerings:

- Does not imply an endorsement by the DoD or any of the military services
- Does not ensure the military services will support funding toward the training or credential
- Does not guarantee the continued posting of the training or credential, if the services' needs change
- Does not imply that any of the training vendor's or credentialing agency's other credentials (if applicable) can or will be approved or posted
- Does not require the training vendor or credentialing agency's acknowledgement or concurrence to be included
- Does not require the training vendor or credentialing agency's acknowledgement or concurrence to be removed
- Is based strictly on the needs of DoD and military services and is subject to change based on the needs of the DoD and each military service

The intent of this review is NOT to change the business model of the training vendor or credentialing agency, or for the training vendor or credentialing agency to create training, a credentialing program, or standard that is tailored solely to the DCWF. This is merely an assessment tool to help the identify which training or credentials may meet their needs within the DCWF programs. This review should not infer/imply that DoD or the military services are directing training vendors or credentialing agencies to make changes to their business models or practices. Any costs incurred by internal changes by the training vendor or credentialing body is solely a business decision of the training vendor or credentialing body and will not be compensated by the DoD or Services.

For questions regarding the DoD 8140 Certification or Training Approval Process, DoD 8140 policy inquiries, or technical process questions, or for more information, visit *https://public.cyber.mil/wid/cwmp/,* or contact the DoD CIO Workforce Innovation Directorate (WID) at *osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil*.

Mutual Non-Disclosure Agreement (NDA)

To access your DoD 8140 provider account, you will need to review and accept the following mutual non-disclosure agreement. This is a clickthrough process, and your onscreen acceptance will be considered an authorization and agreement to the terms contained in it.

For informational purposes, DoD employees and contractors are prohibited from releasing any confidential information in use as part of the DoD Cyber Workforce Qualification Program to anyone outside of the agency.

Disclosure of Confidential Information Generally (18 USC 1905)

Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Federal Housing Finance Agency, or agent of the Department of Justice as defined in the Antitrust Civil Process Act (15 U.S.C. 1311–1314), or being an employee of a private sector organization who is or was assigned to an agency under chapter 37 of title 5, publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.

Note:

The end user must scroll all of the way to the bottom of the text before being presented the "I AGREE" and "DO NOT AGREE" buttons.

I AGREE:

After clicking "I AGREE," the provider end user can print a copy of the executed version, plus they will receive an executed copy via email.

DO NOT AGREE:

After clicking "DO NOT AGREE," the end user will receive an onscreen message that says their account registration has been canceled, and they will be returned to the logged out screen without having access to the system.

Click-Through Service Provider And AVUE Mutual Non-Disclosure Agreement

A. The Service Provider ("Provider") identified at the end of the NDA Agreement below, acting through the user of this application, is entering this DoD Cyber Workforce Qualification Program Application System ("Qualification System") to apply for Department of Defense (DoD) approval of the Provider's program(s) and/or course(s) for use within DoD. The Qualification System is provided by Avue Technologies Corporation ("Avue").

B. As part of the application process, the Provider will submit information and materials that the Provider deems confidential and/or proprietary into the Qualification System. Conversely, in the course of the Provider's use of the Qualification System, the Provider will access and be exposed to the design, functions, calculations, data, and operations of the Qualification System, including without limitation matters pertaining to artificial intelligence and machine learning (AI/ML), all of which Avue deems to be confidential and/or proprietary.

C. To protect each party's proprietary and confidential information, the Provider and Avue are entering into this Click-Through Service Provider and Avue Mutual Non-Disclosure Agreement ("NDA Agreement").

D. To proceed into the Qualification System, a user authorized to act on behalf of the Provider must first review and indicate the Provider's agreement with the terms of this NDA Agreement. ***THE USER CANNOT PROCEED WITH THE APPLICATION UNLESS THE USER ACCEPTS AND AGREES TO THIS NDA AGREEMENT ON THE PROVIDER'S BEHALF.***

THIS NDA AGREEMENT is entered into as of today ("Effective Date") by and between AVUE and the Provider. Avue will automatically execute this NDA concurrent with execution by the user on behalf of the Provider, as provided below.

1. **Proprietary Information, Ownership, Non-Disclosure and Remedies**.
    a. **"Proprietary Information"** means: (1) In the case of the Provider, all data, information, and materials disclosed by the Provider in the course of the Provider's application for approval using the DoD Cyber Workforce Qualification Program Application system ("Qualification System"); and (2) In the case of Avue, the design, functions, data, and operation of the Qualification System, including, without limitation, all content on all web pages and all matters pertaining to artificial intelligence and machine learning (AI/ML). The obligations of confidentiality will not apply to any Proprietary Information which: (A) is now, or hereafter becomes, through no fault or involvement on the part of the other party, generally known or available to the public; or (B) can be proven, by clear and convincing evidence, to have been (i) known or lawfully in possession of the other party before the Effective Date, and not subject to an existing confidentiality obligation, (ii) legally obtained from sources without a confidentiality obligation, or (iii) developed by employees or agents of the other party independently of and without reference to any Proprietary Information.
    b. **Ownership.** All Proprietary Information of each party will remain their sole property.
    c. **Non-Disclosure.** Each party will hold all Proprietary Information of the other in strict confidence and will not disclose any Proprietary Information to any third party, provided, however, that the Provider understands and agrees that DoD (including its employees and authorized representatives) will access and use the Provider's Proprietary Information as part of the qualification approval process. Neither party will use any Proprietary Information of the other party for any purpose other than the submittal and processing of the Provider's application for approval. The confidentiality obligations in this paragraph will survive and continue into perpetuity.
    d. **Remedies.** Each party agrees that, due to the unique nature of the Proprietary Information, the unauthorized disclosure or use of the Proprietary Information will cause irreparable harm and significant injury to the other party, and therefore agrees that the owner of the Proprietary Information, in addition to any other available remedies, will have the right to an immediate injunction and other equitable relief

enjoining any breach or threatened breach of this NDA Agreement, without the necessity of posting any bond or additional security.

2. **Other Provisions.** This NDA Agreement constitutes the parties' entire agreement concerning the subject matter. No amendment, cancellation, modification, or waiver of any provision of this NDA Agreement will be effective unless in a written agreement signed by both parties. No delay or omission on the part of either party to exercise or avail itself of any right or remedy it has or may have will operate as a waiver of any right or remedy. This NDA Agreement shall be governed by and construed following the laws of the Commonwealth of Virginia without reference to its conflicts of laws provisions. This NDA Agreement and parties' rights and obligations under it may not be assigned or delegated by either party, in whole or part, whether voluntarily, by operation of law, change of control, or otherwise, without the prior written consent of the other party. Subject to the preceding sentence, this NDA Agreement will be binding upon and inure to the benefit of the parties and their respective successors and permitted assigns.

ON BEHALF OF THE PROVIDER, YOU MUST READ THIS NDA AGREEMENT CAREFULLY AND UNDERSTAND IT. **BY CLICKING THE "AGREE" BUTTON** LOCATED ON THIS PAGE: **(1) YOU ARE REPRESENTING THAT YOU ARE AUTHORIZED TO ACT ON BEHALF OF THE PROVIDER, and (2) THE PROVIDER AGREES TO BE BOUND BY THIS NDA AGREEMENT.** IF YOU ARE (A) NOT AUTHORIZED TO ACT ON BEHALF OF THE PROVIDER OR (B) DO NOT AGREE WITH ALL THE TERMS OF AND AGREE TO BE BOUND BY THIS NDA AGREEMENT, PLEASE CLICK THE "**DO NOT AGREE**" BUTTON. ***IF YOU DO NOT AGREE WITH THE PROPOSED TERMS ABOVE, YOU WILL NOT BE ALLOWED TO CONTINUE FORWARD IN THE SYSTEM***.

AFTER CLICKING "I AGREE", YOU WILL BE ABLE TO PRINT A COPY OF THIS AGREEMENT. YOU WILL ALSO BE EMAILED AN EXECUTED COPY.