BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE
MANUAL 17-1305

7 JUNE 2024

CYBERSPACE OPERATIONS

DAF CYBERSPACE WORKFORCE MANAGEMENT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CNSF

Certified by: SAF/CNS
(Dr. Keith Hardiman)

Supersedes: Air Force Manual 17-1303, 12 May 2020

Pages: 42

This publication implements Department of Defense Directive (DoDD) 8140.01 *Cyberspace Workforce Management*, Department of Defense Instruction (DoDI) 8140.02 *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements*, and Department of Defense Manual (DoDM) 8140.03 *Cyberspace Workforce Qualification and Management Program*. It provides guidance and procedures on the Department of the Air Force (DAF) implementation of DoD 8140 series policies and the DoD Cyberspace Workforce Framework (DCWF) positions, qualification, training and certification requirements and is the authoritative policy on cyber workforce reporting, metrics, and validation throughout the DAF. It applies to all DAF civilian employees and uniformed members of the Regular Air Force, the United States Space Force (USSF), the Air Force Reserve (AFR), the Air National Guard (ANG), the Civil Air Patrol (CAP) when conducting missions as the official Air Force Auxiliary, where applicable, foreign nationals in accordance with applicable agreements, the Special Access Programs (SAP) community, cyber contracted support and those with a contractual obligation to abide by the terms of DAF publications, except where noted otherwise. This manual requires the collection and or maintenance of information protected by 5 U.S.C. §552a (The Privacy Act of 1974), as authorized by Title 10 United States Code, Section 9013, Secretary of the Air Force. The applicable System of Records Notices, F036 AF PC C, Military Personnel Records System and F036 AF PC Q, Personnel Data System (PDS), are located at **https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/Air-Force-Article-List/**.

Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command, via the Air Force Major Command (MAJCOM), Space Force Field Command (FLDCOM), or Field Operating Agencies/Direct Reporting Units (FOA/DRU) representatives as described in this manual.

This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing, unit, delta, or garrison level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

SUMMARY OF CHANGES

This document is substantially different from its predecessor and should be completely reviewed. Changes include additional positions and requirements placed on all individuals and roles including the Secretary of the Air Force. References from previous versions have been updated or removed, as necessary. This update also includes requirements from DoDD 8140.01 *Cyberspace Workforce Management,* DoDI 8140.02 *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements,* and DoDM 8140.03 *Cyberspace Workforce Qualification and Management Program*. Accordingly, some changes to corresponding terminology were required i.e., changing "Wing Cybersecurity Offices" to "Wing Cyberspace Offices", and incorporating similar changes for the "United States Space Force Delta Cyberspace Offices".

Chapter 1

GENERAL INFORMATION

1.1. Overview.

1.1.1. The DAF Cyberspace Workforce Management Program furthers the Department's obligations to support DoD's goals to develop a DoD cybersecurity workforce with a common understanding of the concepts, principles, and applications of cyberspace; to establish the DCWF as the authoritative reference for the identification, tracking, and reporting of cyberspace positions; and to manage and align specific workforce elements for each category, level, and cyberspace work function to ensure the confidentiality, integrity, and availability under an enterprise model of DoD information, Information Systems, networks, and the information stored within.

1.1.2. The DAF maintains a Total Force management posture to qualify and enable authorized cyberspace government employed civilian, military, and foreign national personnel to perform cyberspace roles and responsibilities. Contracted services supports and augments these personnel, where appropriate. These personnel and contracted services, collectively function as an integrated workforce with complementary skill sets to provide an agile, flexible response to meet DAF mission requirements. The appropriate mix of government civilian, military, and contracted support personnel designated to perform in cyberspace work roles is determined in accordance with DoDI 1100.22, Policy and Procedures for Determining Workforce Mix.

1.1.3. All persons performing cyberspace work roles must be identified in respective authoritative manpower and personnel systems and fully qualified according to DoD standards and all DAF specific workforce qualification and training requirements as outlined in this manual.

1.1.4. Cyberspace work comprises tasks executed by personnel assigned to workforce elements, which include Information Technology (IT), Cybersecurity, Cyberspace effects, Intelligence workforce (cyberspace), Cyberspace enablers, Software Engineering, and AI/Data.

1.1.5. The DCWF is the reference model for the identification, tracking, and reporting of DoD cyberspace positions and establishes the baseline of cyberspace workforce qualifications. All positions requiring the execution of cyberspace work must be DCWF coded in accordance with DoDD 8140.01.

1.1.6. This manual identifies DAF cyberspace workforce positions and qualification requirements. It also provides policy on workforce reporting, metrics, and validation, and provides a structure towards moving the Civilian and Military Cyber Workforce toward modernization as provided by the DCWF in accordance with DoDI 8140.02 (resources available on the DoD Cyber Exchange Website at **https://www.cyber.mil**). The requirements specified in this manual are the minimum required, unless otherwise noted. Commanders and Program Managers are authorized to apply more stringent requirements to reflect specific mission directives and budget constraints.

1.1.7. This manual does not address the operational employment of the cyberspace roles. Operational employment of the cyberspace workforce is determined by mission requirements as directed by the Joint Staff, Combatant Command, and other DoD Components. Fully

implemented, DCWF facilitates allocation of personnel according to mission needs at every organizational level.

1.2. Network Access Requirements

1.2.1. All users regardless of rank, position, or role requiring access to the AF Information Network (AFIN) Information System(s), or Platform Information Technology (PIT) Systems will complete initial Cyber Awareness training as a prerequisite for access. All users will complete refresher training to maintain network or system access as new versions are published and made available via SAF/CN approved means **(T-1)**, which includes 1) the AF learning management system, MyLearning **https://lms-jets.cce.af.mil/moodle/**); 2) the DoD Cyber Exchange NIPR (Non-classified or Non-secure Internet Protocol Router) portal: **https://www.cyber.mil**; or 3) using any other method that SAF/CN designates. MyLearning is the preferred training method as it provides reporting updates to other DAF systems. All users must complete the training on an individual basis using the Computer Based Training (CBT) from an approved platform to receive initial or annual training credit. Group delivery may be used as a command tool but is specifically not DAF approved to satisfy initial or annual requirements.

1.2.2. Course updates normally occur about October of each year. Users without network access can take the course at the DoD Cyber Exchange Public portal and present their certificate of completion to their unit training manager to manually update their training record with the date of completion on the certificate. Users will refresh their training within 365 calendar days when newer versions of the training becomes available.

1.2.3. User network access may be suspended by technical enforcement controls for non-compliance with refresher training. The authoritative record for Cyber Awareness training status is stored in Air Force Information Directory (AFID). Unit training managers are authorized to manually update user training status via MyLearning when a user completes the training requirement off-network and presents proof of completion (i.e., certificate).

1.2.4. To promote DoD Enterprise reciprocity, users reporting to joint assignments, deployments, TDY, etc. or requiring access to other networks must ensure their training status has been refreshed within the past 90 days. They may be requested to present a hard or soft copy of their certificate by the gaining agency, organization, or unit. Users are responsible for maintaining their status through their date of return to their home unit.

1.3. Identification

1.3.1. All DAF civilian and military cyberspace workforce positions requiring performance of at least one cyberspace task must be identified on a Unit Manning Document (UMD) using established Special Experience Identifiers (SEIs) and all applicable DCWF work role and proficiency level codes via the appropriate Manpower Programming and Execution System (MPES) entries.

1.3.2. Civilian and military personnel: The cyberspace workforce information must be recorded in manpower and personnel databases or systems (e.g., Military Personnel Data System- MilPDS or Defense Civilian Personnel Data System-DCPDS [to be replaced by the Defense Civilian Human Resource Management System-DCHRMS]). The record will include the AF Specialty Code (AFSC), Space Force Specialty Code (SFSC), or civilian occupational

series as a required data field as applicable. Relevant information is also recorded on civilian position description or core personnel documents.

1.3.3. Contractors: All cyberspace requirements including continuing education must be listed in the contract requirements and associated Statement of Work (SOW) or Performance Work Statement (PWS) in accordance with DoDM 8140.03 para 3.2. **(T-0).** Details on the contractor cyberspace workforce must be locally collected and tracked with the program office until such time as personnel and management systems can fully accommodate contractors **(T-1)**.

1.3.4. Foreign nationals: All cyberspace requirements, consistent with appliable international agreements, including DCWF coding shall be locally collected and tracked with the program office and forwarded to the Wing/Delta Cyberspace Office until such time as personnel and management systems can fully accommodate them. A memorandum for record shall be forwarded to the MAJCOM/FLDCOM representative to include the list of names and position identification information **(T-1)**.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. The Secretary of the Air Force shall:

2.1.1. Act as the DoD Executive Agent for the Department of Defense Cyber Crime Center (DC3) and for digital/multimedia forensics within the DoD Forensic Enterprise, in accordance with DoDDs 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, and 5205.15E, *DoD Forensic Enterprise*.

2.1.2. Support development of standards for digital forensics personnel training and qualifications.

2.1.3. Coordinate with the DoD Chief Information Officer (CIO), the Under Secretary of Defense (USD I&S), and the Secretaries of the other Military Departments to integrate appropriate training and education for DoD personnel who perform cyberspace investigations, digital forensics, and cyberspace analysis.

2.2. The DAF Chief Information Officer (SAF/CN) shall:

2.2.1. Coordinate with the Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/A2/6), Deputy Chief of Space Operations for Operations, Cyber and Nuclear **(**SF/COO), Offices of the Undersecretary of Defense, the SAP community (not including those for Sensitive Compartmented Information and other intel-funded capabilities regardless of classification level), and DoD CIO on policy development and implementation of DAF cyberspace workforce requirements and processes.

2.2.2. Interpret DoD policy, guidance, and directives and promulgate DAF cyberspace workforce directives, policies, and requirements.

2.2.3. Provide direction on position determinations, identification, and coding for the cyberspace workforce in accordance with DoDI 1100.22 and DoDM 8140.03 paragraph 4.3 and ensure this is completed not later than 15 February 2026 **(T-0)**.

2.2.4. Coordinate with AF/A2/6 and SF/COO on updates to the Enlisted and Officer Classification Directories to reflect SEI requirements and updates to the civilian cyber work role and proficiency level codes for the cyberspace workforce.

2.2.5. Provide direction and oversee the reporting of metrics on the cyberspace workforce in accordance with DoDI 8140.02 paragraph 5, and any DAF internal or external validations.

2.2.6. Coordinate with AF/A2/6 and SF/COO to provide programming and budget guidance to MAJCOMs, FLDCOMs, FOA/DRUs and Program Management Offices (PMOs) for cyberspace workforce management to include certification exam and maintenance fee costs and computer-based training.

2.2.7. Provide direction on supplemental cyberspace workforce training.

2.2.8. Ensure reasonable accommodations for military and civilian personnel in accordance with DAFI 36-2710, *Equal Opportunity Program.*

2.2.9. Oversee guidance to the DAF Cyberspace Workforce Management Program and distribution of certification funds for the DAF.

2.2.10. Identify, track, and report qualifications for DAF personnel who perform cyberspace work roles in accordance with DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, DoDI 7730.68, *Uniformed Services Human Resources Information System*, Volume 4 of DoDI 1444.02.

2.2.11. Report unit-based workforce readiness status in the Defense Readiness Reporting System in accordance with DoDD 7730.65, *DoD Readiness Reporting System*.

2.2.12. Adhere to all labor-management obligations in accordance with Volume 711 of DoDI 1400.25, *DoD Civilian Personnel Management System.*

2.2.13. Identify total manpower required to perform cyberspace work roles in authoritative manpower and personnel systems in accordance with the Federal Cyber Workforce Assessment Act of 2015.

2.2.14. Track Authorizing Official (AO) signed certification waivers, as discussed in **Chapter 4**.

2.2.15. Assist certification providers with DAF policy when applying to use the .mil network to proctor electronic certification exams (e.g., assess software needed by the education offices using .mil).

2.2.16. Assist AF/A2/6 and SF/COO/S6 with integrating institutional education and training programs and requirements (i.e., ancillary, Professional Military Education [PME], and accessions) into the appropriate venues prior to levying on the Total Force.

2.2.17. Ensure career-field specific requirements are coordinated with the respective career field manager for integration into Career Field Training and Education Plan, Specialty Training Standard, or Course Training Standard as appropriate.

2.2.18. Coordinate with AF/A2/6, SF/COO/S6, Deputy Chief of Staff for Manpower, Personnel and Services (AF/A1), Deputy Chief of Space Operations for Human Capital (SF/S1), and the Assistant Secretary of the AF, Acquisition, Technology, & Logistics (SAF/AQ) to acquire a capability for MAJCOMs, FLDCOMs, PMOs, CCMDs (Combatant Commands), and/or units to track and manage qualifications for the DAF cyberspace workforce. Such capability shall be compatible with DoD CIO systems where required and supports automated reporting of the DAF cyberspace workforce as necessary.

2.2.19. Update skill-awarding and supplemental courses for the cyber workforce to encourage additional certifications if cost-benefit analysis supports such action.

2.2.20. Ensure Air Education and Training Command (AETC) has the most current DoD approved annual cyberspace user awareness training product(s).

2.2.21. Provide representation to the Cyber Workforce Management Board (CWMB) and other DoD cyberspace workforce governance forums and working groups to support the development and implementation of policies, procedures, and processes required to manage and guarantee compliance with DoDD 8140.01 and DoDI 8140.02 in accordance with DoDM 8140.03 paragraph 4.4.

2.3. Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/A2/6) shall:

2.3.1. Coordinate with SAF/CN to develop policy and direct implementation of DAF requirements and processes.

2.3.2. Oversee updates to the Enlisted and Officer Classification Directories to reflect SEI requirements for the cyberspace workforce.

2.3.3. As Program Element Monitor (PEM), work with SAF/CN to provide programming, sustainment, and budget guidance to MAJCOMs, FLDCOMs and PMOs for cyberspace workforce management and improvement programs to include certification exam and maintenance fee costs, and computer-based training.

2.3.4. Ensure reasonable accommodations for civilian employees and military members in accordance with DAFI 36-2710.

2.3.5. Participate as member on various DoD cyberspace workforce forums and groups.

2.3.6. Oversee the integration of institutional education and training programs and requirements (i.e., ancillary, PME, and accessions) into the appropriate venues for the Total Force.

2.4. Deputy Chief of Space Operations for Operations, Cyber and Nuclear (SF/COO):

2.4.1. Coordinate with SAF/CN to develop policy and direct implementation of DAF requirements and processes.

2.4.2. Oversee updates to the Enlisted and Officer Classification Directories to reflect SEI requirements for the cyberspace workforce.

2.4.3. As Program Element Monitor (PEM), work with SAF/CN to provide programming, sustainment, and budget guidance to FLDCOMs and PMOs for cyberspace workforce management and improvement programs to include certification exam and maintenance fee costs, and computer-based training.

2.4.4. Ensure reasonable accommodations for civilian employees and military members in accordance with AFI 36-2710.

2.4.5. Oversee the integration of institutional education and training programs and requirements (i.e., ancillary, PME, and accessions) into the appropriate venues for the Total Force.

2.5. Deputy Chief of Space Operations for Human Capital (SF/S1) shall:

2.5.1. Work with SAF/CN to provide a capability to identify, record and track civilian and military cyberspace positions via SEIs in personnel and manpower databases and systems and output on the Unit Manning Document (UMD).

2.5.2. Work with SAF/CN to provide a capability to identify and track civilian and military cyberspace personnel by cyber work role and proficiency level codes in accordance with DCWF, DoDD 8140.01, and DoDI 8140.02 paragraphs 4 and 5 in personnel and manpower databases and systems and output on the Unit Manning Document (UMD).

2.5.3. Provide advice on union representation or Space Force's collective bargaining obligations related to cyberspace workforce requirements.

2.5.4. Ensure guidance is provided to support human resources (HR) organizations for management of cyberspace workforce within manpower and personnel databases or systems.

2.6. Deputy Chief of Staff for Manpower, Personnel and Services (AF/A1) shall:

2.6.1. Work with SAF/CN to provide a capability to identify, record and track civilian and military cyberspace positions via SEIs in personnel and manpower databases and systems and output on the UMD.

2.6.2. Work with SAF/CN to provide a capability to identify and track civilian and military cyberspace personnel by cyber work role and proficiency level codes in accordance with DCWF, DoDD 8140.01, and paragraphs **4** and **5**. of DoDI 8140.02 in personnel and manpower databases and systems and output on the UMD.

2.6.3. Provide advice on union representation or Air Force's collective bargaining obligations related to cyberspace workforce requirements.

2.6.4. Ensure guidance is provided to support human resources (HR) organizations for management of cyberspace workforce within manpower and personnel databases or systems.

2.7. Assistant Secretary of the Air Force, Acquisition, Technology & Logistics (SAF/AQ) shall:

2.7.1. Ensure acquisition strategies and contracts for Systems address cyberspace workforce requirements.

2.7.2. Ensure programs appropriately budget for qualified cyberspace personnel to support systems throughout life cycles.

2.7.3. Work with AF/A1, AF/A2/6, and SAF/CN on a capability to automate reporting of the DAF cyberspace workforce (e.g., qualification status).

2.8. DAF Cyber Career Field Managers shall:

2.8.1. Maintain updated AFSCs, SFSCs, or occupational series and DCWF for inclusion or removal to the cyberspace workforce program.

2.8.2. Provide guidance to ensure SEIs are updated on UMDs, enlisted and officer classification directories and/or appropriate civilian personnel databases and systems.

2.8.3. Provide guidance to ensure that the personnel section and supervisor over civilians will ensure the SCPD, CPD, or PRD and appropriate civilian personnel databases or systems reflect accurately the cyberspace workforce requirements**. (T-2)**.

2.8.4. Ensure the servicing personnel section and position classification activity or section are notified of any changes to civilian positions in the cyberspace workforce.

2.8.5. Confirm approved SEI changes in cyberspace qualifications are completed for civilian or military personnel and are updated in civilian or military personnel databases or systems as appropriate.

2.8.6. Ensure updates are made to civilian cyber work role and proficiency level codes for tracking cyberspace workforce requirements that align with the AFSCs, SFSCs, and occupational series under the purview of the career field manager.

2.8.7. Ensure position description, cyber work role and proficiency level guidance is provided to HR, supervisors, Unit Deployment Managers, and personnel to facilitate proper coding and tracking of cyberspace workforce requirements in accordance with DoDI 8140.02, DODM 8140.03, and the DCWF.

2.8.8. Apply appropriate risk prioritization to ensure highest risk work roles or workforce categories are fully compliant with requirements and qualifications are maintained.

2.9. Major Commands, Field Commands, Field Operating Agency, Direct Reporting Units shall:

2.9.1. Provide oversight over the cyberspace workforce within their respective commands, agencies, and units, ensuring the cyberspace workforce is identified, trained, qualified, tracked and managed in accordance with DoD and DAF Cyberspace Workforce Management Program directives and policies (e.g., DoDD 8140.01, DoDI 8140.02, DoDM 8140.03 and this manual).

2.9.2. Ensure the cyberspace workforce positions are reviewed periodically and validated annually in accordance with SAF/CN guidance **(T-1)**.

2.9.3. Act as the command focal point on cyberspace workforce issues.

2.9.4. Consolidate Base, Wing, or Delta and other subordinate organization reporting inputs on civilian, military, and contractor cyberspace workforce metrics.

2.9.5. Report the status of their cyberspace workforce metrics to SAF/CN at the close of each fiscal year or as directed.

2.9.6. Appoint in writing an A6/S6 Directorate representative to act as a focal point to collaborate with OPR to advise and advocate on behalf of MAJCOM/FLDCOM/FOA/DRU and CCMD specific issues. Collectively, representatives become the DAF Cyberspace Workforce Improvement Group (DAFCWIG) and will collaborate on projects and think-tanks to improve the DAF Cyberspace Workforce.

2.9.6.1. The representative shall be responsible to the MAJCOM/FLDCOM/FOA/DRU or CCMD for establishing Memorandums of Understanding (MOUs) with subordinate, peer, and other organizations and coordinating boundaries with other MAJCOM/FLDCOM/FOA/DRUs for the purposes of reporting and data collection efforts to produce comprehensive coverage and reduce overlap.

2.9.6.2. The representative shall coordinate with cyber leaders at their organizational level and subordinate level Supervisors, Program Offices, Contracting Officers, Authorizing Officials, and all personnel to ensure workforce qualification data is maintained and updated and metrics are submitted as requested.

2.9.6.3. The representative shall ensure alternative experience requests meet all requirements for endorsement per DoDM 8140.03 paragraph 3.2.b(2) and forward approved requests to the appropriate AO for signature and forwarding to SAF/CNSF.

2.10. Air Combat Command shall:

2.10.1. Collect, monitor, and analyze data in support of Cyber workforce management actions.

2.10.2. Submit Program Objective Memorandum (POM) for DAF-wide training and tracking of approved civilian and military cyberspace workforce authorizations.

2.10.3. Supplement formal training programs with commercial cyberspace training as needed.

2.10.4. Provide online training materials via AF e-Learning website, the Air Force Portal, or MyLearning as appropriate.

2.10.5. Publish information regarding DAF-endorsed certifications and mapping to vendor available certifications per DODM 8140.03 paragraph 3.2 (b)(1)(C).

2.10.6. Execute the DAF Certification Program funds for preferred certifications and maintenance fees.

2.10.7. Maintain a record of personnel certifications mapped to Electronic Data Interchange Personal Identifier (EDIPI, also known as DoD ID Number) and provide access to MAJCOM/FLDCOM/FOA/DRU and CCMD representatives in accordance with **paragraph 2.9.6** of this manual until no longer required and/or capabilities as outlined in **paragraph 2.2** of this manual are fully operational, whichever is later.

2.10.8. Publish list of DAF sponsored training programs in compliance with meeting minimum standards of 70% knowledge, skills, ability (KSA) coverage of core task for the applicable proficiency level as per DoDM 8140.03 paragraph 3.2.b.(1)(b).

2.10.9. Coordinate with AFPC to collect data as required per DoDI 8140.02 paragraph 5.2 and DoDM 8140.03 paragraph 5.2.g.

2.10.9.1. Such data shall be maintained in a readily reportable format.

2.10.9.2. Any systems that are used to collect such data must be authorized with system and data protections in place to maintain High Confidentiality and High Integrity with Classification determined sufficient for the aggregation of data.

2.11. Air Education and Training Command shall:

2.11.1. Provide and sustain availability and support of cybersecurity user awareness training for all DAF users with the SAF/CN provided curriculum.

2.11.2. Provide schoolhouse training, certification testing, and cybersecurity user awareness training to students (civilian, military, and foreign military), as appropriate.

2.11.3. Provide for the updating of cybersecurity awareness training records for civilian, military, foreign military, and contractor personnel for continued network access.

2.11.4. Develop and provide credentialing and certification service in accordance with DoDI1322.33_DAFI 36-2683, *Department of the Air Force Voluntary Credentialing Programs*.

2.11.5. Provide coordination where appropriate with Space Training and Readiness Command (STARCOM) for inherited or assumed functions described by **paragraph 2.10** of this manual.

2.12. Air Force Personnel Center shall:

2.12.1. Upon the request of the appropriate DAF Career Field Manager, update the appropriate AF Enlisted Classification Directory (AFECD) or AF Officer Classification Directory (AFOCD) with SEIs to track the military cybersecurity workforce roles and proficiency levels.

2.12.2. Coordinate with supervisors, program managers, and employees to ensure that Cyber Work role codes properly appear on Standard Core Personnel Documents (SCPDs), Core Personnel Documents (CPDs), and/or Position Requirements Documents (PRDs) consistent with management's request as appropriate.

2.12.3. Assist with extract reports as requested from manpower and personnel databases or systems (e.g., MilPDS and DCPDS/DCHRMS) to identify cyberspace workforce requirements and alignment with personnel for DAF compliance reporting.

2.12.4. Upon request, will provide technical assistance to AF/A2/6 and SAF/CN on manpower and personnel systems (e.g., data field entries).

2.12.5. Provide data on incumbent cyberspace workforce positions to the Defense Manpower Data Center (DMDC) in accordance with DoDIs 8140.02, DoDI 7730.64, *Automated Extracts of Manpower and Unit Organizational Element Files*, DoDI 7730.68, and Volumes 1-4 of DoDI 1444.02, *Data Submission Requirements for DoD Civilian Personnel*.

2.12.6. Provide coordination to a Servicing Classification Office not located within AFPC, that inherits or assumes functions described by **paragraph 2.12** of this manual where appropriate.

2.12.7. Provide coordination with USSF Enterprise Talent Management Office for inherited or assumed functions described by **paragraph 2.12** of this manual.

2.13. Authorizing Officials shall:

2.13.1. Comply with cybersecurity training requirements in accordance with **paragraph 5.3** of this manual. The DoD AO training is located at this link on the DoD Cyber Exchange NIPR portal (Common Access Card-enabled): **https://cyber.mil/cyber-training/training-catalog/**.

2.13.2. Comply with DAF mandated AO training requirements consistent with AO onboarding, located on the DAF Risk Management Framework (RMF) Knowledge Service, located at: **https://rmfks.osd.mil/rmf/Collaboration/Component%20Workspaces/AirForce/Pages/default.aspx**.

2.13.3. Determine the appropriateness of residential qualification requirements based on work roles for all personnel under their oversight and provide funding to meet the training requirements for all subjected personnel. Reasonable efforts should be made to utilize training resources that are already within the DAF and then DoD resources before procuring commercial training.

2.13.4. Provide oversight over the DoD approved cyberspace foundational certification waiver process, following guidelines outlined in **Chapter 4** of this manual for cyberspace positions and personnel under their purview **(T-1)**.

2.13.5. Provide oversight over cyberspace personnel and positions, applying risk mitigation strategies in administering the exemption process as outlined in **paragraph 4.3** of this manual,

for personnel with assigned cyberspace roles who work with the Information Systems or PIT Systems in their Areas of Responsibility.

2.13.6. Ensure alternative experience requests meet all requirements for endorsement per DoDM 8140.03 paragraph 3.2.b.(2).

2.13.7. Ensure training and qualification standards are met and reporting of metrics to SAF/CN for personnel under their purview that are otherwise not accounted for under other organizational structures.

2.14. Wing/Delta Cyberspace Offices (formerly known as Cybersecurity Offices) (WCO/DCO) shall:

2.14.1. Monitor status on all Wing/Delta cyberspace workforce personnel.

2.14.2. Report status on all Wing/Delta cyberspace workforce personnel to appropriate MAJCOM representative.

2.14.3. Collect the UMD position validation status from units.

2.14.4. Collect qualification status data from units.

2.14.5. Collect contractor status data from units.

2.14.6. Serve as focal point/enforcement for the Wing/Delta's implementation of DoDI 8140.02, DoDM 8140.03, and this manual.

2.14.7. Monitor cyberspace workforce positions for accuracy and conduct validation at the close of each fiscal year in accordance with SAF/CN guidance or as directed.

2.14.8. Consolidate unit reporting inputs on civilian, military, and contractor cyberspace workforce metrics.

2.15. Program or Project Managers (PMs), System Managers, Program Management Offices (PMOs), Developmental or Operational Test Agencies and all Units shall:

2.15.1. Identify, track, and manage all cyberspace workforce positions according to guidance as issued by the appropriate career field manager and this manual.

2.15.2. Identify all civilian and military cyberspace positions in manpower and personnel databases or systems.

2.15.3. Ensure every civilian and military with privileged accounts are assigned to a cyberspace coded position on the UMD.

2.15.4. Ensure all cyberspace workforce personnel are qualified in accordance with DoDD 8140.01 and this manual.

2.15.5. Verify that the Program Office maintains a copy of a signed formal statement of assigned cybersecurity responsibilities for all personnel. Suggested formats are available in **Attachment 2** of this manual.

2.15.6. Review the UMD to ensure all civilian and military positions are identified and recorded with the appropriate SEI and DCWF cyber work role and proficiency levels. Identify positions that require update and notify the servicing manpower office to update the relevant fields in manpower and personnel systems to ensure that the UMD is correct.

2.15.7. Ensure all personnel in cyberspace workforce positions possess the appropriate clearance or national security investigation for their position **(T-0)** and that adjudication is completed before approval for privileged access is granted **(T-1)**.

2.15.8. Take appropriate actions as outlined in **paragraph 4.3** of this manual on military and civilian personnel in cybersecurity workforce positions when any of the following scenarios occur: DoD approved cybersecurity foundational certifications are not achieved within nine (9) months of assignment, a required foundational certification has expired, an individual has become decertified, foundational certification waivers are not obtained, or residential qualifications are not met within twelve (12) months of assignment **(T-0)**.

2.15.9. Conduct an annual validation of civilian and military cybersecurity workforce positions on the UMD and the data in personnel databases or systems (e.g., DCPDS for civilians to be replaced by DCHRMS, and Military Personnel Data System for military) **(T-1)**.

2.15.10. Include all contractor foundational and continuing education cyberspace requirements in new, renewed, or modified contracts and associated SOW or PWS and provide this information to contracting officers for all contracts in accordance with DoDD 8140.01 as prescribed at Defense Federal Acquisition Regulation Supplement (DFARS) subpart 239.7103(b) **(T-0)**.

2.15.11. Subsequent to identification of the requirement, and prior to issuance of a contract solicitation that requires a contractor to be provided cybersecurity requirements, the PM shall provide the Contracting Officer with an itemized list of required deliverables in the format specified by the contracting officer, information required under DFARS subpart 239.71, and any additional information required for the acquisition. A formal statement of Cyberspace Responsibilities shall be included in the list of required deliverables in the Contract Data Requirement List (CDRL) **(T-1).**

2.15.12. Ensure contractor cybersecurity requirements are evaluated for position sensitivity using the Office of Personnel Management Position Designation Tool, available at **https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool** as required by 5 C.F.R. § 1400. **(T-0)**.

2.15.13. Coordinate with the supporting Personnel Security Management Office or equivalent for submission of national security background investigations when contractor roles are identified as sensitive positions without a requirement for access to classified information **(T-1)**.

2.15.14. Coordinate with the Contracting Officer to ensure security background investigation and clearance requirements (when appropriate) are incorporated into the contract and associated SOW or PWS **(T-1)**.

2.15.15. Notify Contracting Officer whenever contractor cyberspace requirements must be added or modified, provide a revised SOW or PWS, and additional funding and/or updated budget as necessary **(T-1)**.

2.15.16. Verify with the Contracting Officer that all contractor personnel meet contract cyberspace requirements (e.g., initial and annual cybersecurity awareness training, DoD approved cyberspace foundational requirements and continuing education) prior to supporting

any cyberspace tasks on new, renewed, or modified contract and that they are satisfactorily maintained throughout the period of performance **(T-0)**.

2.15.17. Report DoD approved cyberspace foundational qualification statuses of contractor personnel to the Contracting Officer **(T-1)**.

2.15.18. Deny systems access, document the basis for the action, and initiate removal of contractor personnel who do not meet or maintain DoD approved cyberspace foundational or continuing education requirements (in accordance with contract requirements) via the Contracting Officer **(T-0)**. The Contracting Officer (or Representative) may prescribe other contractual remedies.

2.15.19. Notify the Contracting Officer (or Representative) regarding any contractor employee who has not satisfied residential qualifications when required by SOW or PWS within 12 months or maintained related continuing education.

2.15.20. Collect cyberspace workforce metrics and report them annually or as requested, in support of **paragraph 2.2.5** of this manual **(T-1)**.

2.15.21. Report cybersecurity workforce (civilian, military, and contractor) metrics or statistics to WCO/DCO, as required. **(T-0)**. SAF/CN will provide the instructions (e.g., reporting requirements, criteria, template, and reporting frequency) **(T-1)**.

2.15.22. Develop suitable Privacy Act compliant manual tracking and reporting for contractor cyberspace requirements **(T-1)**.

2.15.23. Define supplemental training details and methods as needed in conformance with residential training requirements according to DoDM 8140.03. Acceptable training methods include formal or classroom instruction, on-the-job training, and/or computer based or web-based training.

2.16. Contracting Officers shall:

2.16.1. Work with Program Managers, System Managers, Program Management Offices and Developmental or Operational Test Agencies to assure contract requirements are aligned with the requirements of this manual, applicable DFARS, verify contractor compliance with contract requirements, and remedy any contract deficiencies.

2.16.2. Include DFARS clause 252.239-7001 in solicitations and contracts involving contractor performance of cyberspace functions in accordance with DoDD 8140.01 as prescribed at DFARS subpart 239.7103(b) **(T-0)**.

2.16.3. Immediately notify contractor company to stop any contractor employee from performing any cyberspace related work under a government contract when that contractor employee does not meet or maintain required DoD approved cybersecurity foundational qualification **(T-0)**. Contractors are ineligible for foundational waivers as described in **Paragraph 4.3** **(T-0)**.

2.16.4. Immediately notify contractor company to stop any contractor employee from performing cyberspace work on a government contract if that contractor employee is not foundationally qualified, does not meet annual training or continuing education requirements or does not meet residential requirements as specified in the SOW or PWS **(T-0)**.

2.16.5. For the purposes of this manual, all responsibilities include the Contracting Officer Representative when permissible functions have been delegated in writing.

2.17. Information System Security Managers (ISSMs) shall:

2.17.1. Validate that all personnel are properly coded and qualified and provide updates at the close of each fiscal year to the Authorizing Official on the status of personnel within their area of responsibility or as directed.

2.17.2. Validate an individual has signed a Privileged User Agreement, completed the appropriate clearance or national security investigation appropriate for access, and meets required DoD approved cyberspace foundational requirements before a privileged account to any Systems is granted **(T-1)**.

2.17.3. Track Privileged User Agreements for each Systems as assigned and provide updates at the close of each fiscal year to the AO or WCO/DCO or as directed **(T-1)**.

2.17.4. Ensure the cyberspace workforce optional requirements meets compliance for mission readiness and management review items **(T-1)**.

2.17.5. Ensure the reporting of contractor continuing education in a manner to be prescribed by the CWMB.

2.17.6. Ensure recording and tracking of cyberspace requirements of all foreign nationals and contractors per **paragraph 1.3** of this manual.

2.18. Civilian Personnel Sections shall:

2.18.1. Process personnel action requests (e.g., Manpower Change Requests [MCRs]) in accordance with AFI 38-101, *Manpower and Organization* to identify cyberspace workforce requirements within appropriate personnel databases or systems **(T-2)**.

2.18.2. Ensure information is forwarded to the Air Force Personnel Center (AFPC) Classification Office for review and appropriate action to include updating personnel data systems and updating core personnel document and position classification **(T-2)**.

2.18.3. Work with the Labor Relations Officer to confirm collective bargaining obligations are met. **(T-2)**.

2.19. Supervisors shall:

2.19.1. Incorporate cyberspace qualification requirements in accordance with Chapters **3** and **4** of this document within the master training plan and training documentation for the cyberspace workforce.

2.19.2. Ensure personnel identified in the cyberspace workforce are properly DCWF coded and provided guidance to obtain and maintain qualifications.

2.19.3. Review all manpower positions, duty descriptions, and contract requirements to determine if cyberspace tasks are required of that position **(T-0)**.

2.19.4. Document all qualification requirements, including proficiency levels for all positions with intent to ensure that the most stringent requirements are met that covers all tasks that may span across responsibilities.

2.19.5. Reduce or limit the number of individuals requiring privileged accounts to the minimum necessary to support mission tasks in consideration of risk mitigations for accountability, non-repudiation, and availability.

2.19.6. Coordinate with the appropriate Civilian or Military Personnel Section or Servicing Classification Office to ensure the SCPD, CPD, or PRD and appropriate personnel databases or systems reflect accurately the cyberspace workforce requirements and work role codes.

2.19.7. Request the appropriate personnel section to extract reports from manpower and personnel databases or systems (e.g., MilPDS and DCPDS/DCHRMS) and to identify cyberspace workforce requirements and alignment with personnel for DAF compliance reporting.

2.19.8. Confirm all cyberspace assigned personnel complete and sign a formal statement of assigned cyberspace responsibilities **(T-0)**. **Attachment 2** lists examples of a formal statement.

2.19.9. Ensure appropriate plans are in place to account for all personnel meeting 20 hours of Continuing Education Unit (CEU) or Continuing Professional Education (CPE) requirements by the commercial provider of their Foundational Certification (whichever is greater) in accordance with **paragraph 4.1.2** of this manual **(T-2)**.

2.19.10. Approve certification exam requests only for eligible civilian and military personnel in coded cyberspace workforce positions who have more than one (1) year before a confirmed retirement or separation date **(T-1)**.

2.19.11. Ensure good stewardship over testing voucher approvals by evaluating if members can achieve qualifications through non-commercial means.

2.19.12. Validate civilian and military personnel have completed the appropriate residential requirements in accordance with paragraphs **3** and **4** of this manual for assigned tasks **(T-0)**.

2.19.13. Conduct review with employees not less than annually and revalidate their SEI, DCWF work roles, and proficiency levels **(T-2)**.

2.19.14. Report CEU or CPE status of all personnel in a manner to be determined by the CWMB.

2.19.15. Ensure appropriate reports are provided to ISSMs for workforce validation purposes.

2.20. Individuals (Civilian and Military) shall:

2.20.1. Obtain or meet appropriate DAF approved cyberspace foundational requirements applicable for cyberspace tasks required for any position held, within nine months of assignment in accordance with DoDI 8140.02 and obtain residential qualifications within 12 months of assignment **(T-0)**.

2.20.2. Maintain valid (i.e., in good standing) DAF approved cybersecurity foundational certification(s) in accordance with DODI 8140.02 if used to satisfy foundational requirements for the role **(T-0)**.

2.20.3. Become and remain qualified in their assigned cyberspace position as defined in Chapters **3** and **4** of this document **(T-0)**.

2.20.4. **(For personnel assigned to the cybersecurity workforce element or assigned a cybersecurity role)** Sign a formal statement of assigned cybersecurity responsibilities and submit to the appropriate program management office.

2.20.5. Sign a Privileged User Agreement for every privileged account assigned and submit to the appropriate program management office.

2.20.6. Authorize release of DoD approved cybersecurity foundational certification data to DoD **(T-0)**. Personnel can access and submit release authorization at this link **https://cwip.cce.af.mil** (**T-1**).

2.20.7. **(Civilians only)** Report CEU or CPE status to supervisor **(T-0).**

2.20.8. Work with their supervisors to ensure the appropriate manpower and personnel databases or systems appropriately contain the information as required by **paragraph 1.3.2** of this manual.

2.21. Individuals (Contractor Personnel) shall:

2.21.1. Obtain or meet appropriate cyberspace qualification applicable for assigned cybersecurity workforce position prior to start of contractual tasks in accordance with DoDM 8140.03 **(T-0)**.

2.21.2. Maintain valid (i.e., in good standing) DoD approved cyberspace foundational requirements **(T-0)**.

2.21.3. Maintain qualifications for cybersecurity contractor position as defined in their contract, SOW, or PWS.

2.21.4. Sign a formal statement of assigned cybersecurity responsibilities **(T-0)**.

2.21.5. Sign a Privileged User Agreement for every privileged account assigned.

2.21.6. Authorize release of DoD approved cyberspace foundational certification data to DoD if used to meet foundational requirements. **(T-0)** Personnel can access and submit release authorization at this link **https://cwip.cce.af.mil/** **(T-1)**.

2.21.7. Fulfill continuing educational requirements of a minimum of 20 hours per year as required by DoDM 8140.03.

2.21.8. Report status of continuing education requirements in manner prescribed by Contracting Officer.

Chapter 3

GUIDANCE AND PROCEDURES

3.1. Description of the DoD Cyberspace Workforce Framework

3.1.1. The DCWF describes the work performed by the Cyberspace workforce and serves as a fundamental building block for the development of qualification standards and career planning, accession, and promotion through technical or managerial tracks. It is the DoD implementation of the Federal Cyber Workforce Assessment Act (FCWAA) of 2015 and is envisioned to help DoD organizations recruit, train, educate and retain a qualified cyberspace workforce. In accordance with DoDD 8140.01, the Cyberspace workforce is defined as: "personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources, conduct related intelligence activities, enable future operations, and project power in and through cyberspace." A DAF position pursuing this mission, regardless of AFSC or SFSC, job title, occupational series, or contractor job title that performs one or more cyber-related tasks is part of the DoD cyberspace workforce.

3.1.2. The DCWF employs a hierarchical structure with categories, specialty areas, and work roles. Each role has three elements: 1) a definition; 2) a list of core and additional tasks; and 3) KSAs that describe what is needed to execute critical functions. The DCWF standardizes naming, numbering convention, and descriptions of individual roles, tasks, and KSAs to support joint assignments, reciprocity, career development, and interoperability across the DoD Enterprise.

3.1.3. Cyberspace work roles align to one of 7 workforce elements. They are: 1) IT; 2) Cybersecurity; 3) Cyberspace Effects; 4) Cyberspace Intelligence workforce; 5) Cyberspace Enablers; 6) Software Engineering; and 7) AI/Data. DAF anticipates the workforce elements and/or alignment of the DCWF to be reviewed and updated annually under the authority of the CWMB and will be available on the DoD Cyber Exchange website, the authoritative source for published updates located at **https://www.cyber.mil**. This manual will be updated as necessary to accommodate major structural changes.

3.1.4. DCWF work roles contain an occupational descriptor, composed of a civilian occupational series or military occupational code (AFSC or SFSC), and a three-digit specialty code (for civilians and military), but they **do not** align with a specific occupation **(T-0)**. They may however align with more than one career field or may be used alongside or in conjunction with other work roles. DCWF work roles always have associated KSAs and tasks.

3.2. Structure of the Workforce

3.2.1. The DCWF includes DoD civilian employees, military service members, and contractors assigned to positions requiring performance of cyberspace work and coded with a DCWF primary and additional work role codes as necessary. An individual may have up to three assigned work role codes **(T-0)**. A proficiency level is assigned for each code. There is no prioritization required to be assigned among the additional roles, though they may be assigned to meet mission requirements. The primary work role code identifies the work role that includes the majority of a position's responsibilities and represent its most significant requirement. Codes may not be used more than once to describe any position. A position may require performance of the roles at different proficiency levels.

3.2.2. Each cyberspace work role has in its qualification matrix as many as four areas to identify the options available to achieve qualifications associated with each role. These areas are: 1) Foundational Qualifications composing of education, training, or certification. In some circumstances, actual experience performing in the role may serve as a conditional alternative; 2) an optional foundational qualification based on experience; 3) a residential qualification that is based on demonstration of capability, which always includes a specific On-the-Job qualification and may include any environmental or organizational specific requirements; and 4) continuous professional development of a minimum of 20 hours per year (or vendor certification maintenance minimums, whichever is greater). Additional information regarding the location and management of these matrices can be found on the DoD Cyber Exchange site at: **https://cyber.mil/wid/dod8140/qualifications-matrices**.

3.3. Position Identification

3.3.1. While work role positions always have an associated proficiency requirement they are only to describe the levels of capability required to successfully perform the work and are not tied to any rank, grade, or seniority. They are defined by one of three designations: Basic, Intermediate, and Advanced. The definitions of each pursuant to DoDI 8140.02 paragraph 4.a.(1)(b) are thus:

3.3.1.1. Basic - the role requires an individual to have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance. An individual must be able to perform successfully in routine, structured situations.

3.3.1.2. Intermediate - 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.

3.3.1.3. Advanced - 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 provide guidance to others.

3.3.2. Civilian positions in any designated cyber occupational series must have a designated cyberspace work role or a documented justification for lack of coding. All positions aligned to the 2210, 1550, 0332, and 0335 occupational series must be coded with DCWF work roles and proficiency levels (the requirements of this paragraph are relaxed during the DAF transition period in favor of allowances contained in **paragraph 4.1.8.1** of this manual).

3.3.3. In accordance with DoDI 8140.02 paragraphs 4.b.(3 and 5), the U.S. Office of Personnel Management (OPM) guidance requires the use of the code “000” and at least one additional cyberspace work role code. Any “000” position must also include an explanation for the use of “000” primary code, where a position has been determined as non-cyberspace **(T-0).** The four civilian occupations series listed in **paragraph 3.3.2** of this manual are prohibited from using the “000” code. The CWMB will update specifics of the manner for explanation of use of the “000” code in the future.

3.3.4. Military position identification can be aided by use of the military occupation crosswalk, available for download at https://www.onetcenter.org/dl_files/2019/military_crosswalk.zip.

3.3.5. Positions occupied by partner nation personnel are also coded.

3.3.6. Any person with privileged access must be coded as an IT privileged user, even if functioning in an alternate work role, with certain exceptions as noted in **paragraph 4.3.2** of this manual.

3.4. Cyberspace Workforce Qualification and Management Program

3.4.1. As per DoDM 8140.03, the DoD Cyberspace Workforce Qualification and Management Program establishes enterprise baseline requirements by work role according to proficiency level to enhance cyberspace mission readiness across the DoD.

3.4.2. The standards are intended to be used in conjunction with OPM Qualification standards rather than as a replacement for those standards. The program is designed to develop a cyberspace workforce with a common understanding of the concepts, principles, and applications of cyberspace functions to enhance interoperability across organizations and mission sets. Cybersecurity KSAs must be integrated into the qualification requirements of all cyberspace work roles regardless of workforce element alignment. All training that meets the requirements of the DoD Cyberspace Operations Forces is accepted as meeting the qualification standards and requirements **(T-0)**.

3.4.3. Meeting the foundational, residential, and continuing education requirements outlined are not waivable, though alternative means of meeting these requirements may be substituted under the authority of the CWMB **(T-0)** with the endorsement of SAF/CNSF. These requirements are explained in DoDM 8140.03 Chap 3.2 and additional information can be found with the qualification matrix information for appropriate work roles at: **https://cyber.mil/wid/dod8140/qualifications-matrices**. Use of the matrices and due care is mandatory to assure the integrity of the enterprise workforce.

Chapter 4

PROCEDURES, EXCEPTIONS, AND WAIVERS

4.1. Normal and Amplified Procedures

4.1.1. DAF civilian and military personnel are qualified after meeting foundational and residential requirements within 12 months of assignment to their cyberspace duties; (2) publication of this manual; and (3) the position has been fully transitioned to DCWF. Completion of foundational requirements must be accomplished within the first nine months. Completion of residential requirements may be accomplished concurrently or after completion of foundational requirements.

4.1.2. Maintenance of qualification requires meeting a continuing education requirement of 20 hours per annum. Personnel relying on a vendor-provided certification to meet foundational requirements must meet the greater of this 20-hour requirement or the vendor's individualized continuing education requirements.

4.1.3. Time requirements commence on the date of assignment to each role assigned and assignment to additional roles does not extend time for any prior assigned roles. Continuing education requirements that have overlapping KSAs may be used to satisfy those requirements for any KSAs contained within the overlap. Proficiency level requirements may differ among roles, as necessary.

4.1.4. The primary work role code identifies work that encompasses the majority of a position's responsibilities. A primary work role code other than "000" indicates that performance of work defined by the skillsets identified in the framework as the primary role of the position. Secondary and tertiary codes are used to capture other key work required of the position. The primary work role indicates that 50% or greater time is spent performing duties aligned to this work role and thus captures the most significant requirements of the position, where additional work roles are used. Use "000," with the appropriate justification, as the primary work role where a position is required to complete work aligned to a specific work role that does not constitute the majority of work duties (<50% time spent), (see **paragraph 3.3** and subparagraphs of this manual). Such positions require a secondary work role, tertiary work role, or both.

4.1.5. Contracted support personnel are required to meet foundational qualifications prior to the assumption of any duties but are not required to meet residential requirements unless required by the Authorizing Official and the requirements are described in the contract, SOW, or PWS.

4.1.6. Performance periods that have commenced prior to 15 Feb 2023 shall not be construed to contain such language imposing these requirements upon contractors unless those contracts or statements of work include or specify DCWF coding. Contracts shall be updated at the earliest, most feasible opportunity to include any new requirements since the publication of this manual.

4.1.7. Authorizing Officials may extend time limits prescribed in 4.1.1. for a specifically dated period, not to exceed six months by authorizing a waiver, but only under severe operational or personnel constraints and shall not authorize any consecutive waivers **(T-0)**. MAJCOM/FLDCOM/FOA/ DRU shall archive approved waivers locally, in a manner

accessible to the representative and notify SAF/CN via **saf.cnsf.mla@us.af.mil**. MAJCOM/FLDCOM/FOA/DRU shall also provide copies to the individual's direct supervisor and the individual for inclusion in their personnel file.

4.1.8. This manual considers the DoD Enterprise and DAF's ongoing transition and paradigm shift from DoDD 8570 series policies to DoDD 8140 series policies and addresses this paradigm shift as follows:

4.1.8.1. All civilian, military, or contractor personnel who are currently filling cyber workforce positions as of the date of this publication have until 15 Feb 2026 to meet Foundational Qualifications. All personnel filling roles that are identified as belonging to the cybersecurity workforce element must be Foundationally Qualified not later than 15 Feb 2025. All 8570 codes shall remain associated with the position and requirements until that position has been fully transitioned in accordance with **paragraph 1.3** and other relevant provisions of this manual.

4.1.8.2. All personnel will continue to keep certifications and training levels in good standing.

4.1.8.3. DoD has directed all Services and components to ensure that all civilian and military positions are assigned DCWF codes and proficiency levels not later than 29 Feb 2024. DCWF coding and proficiency level requirements for current or future Contactor-filled positions have not been set as of the date of this publication.

4.1.9. The DAF has developed a Preferred List of cybersecurity certifications based upon the DoD approved cybersecurity foundational certifications. Those certifications on the DAF Preferred List have priority for funding. The list is maintained and posted on the CCC Certification and Training website at **https://cwip.cce.af.mil**.

4.1.10. To facilitate reciprocity across the DoD Enterprise, personnel may obtain or maintain certifications from the DoD approved cybersecurity foundational certification list as vetted by the CWMB.

4.1.11. Vouchers are only issued for initial and annual payment of vendor certification fees for civilian and military personnel. Issuance of any vouchers requires the individual is assigned to a cyber coded position. Vouchers may be requested via the CCC Certification and Training website: **https://cwip.cce.af.mil**.

4.1.12. CCC will pay for one exam voucher at the specified AFSC, SFSC, or DCWF requirement when the member does not already have a certification or have training or education that satisfies the foundational requirement for their primary assigned position. CCC will pay for additional exam vouchers from the DAF Preferred List when an individual is assigned additional DCWF codes that imposes additional requirements. Such allowances are subject to end of fiscal year budgetary constraints and may be on first-come basis after all DAF primary positions are served.

4.1.13. CCC may pay for annual vouchers for members who are cyber coded but currently serving in civilian development positions such as career broadening, key career positions, civilian development long-term training schools and civilian strategic leadership programs. Wherever possible, these individuals would retain their cyber codes. **(T-2)** To facilitate the return to their normal career progression, civilian personnel will maintain their qualifications

in good standing even while serving in a joint assignment, special duty assignment, or deployment.

4.1.14. CCC funds will not be used to pay for exam vouchers for civilian or military personnel who are within one (1) year of a confirmed retirement or separation date **(T-1)**.

4.1.15. Civilian personnel can update civilian personnel database(s) or system(s) through a self-certification process in the MyBiz+ application. The status of the certification would be listed as "self-certified" in the member's record. The member routinely receives an automated email with a link to upload the certificate into the AF Personnel Services application where it is verified by AFPC at Joint Base San Antonio -Randolph, TX. Once verified, the status in MyBiz+ would change to "Verified." MyBiz+ is available on the DCPDS portal: **https://compo.dcpds.cpms.osd.mil/**.

4.1.16. Military personnel (officers and enlisted) will complete DAF Form 2096, *Classification/On-the-Job Training Action*, to indicate award of the SEI for the highest cyberspace qualification obtained **(T-1)**.

4.1.16.1. The DAF Form 2096 shall be submitted within 10 working days after vendor notification of completing the DoD approved cyberspace certification. Members shall submit this form to the appropriate servicing personnel function (e.g., Force Support Squadron, Military Personnel Flight, or equivalent) to update their personnel record, after the supervisor and commander signs the form.

4.1.16.2. The SEI reflects coding for assigned UMD billet, position, AFSC or SFSC and/or DCWF requirement.

4.1.17. Cyberspace coding is based upon serving in an identified Cyber role and not as a function of rank, position of prestige, or appointment.

4.1.18. Graduates of Undergraduate Cyber Training are expected to become cyber coded and meet qualification requirements as a precondition for matriculation (entry) into the career field **(T-1)**.

4.1.18.1. Once assigned to cyberspace-coded position, Cyber Operations (17XX) officers will meet DCWF foundational requirements within nine (9) months of duty assignment **(T-0)**.

4.1.18.2. Once DCWF qualifications are obtained, 17X officers will maintain their qualifications in good standing even while serving in a joint assignment, special duty assignment, or deployment **(T-1)**.

4.1.19. An individual's cyberspace certification may be accepted for credit at the Community College of the Air Force, based on applicable degree requirements. It is recommended for individuals contact their local education office to verify applicability.

4.2. Exceptional Procedures

4.2.1. DAF Civilian and military personnel may temporarily perform cyberspace position duties while working toward meeting qualification requirements under the direct observation and supervision of a qualified individual. The responsible AO, with a recommendation from the ISSM must determine the allowable period. If such observation is not feasible, the

observational requirement may be waived due to severe operational or personnel constraints, otherwise the individual must be reassigned duties consistent with their qualifications **(T-1)**.

4.2.2. Deployment line remarks may be established for each DCWF code and proficiency level of cyberspace qualifications to allow the Combatant Commanders the flexibility to identify the appropriate cyberspace workforce requirements in a deployed environment not already identified in the Unit Type Code (UTC) Manpower Details section and/or to facilitate reciprocity across the DoD Enterprise.

4.2.3. Each military member assigned or tasked as a UTC substitute will meet the cybersecurity certification requirements where the Mission Capability Statement or manpower detail SEI includes cybersecurity responsibilities **(T-1)**.

4.3. Waivers to procedure

4.3.1. Units will initiate a waiver from normal procedures, as appropriate, by consulting their appointed representative as noted in **paragraph 2.9.6** of this manual. After vetting the request, representatives shall endorse the request with rationale and forward to the responsible Authorizing Official for their consideration if within the scope of the Authorizing Official's authority. Requests requiring higher authority are considered and endorsed with SAF/CN and as appropriate, forwarded to the CWMB for final approval.

4.3.2. Cybersecurity is critical for ensuring information is protected and the Systems meets the operational requirements as designed under any cyber situation. Select DAF workforce personnel (e.g., aircrew, maintenance, researchers, and system technicians) may need limited elevated permissions to perform tasks as required by DAF publications (e.g., technical orders, aids, software handbooks, checklists, and contractor-developed technical manual procedures) to facilitate operation, troubleshooting and repair of systems. Limited elevated permissions are elevated network rights for a specific requirement as required by DAF publications but do not include all permissions of a privileged user. These tasks potentially require DCWF qualifications beyond the requirements established in publications such as mission design series documents and technical orders. These DAF publications have been vetted and approved by the responsible AO under previous models to prevent the unauthorized alteration of a system cybersecurity posture. Such approvals should be newly reviewed for applicability by relevant responsible parties. The responsible AO shall make a DCWF identification and requirements determination, exempting individuals who have limited elevated network or system permissions to systems. The determination must apply only to systems under the AO's authority and responsibility for risk acceptance **(T-1)**. The PM will initiate the exemption determination memo, the ISSM will coordinate on the memo and the AO will sign the memo **(T-1)**. The PM will ensure the exemption determination memo includes the following items:

4.3.2.1. General description of specific systems.

4.3.2.2. Details on specific positions, including AFSC, SFSCs, or occupational series to be exempted.

4.3.2.3. Rationale why a DoD approved cyberspace foundational qualification is not required.

4.3.2.4. Details on specific actions to be performed by an individual or individuals as required by DAF publications that necessitate limited elevated permissions.

4.3.2.5. Details on security risk mitigations implemented to enable limited permissions. Relevant details include reference info (e.g., hyperlinks, pointers, nomenclature) for DAF publications (e.g., Technical Orders, aids, software handbooks, checklists, and contractor-developed technical manual procedures).

4.3.2.6. Statements indicating the AO has vetted and accepted risk as described in DAF publications.

4.3.2.7. Statements describing process on how exempted personnel are vetted initially and annually.

4.3.2.8. Details on the specialized training and recurrence of exempted individuals (e.g., personnel must be recertified every "X" months on checklist procedures by 7-level evaluator or technician).

4.3.2.9. Statements indicating exempted individuals sign a user agreement stipulating the authorized actions or procedures to be performed.

4.3.2.10. The PMO or functional system owner will maintain the exemption memo and forward a copy of the signed memo to the DAF CISO for the affected Systems.

4.3.2.11. Exempted individuals must be classified as "Authorized Users" on the approved network or system account request form (e.g., DD Form 2875, *System Authorization Access Request* (SAAR)).

4.3.2.12. The PMO or unit must complete and document in memo format an annual validation, occurring on anniversary date of exemption approval that includes identifying information of all exempted personnel and Systems. The ISSM will sign the memo and route to the AO for approval. The PMOs and units must maintain and track validation memos locally and forward a copy of the signed validation letter to the DAF CISO via SAF/CN.

4.4. Failure to meet or maintain qualifications

4.4.1. Civilian and military personnel may be subject to administrative action if they do not obtain or maintain foundational requirements within nine months of assignment to a DCWF coded role, meet residential requirements within 12 months of assignment to DCWF coded role, or maintain their qualified status by meeting continuing education requirements.

4.4.1.1. During the 8570 to 8140 transition period, incumbent members are expected to maintain DAF funded certifications by meeting continuing education requirements and requesting and submitting their voucher for annual fees, unless officially notified that the certification will not be required for any of their DCWF coded role and their role is in progress to transition to DCWF in that fiscal year.

4.4.1.2. Waivers may be obtained pursuant to applicable provisions and procedures as outlined in this manual.

4.4.1.3. Maintenance of self-funded certifications are recommended but not required, but if the civilian or military member has maintained a self-funded certification and it fulfills the foundational requirements for their new DCWF coded role, a reimbursement can be made subject to end of fiscal year funding allowances. This provision expires at the end of FY24.

4.4.2. CCC will not pay for any re-testing required after an initial exam failure or decertification for civilian or military personnel, except where re-testing was conducted at initial skills training (IST) or schoolhouses. The individual will be responsible for paying to re-test, however PMOs or units may fund with internal resources for a re-testing at their discretion. SAF/CN may direct exceptions on a case-by-case basis, in coordination with AF/A2/6 or SF/COO, as appropriate.

4.4.3. Privileged access shall be removed for any personnel who does not have or maintain qualifications in active and good standing after the transition date.

4.4.4. Civilian personnel that have not obtained foundational qualifications commensurate with their DCWF coded position within nine months of assignment or have not obtained residential qualifications within 12 months of assignment may not perform any cyberspace tasks unless under the direct supervision of a cyberspace qualified individual. **(T-1).** The commander determines appropriate actions in accordance with local civilian personnel policies.

4.4.4.1. The commander shall immediately contact the servicing civilian personnel section and follow local administrative procedures regarding the individual's primary duties, DCWF role, or both.

4.4.4.2. Remaining cyberspace tasks must be reassigned to another individual who has the appropriate qualification in good standing. The commander has the discretion to allow individuals to resume additional tasks once that individual obtains the appropriate qualification(s) **(T-3)**.

4.4.5. Military members that have not obtained foundational qualifications commensurate with their DCWF coded position within nine months of assignment or has not obtained residential qualifications within 12 months of assignment may not perform any cyberspace tasks unless under the direct supervision of a cyberspace qualified individual.

4.4.5.1. Commanders may place military members in remedial training (e.g., CBT, hands-on training or instructor-led training) during this time. Military members with demonstrated capacity for good study habits may be approved for a curriculum of self-study.

4.4.5.2. If the military member is not incumbent to the position the commander shall meet with both the supervisor and military member to reassess whether the individual possesses the necessary skills to perform in the cyberspace position. This assessment should include but is not limited to contextual factors of the individual's aptitude, motivation, experience, and knowledge level to perform at the required proficiency level in the cyberspace position. Commanders should exercise restraint from using this section as the basis for administrative or punitive action against the member when reasonableness in making the assignment could have prevented failure.

4.4.5.3. Commanders shall begin AFSC or SFSC disqualification actions in accordance with AFMAN 36-2100, Military Utilization and Classification after second test failure where a certification is indicated to meet foundational qualification for matriculation into an AFSC or SFSC and it has not been met within the time period prescribed **(T-1)**.

4.4.5.3.1. Waivers are not appropriate for granting time extensions due to examination failure.

4.4.5.3.2. If required certification is not attained or maintained, applicable SEI codes must be removed from the individual's military personnel records **(T-1)**.

4.4.5.3.3. Commanders of PMOs or units have the discretion to retain the individual or pursue other appropriate administrative actions.

4.4.5.3.4. If the military member is retained, supervisors shall validate the member's readiness for re-testing and ensure the member is scheduled to retake the certification.

Chapter 5

CYBERSPACE WORKFORCE TRAINING

5.1. Skills Training and Learning Resources

5.1.1. Initial Skills Training (IST) for various AFSC or SFSCs include cybersecurity concepts and practices as well as an organic, schoolhouse provided test preparation course for a cyberspace certification exam. Distributive or online learning is available, or units can elect to fund training for those civilian and military personnel who cannot attend one of these IST programs.

5.1.2. Distributive learning resources are available at no cost to civilian and military users. Examples include e-Learning on the AF Portal, Digital University, and the Federal Virtual Training Environment managed by the Department of Homeland Security. PMOs or units have the discretion to provide additional training resources that can supplement resources provided by AF/A2/6, SAF/CN, AETC, or CCC.

5.1.3. AO candidates must complete the AO CBT (3.0 hours), Personally Identifiable Information (PII) CBT (1.0 hours), and the eMASS CBT (2.0 hours) prior to appointment as an AO. Candidates must complete the DoD AO Course within 60 days of appointment **(T-0).** DAF mandated training must be completed within 120 days of assignment **(T-1)**. Other AO requirements are anticipated to be listed in the upcoming (revision) DAFI 17-101, *Risk Management Framework for Information Technology*.

5.1.4. PMOs or units may procure instructor-led training or virtual instructor-led training to provide certification specific training for personnel unable to obtain certification through distributive learning. The PMO or unit must use appropriate contracting methods.

5.2. Military Specific Training Options

5.2.1. Military career accession has several options for military members, any combination of which can be used to satisfy foundational, residential, or continuing education qualifications.

5.2.2. DAF Specialty Training schoolhouses or technical schools provide the building blocks for military cyber training and provide apprentice-level learning.

5.2.3. CBTs or DoD developed classroom training are recommended to provide additional training not covered by formal AFSC or SFSC Specialty training, schoolhouse technical schools, or commercially available courses.

5.2.4. Residential or Operating System training completion certificates can be obtained from vendor-provided commercial training. Commercial training is at the discretion of and can be funded by the MAJCOM, FLDCOM, AO, or individual PMO or unit. The AO, PMO, or unit must use appropriate contracting methods.

5.3. Civilian Specific Training Options

5.3.1. Civilian career accession has several options for civilian members, any combination of which can be used to satisfy foundational, residential, or continuing education qualifications.

5.3.2. Use of CBTs or DoD-developed classroom training are the preferred methods for obtaining residential or Operating System training completion certificates. Training can be

obtained through various sources (e.g., AF learning management systems, the DoD Cyber Exchange NIPR portal, DC3, Cyber Training Academy [CTA], etc.).

5.3.3. Residential or Operating System training completion certificates may be obtained from commercial sources. This training is at the discretion of and can be funded by the MAJCOM, FLDCOM, or individual PMO or unit. The PMO or unit must use appropriate contracting methods.

5.4. Contractor Specific Training Options

5.4.1. Contractors are responsible for their own Residential or Operating System training unless otherwise stated in the contract requirements. Provisions provided in paragraphs of 5.2 and 5.3 of this manual are available for inclusion in contract requirements **(T-3)**.

Chapter 6

REPORTING AND METRICS

6.1. DAF Internal Reporting

6.1.1. MAJCOM/FLDCOM/DRU representatives shall prepare a report at the end of each fiscal year and as requested on the health and status of the Cyber workforce in the format and manner to be prescribed according to the request. Reports may include lessons learned and are signed by a functional at the GO/SES level. Reporting is intended to make internal improvements and recommendations to the DAF Cyberspace Workforce Improvement Group as well as better inform the OPR as to policy effectiveness, alignment with intent, and the reduction of non-productive administrative overhead.

6.2. Reporting Formats

6.2.1. Reporting formats may be updated in a future revision of this manual in accordance with requirements of the CWMB.

6.3. DAF External Reporting

6.3.1. SAF/CNSF may periodically report the status of total force compliance with Cyber Awareness training. MAJCOM/FLDCOM/DRU representatives may be required to assist with providing per unit metrics until the DoD Identity, Credential and Access Management (ICAM) program is fully functioning to meet the data collection requirements, then the requirement may be discontinued at SAF/CN option.

MRS. VENICE M. GOODWINE, SES, DAF
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Committee for National Security Systems (CNSS) 4009 Glossary, 2 March 2022

DoDI 1100.22, *Policy and Procedures for Determining Workforce Mix,* April 12, 2010

DoDI 7730.68, *Uniformed Services Human Resources Information System*, September 1, 2023

DoDI 1400.25, *DoD Civilian Personnel Management System,* January 10, 2022

DoDI 1444.02, *Data Submission Requirements for DoD Civilian Personnel,* July 23, 2020

DoDD 5124.02, *Under Secretary of Defense for Personnel and Readiness (USD(P&R)),* June 23, 2008

DoDD 5205.15E, *DoD Forensic Enterprise*, October 15, 2018

DoDD 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, July 27, 2017

DoDI 7730.64, *Automated Extracts of Manpower and Unit Organizational Element Files*, December 11, 2004

DoDD 7730.65, *DoD Readiness Reporting System*, 31 May 2023

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, 27 July 2017

DoDD 8140.01, *Cyberspace Workforce Management*, 5 October 2020

DoDI 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements*, 21 December 2021

DoDM 8140.03, *Cyberspace Workforce Qualification and Management Program*, 15 February 2023

DoDI 8500.01, *Cybersecurity*, 7 October 2019

AFI 17-101, *Risk Management Framework for Information Technology (IT)*, 6 Feb 2020

AFI 33-322, *Records Management and Information Governance Program,* 23 Mar 2020

DoDI 1322.33_DAFI 36-2683, *Department of the Air Force Voluntary Credentialing Programs*

AFMAN 36-2100, *Military Utilization and Classification*, 7 Apr 2021

DAFI 36-2710, Equal Opportunity Program, 18 June 2020

AFI 38-101, *Manpower and Organization,* 6 Jul 2021

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

DAF Form 2096, *Classification/On-the-Job Training Action*

DD Form 2875, *System Authorization Access Request (SAAR)*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFECD—Air Force Enlisted Classification Directory

AFI—Air Force Instruction

AFIN—Air Force Information Network

AFMAN—Air Force Manual

AFOCD—Air Force Officer Classification

AFPC—Air Force Personnel Center

AFPD—Air Force Policy Directive

AFR—Air Force Reserve

AFSC—Air Force Specialty Code

AI—Artificial Intelligence

ANG—Air National Guard

AO—Authorizing Official

CBT—Computer Based Training

CDRL—Contract Data Requirement List

CEU—Continuing Education Units

CIO—Chief Information Officer

CISO—Chief Information Security Officer

CCMD—Combatant Command

CPD—Core Personnel Document

CPE—Continuing Professional Education

CPS—Civilian Personnel Section

CTA—Cyber Training Academy

CWMB—Cyberspace Workforce Management Board

DAF—Department of Air Force

DAFCWIG—DAF Cyberspace Workforce Improvement Group

DAFDPO—Department of Air Force Departmental Publishing Office

DC3—DoD Cyber Crime Center

DCHRMS—Defense Civilian Human Resource Management System

DCWF—DoD Cyberspace Workforce Framework

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DRU—Direct Reporting Unit

FAR—Federal Acquisition Regulation

FCWAA—Federal Cyber Workforce Assessment Act

FLDCOM—Field Command (USSF only)

FOA—Field Operating Agency

HR—Human Resources

ISSM—Information Systems Security Manager

IST—Initial Skills Training

IT—Information Technology

KSA—Knowledge, Skills, Ability

MAJCOM—Major Command (USAF only)

MCR—Manpower Change Requests

MOU—Memorandum of Understanding

MPES—Manpower Programming and Execution System

OPR—Office of Primary Responsibility

OPM—Office of Personnel Management

PEM—Program Element Monitor

PIT—Platform IT (System)

PME—Professional Military Education

PMO—Program Management Office

POM—Program Objective Memorandum

PRD—Position Requirements Document

PWS—Performance Work Statement

SAP—Special Access Programs

SCPD—Standard Core Personnel Documents

SEI—Special Experience Identifier

SFSC—Space Force Specialty Code

SOW—Statement of Work

STARCOM—Space Training and Readiness Command

UMD—Unit Manning Document

USAF—United States Air Force

USSF—United States Space Force

UTC—Unit Type Code

WCO—Wing Cyberspace Office

Office Symbols

AF/A1—Deputy Chief of Staff for Manpower, Personnel and Services

SAF/AA—The Administrative Assistant to the Secretary of the Air Force

SAF/AQ—Assistant Secretary of the Air Force, Acquisition, Technology, & Logistics

SAF/CN—DAF Chief Information Officer

SAF/CNSF—Civilian Force Development

SF/COO—The Deputy Chief of Space Operations for Operations, Cyber and Nuclear

SF/S1—Deputy Chief of Space Operations for Human Capital

USD (I&S)—Under Secretary of Defense for Intelligence and Security

Terms

Approval Authority—Senior leader responsible for contributing to and implementing policies and guidance/procedures pertaining to his/her functional area(s) (e.g., heads of functional two-letter offices). As used in this document refers to Tier-level.

Civilian Employee—as defined by OPM, and for the purposes of this document, includes overhires.

Contracting Officer—See FAR 2.101. For purposes of this manual, includes contracting officer's representative when the task or function is delegated to the contracting officer's representative in the contracting officer's letter of designation.

Cyber Occupational Series—Every position within the occupational or career management field or program that is considered cyberspace. This could include members of the IT Workforce.

Cyberspace Effects Workforce—Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

Cyberspace Enabler Workforce—Personnel who perform work roles to support or facilitate the functions of cyber IT, cybersecurity, cyberspace effects, or intelligence workforce (cyberspace) work roles. This includes actions to support acquisition, training and leadership activities.

Cyberspace Operations—Defined in CNSSI 4009.

Cyberspace Operations Forces—Five operational groups specifically categorized as the DoD Cyberspace Operations Forces, including cyber mission forces, United States Cyber Command subordinate command elements, DoD Component network operations centers and cyber security service providers, special capability providers and specially designated units.

Cyberspace Workforce—Personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to cyberspace workforce elements.

Cyberspace Workforce Elements—Also referred to as "skill categories." The DoD cyberspace workforce is divided into seven elements: IT, cybersecurity, cyberspace effects, intelligence workforce (cyberspace), cyberspace enablers, software engineering, and AI/Data.

DoD Cyberspace Workforce Framework (DCWF)—The authoritative reference for the identification, tracking, and reporting of DoD cyberspace positions and the foundation for developing enterprise baseline cyberspace workforce qualifications.

Information System—Defined in CNSSI 4009.

Intelligence Workforce (Cyberspace)—Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.

IT—Defined in CNSSI 4009.

IT Privileged User—A user who has roles that allow read, write, or change access to manage IT systems including system, network, or database administrators and security analysts who manage audit logs. IT privileged user roles are generic to all IT infrastructure, including transport, hosting environments, cybersecurity, and application deployment.

IT Workforce—Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize implement, evaluate, and dispose of IT as well as information resource management, and the management, storage, transmission, and display of data and information.

KSAs—The attributes required to perform a job, typically demonstrated through qualifying experience, education, or training.

Manpower Data—Information about the cyberspace position or billet.

Personnel Data—Information about the person performing cyberspace work in the specified position or billet.

Primary Work Role Code—The primary work role code is used to identify a specific work role within the DoD cyberspace workforce and identifies the work role that encompasses most of the billet's responsibilities. If a primary work role code from 111 to 999 is used, this indicates that cyberspace work is the primary role of the billet.

Platform Information Technology—As defined in DoDI 8500.01, as IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Platform Information Technology System—As defined in DoDI 8500.01, as a collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. In some instances, the terms PIT and PIT System are used interchangeably.

Qualified—An established set of criteria aligned with the KSAs and tasks of a specific cyberspace work role that shows that an individual can do them. Qualification criteria consists of these three minimum requirements: 1) Foundational (education, training, or personnel certification); 2) Residential (on-the-job qualification and discretionary environment-specific requirements); and 3) Continuous Professional Development requirements.

Task—An activity a person performs to carry out the functions of the job. It may be regular or infrequent.

Total Force—Defined in DoDD 5124.02, *Under Secretary of Defense for Personnel and Readiness (USD(P&R))* as: "The organizations, units, and individuals that comprise the DoD resources for implementing the National Security Strategy. It includes DoD Active and Reserve Component military personnel, military retired members, DoD civilian personnel (including foreign national direct- and indirect-hire, as well as nonappropriated fund employees), contractors, and host-nation support personnel."

Work Role—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.

Attachment 2

FORMAL STATEMENT OF RESPONSIBILITES (APPLICABLE FOR CIVILIANS AND MILITARY)

A2.1. The Formal Statement of Assigned Cybersecurity responsibilities may be completed using **Figure A2.1**.

Figure A2.1. Sample Formal Statement of Assigned Cybersecurity Responsibilities.

(Appropriate letterhead)

Date

MEMORANDUM FOR RECORD

SUBJECT: Formal Statement of Assigned Cybersecurity Responsibilities

1. I understand I have been assigned to a cybersecurity position on the [INSERT UNIT NAME HERE] Unit Manning Document (UMD). In accordance with DAFMAN 17-1305, *Department of Air Force Cyberspace Workforce Management Program*, chapter 2, supervisors and members will sign a formal statement of assigned cybersecurity responsibilities. Details of the UMD position number, Special Experience Identifier (SEI), Cybersecurity Workforce Category or Specialty, and Cybersecurity Workforce Level have been identified and are listed below:

UMD Position Number:
SEI Required:
DCWF Code:
DCWF Proficiency Level:

2. Upon being assigned, I am or may be expected to perform all or some of the cybersecurity tasks as defined in DAFMAN 17-1305, my Position Description or other applicable documents. My supervisor has reviewed with me the applicable tasks.

3. I will obtain and maintain the necessary DCWF Foundational and Residential Qualifications applicable for the cybersecurity role assigned above for the above position in accordance with DAFMAN 17-1305.

Member’s Signature Block

Supervisor’s Signature Block

A2.2. The Formal Statement of Assigned Cybersecurity responsibilities for contractors may be completed by using **Figure A2.2.** as an example as identified in **chapter 2**. The document is kept locally.

Figure A2.2. Sample Formal Statement of Assigned Cybersecurity Responsibilities.

(Appropriate letterhead)

Date

MEMORANDUM FOR RECORD

SUBJECT: Formal Statement of Assigned Cybersecurity Responsibilities

1. In accordance with paragraph 2.21.4 of DAFMAN 17-1305, *Department of Air Force Cyberspace Workforce Management Program*, I understand my contract role has a DCWF Foundational (and Residential) Qualification requirement as stipulated in [PLEASE INSERT CONTRACT NAME] and that I must be Foundationally Qualified before commencement of assigned duties. (If Residential Qualifications are required, compliance must be attained within 12 months and specified in the Statement of Work per chapters 4 and 5.)

2. I must meet annual continuing education requirements to maintain my Foundational Qualifications as per Paragraph 2.21 of DAFMAN 17-1305.

Details of my role have been identified and are listed below:
Contract or PWS Name:
DCWF Code:
DCWF Proficiency Level:

CAUTION: For Contractors, only collect contract information on the Formal Statement of Responsibilities Form in accordance with the Paperwork Reduction Act process.

Contractor's Signature Block

COR or Designated Gov Representative's Signature Block

A2.3. Privileged User agreement addendum

Figure A2.3. Privileged User Agreement Addendum

I understand, acknowledge and consent to the following:

1) I am accessing a U.S. Government Information System (which includes any device attached to this Information System) that is provided for U.S. Government authorized used only.

2) The U.S. Government routinely intercepts and monitors communications on this Information System for purposes including, but not limited to, penetration testing, Information Systems Security Monitoring, network operations and defense, personnel misconduct, law enforcement and counterintelligence investigations.

3) The U.S. Government may inspect and seize data stored on this Information System, at any time.

4) Communications using, or data stored on, this Information System are not private; are subject to routine monitoring, interception and search; and may be disclosed or used for any U.S. Government-authorized purpose.

5) This Information System includes security measures (e.g., authentication and access controls) to protect U.S. Government interests – not for my personal benefit or privacy.

a. I understand that access to a U.S. Government system or network is a revocable privilege, and that failure to comply with requirements is a violation of the trust extended to me and may result in one or more administrative or judicial actions such as, but not limited to: chain of command revoking access or user privileges; counseling; adverse actions under the UCMJ or criminal prosecution; discharge or loss of employment; security incident reporting; or revocation of security clearances and access.

b. I am responsible for all actions taken under my administrative or root account(s) and understand that the exploitation of this account could have catastrophic effects to all networks for which I have access. I will only use the privileged access granted to me to perform authorized tasks for mission related functions. I will use my general user account at all other times.

c. I will protect the administrative or root account(s), passwords, and other authenticator(s) to the highest level of data or resource it secures.

d. I will not share the administrative or root account(s), passwords, and other authenticator(s) entrusted for my use.

e. I will not create or elevate privileged rights of others, share permissions to Information Systems not authorized, nor allow others access to Information Systems or networks under my privileged account.

f. If I work in a capacity where I have rights to remotely log into users' systems, I will ensure they are positively informed of my presence prior to taking any actions on their systems.

g. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate security representatives.