VICEROY SCHOLAR HANDBOOK

Revised:
July 2025

VICEROY

VICEROY Student Handbook – Table of Contents

Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY) Handbook

I. Introduction

Welcome to the **VICEROY Initiative**. As a VICEROY Scholar, you are joining a national effort to build the next generation of professionals advancing research and operations in cybersecurity, the electromagnetic spectrum, and other areas critical to U.S. defense and national security.

Through your VICEROY institute, you will engage in an academic program aligned with the U.S. Office of Personnel Management (OPM) standards. You will also participate in cyber-spectrum co-curricular clubs and defense-relevant competitions that reflect real-world Department of Defense (DoD) mission scenarios and challenges, and complete applied learning experiences designed to build your technical expertise and connect you with DoD missions and leaders. To remain in good standing, current Scholars must maintain eligibility for a security clearance and a minimum 3.2 GPA.

This guide outlines your responsibilities, program expectations, and the resources available to support your success.

II. VICEROY Scholar Designations

A. VICEROY Scholars

To be recognized as a VICEROY Scholar, you must:

1. Maintain eligibility for security clearance.
2. Complete an academic program aligned with OPM standards.
3. Maintain a minimum GPA of 3.0.
4. Engage in a cyber-spectrum co-curricular club.
5. Participate in cyber competitions.
6. Complete an applied learning experience.

B. VICEROY Scholars with Honors

To earn this designation, you must fulfill all VICEROY Scholar criteria plus:

1. Participate in mentorship and/or engagement initiatives.
2. Complete a DoD related internship.
3. Participate in the annual VICEROY Symposium.

III. Core VICEROY Scholar Tasks

As a VICEROY Scholar, you will practice and maintain VICEROY values and professionalism in all program-related communications, as you complete the following tasks:

RETURN TO TABLE OF CONTENTS

1. Complete a security clearance disclosure form to ensure understanding of eligibility and responsibilities regarding clearance maintenance.
2. Participate in DoD-aligned curriculum including courses and certifications focused on cybersecurity, the electromagnetic spectrum, cryptography, data science, and/or strategic languages.
3. Engage actively in a cyber-spectrum co-curricular club through your local college or university, which offers workshops, seminars, and access to cyber competitions.
4. Participate in at least one cyber competition annually.
5. Complete an applied learning experience such as hands-on projects, research, or earn DoD-approved cybersecurity certifications.

*VICEROY Scholars will be required to submit artifacts demonstrating the completion of required tasks. Submissions will be made through an online platform, access to which will be provided after onboarding.

IV. Supplementary VICEROY Scholar Tasks

In addition to core tasks, you are encouraged to:

1. Pursue guidance and support for obtaining a security clearance.
2. Participate in mentorship programs and community engagement activities.
3. Complete a DoD-related internship or relevant practical experience.
4. Participate in the annual VICEROY Symposium as a presenter or attendee.

V. Virtual Institute-Specific Procedures

Your institution, together with the VICEROY Leadership Team, will provide you with detailed information on:

- Application process and eligibility criteria.
- Institution programs and scholarships.
- Cyber competition training and involvement.
- Cyber-spectrum club engagement.
- Applied learning experiences, including internships and projects.
- Mentorship opportunities, internship placements, and Symposium participation processes.

VI. VICEROY Scholar Onboarding and Certification

- Students will submit their initial application through an online portal managed by the VICEROY Leadership Team.
- Leadership from each student's college or university will conduct institution-specific down selection to determine acceptance into the VICEROY Initiative.
- Upon admittance, the VICEROY Leadership Team will provide access to the VICEROY Learning Management System (LMS), where you will submit evidence of program progress.
- Scholars' achievements will be evaluated through the LMS, and upon meeting program requirements, you will receive formal recognition and a completion stipend.

RETURN TO TABLE OF CONTENTS

- Scholars who earn Honors will receive additional commendations.

VII. Engagement and Community

Active engagement is critical to your success as a VICEROY Scholar. By participating in mentoring sessions, workshops, virtual events, and the annual Symposium, you will deepen your technical expertise, expand your professional network, and contribute meaningfully to the VICEROY community.

You can connect and collaborate with program staff and fellow scholars through multiple channels, including:

- **Monthly webinars:** Expert-led sessions on topics relevant to cybersecurity, the electromagnetic spectrum, and Department of Defense mission areas, designed to support your academic and professional growth.
- **Communication channels:** Stay connected through official platforms and tools shared by your institute and the VICEROY Leadership Team, where you'll receive updates, resources, and opportunities.
- **Annual Symposium participation:** Engage directly with DoD leaders, industry experts, and fellow scholars during this capstone event featuring keynotes, panels, and career development sessions.
- **Exclusive Alumni Network:** Upon successful completion of the VICEROY Initiative, you'll gain access to a private alumni network—open only to program graduates—designed to foster continued collaboration, mentoring, and career advancement in national security fields.

VIII. Internship Participation

Internship Experience

Participating in a VICEROY internship is an invaluable opportunity to:

- Contribute to real-world Department of Defense (DoD) projects and gain hands-on experience in cyber and electromagnetic spectrum research, development, and operations.
- Build your professional network by collaborating with fellow VICEROY Scholars and engaging with DoD professionals from across the country.
- Gain national exposure through placements at host sites across the U.S.—with all travel, housing, and logistical expenses covered.
- Strengthen your resume with meaningful work that supports national security and advances your technical skillset.
- Receive mentorship from subject matter experts committed to your growth and success.
- Open doors to future career opportunities in the defense ecosystem through early engagement and visibility.
- Select from multiple internship tracks based on your goals and experience:

RETURN TO TABLE OF CONTENTS

- **MAVEN** – An 8-week cyber-spectrum bootcamp blending technical immersion with DoD operations, culminating in a mission-aligned capstone, poster session, and research paper.
- **ENVOY** – A 10-week internship directly placing students in DoD operational roles to support high-impact projects; includes security clearance processing if required.
- **MAVEN Assistant** – A leadership position supporting program delivery, mentoring interns, and contributing to cyber and EMS research coordination.

Your Path to Placement: Applications open in early fall; intern selections are made around the New Year, and placements are finalized by mid-spring.

IX. Virtual Institute Roles to Support Scholars

As a VICEROY Scholar, your institute is your primary source of high-quality educational content aligned with Department of Defense (DoD) priorities in cybersecurity and the electromagnetic spectrum. It provides:

- Access to academic programs and credentials aligned with DoD standards (including DoDI 8140 Cyber Work Roles and OPM standards).
- Support to help you meet VICEROY program requirements.
- Guidance on career development, including networking and internship placement.
- Opportunities to participate in VICEROY's annual Symposium.
- Access to cyber-spectrum co-curricular clubs and defense-relevant competitions.
- Opportunities to compete in DoD-aligned cyber and spectrum competitions that simulate real-world mission challenges.
- Opportunities to complete applied learning experiences connected to DoD missions.

X. Contact and Resources

- For questions, support, or more information, please contact us at: **VICEROY@griffissinstitute.org**
- For the latest updates and resources, visit VICEROYScholars.org and follow us on our social media channels:

    - **Twitter:** @VICEROYScholars
    - **LinkedIn:** @VICEROYScholars
    - **Facebook:** @VICEROYScholars
    - **Instagram:** @VICEROYScholars

RETURN TO TABLE OF CONTENTS

Appendix A – DoDI 8140 Cyber Work Roles

DoD Manual 8140.03

Cyberspace Workforce Qualification and Management Program

Originating Component:	Office of the DoD Chief Information Officer
Effective:	February 15, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended
Approved by:	John B. Sherman, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02 and the policy in DoDD 8140.01, this issuance:

- Implements policy, assigns responsibilities, and prescribes procedures for the qualification of personnel identified as members of the DoD cyberspace workforce.
- Identifies members of the DoD cyberspace workforce based on the cyberspace work role(s) of the position(s) assigned, as described in DoD Instruction (DoDI) 8140.02.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to:

a. OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. All DoD personnel assigned to positions requiring the performance of cyberspace work as identified in DoDI 8140.02, in accordance with the DoD Cyberspace Workforce Framework (DCWF). This includes Service members, DoD civilian employees (including non-appropriated fund employees), personnel who provide contracted services (referred to in this issuance as "contractors"), and foreign nationals.

1.2. POLICY.

The DoD:

a. Directs Service members and DoD civilian employees assigned to a position coded with a DCWF work role code (referred to in this issuance as "cyberspace workforce positions") to be fully qualified and identified as such in authoritative manpower and personnel systems in accordance with DoDD 8140.01, DoDI 8140.02, and this issuance.

b. Adheres to the Office of Personnel Management (OPM) General Schedule Qualification Standards and the Federal Wage System Qualifications for the minimum qualification requirements for specific civilian occupation series. The requirements established by this issuance:

(1) Are explicitly for the purpose of defining minimum requirements to serve in positions that are coded for specific cyberspace work roles.

(2) Should not be construed to modify, replace, or conflict with the General Schedule Qualifications experience, education, and proficiency requirements established by the OPM (available at https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards).

c. Requires contractors to be fully qualified by qualification standards and requirements in accordance with DoDD 8140.01 and this issuance.

d. Utilizes the DCWF, as detailed in DoDD 8140.01, DoDI 8140.02, and this issuance, for standardizing qualification criteria for cyberspace work roles across the DoD.

e. Maintains a total force management perspective when staffing identified and authorized DoD cyberspace workforce positions with qualified DoD civilian employees and Service members, augmented, where appropriate, by contractors in accordance with DoDI 1100.22.

f. Accepts, to the extent appropriate and possible, foundational qualification data from other OSD and DoD Components to maximize reciprocity across the enterprise.

g. Requires cyberspace personnel meet security classification standards and sensitivity levels commensurate with position in accordance with DoDI 5200.02 and DoD Manual 5200.02.

1.3. INFORMATION COLLECTIONS.

The routine coordination referred to in this issuance does not require licensing with a report control symbol in accordance with Paragraph 9 of Volume 1 of DoD Manual 8910.01.

1.4. ALIGNMENT OF CYBERSPACE WORK ROLES TO CYBERSPACE WORKFORCE ELEMENTS.

For the purposes of accountability, oversight, and reporting, each cyberspace workforce position is aligned to a workforce element as defined in DoDD 8140.01. A figure representing the alignment of cyberspace work roles to cyberspace workforce elements is available on the DoD Cyber Exchange site at: https://cyber.mil/cw/dcwf/. The figure will be reviewed at least annually and updated, as needed, under the authority of the Cyberspace Workforce Management Board (CWMB).

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

In addition to the responsibilities in Paragraph 2.5., and in accordance with DoDD 8140.01, the DoD CIO:

a. Collaborates with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), Under Secretary of Defense for Intelligence and Security (USD(I&S)), Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), Under Secretary of Defense for Research and Engineering (USD(R&E)), the DoD Principal Cyber Advisor (PCA), and OSD and DoD Component heads to provide recommendations to the CWMB for approval regarding the development of DoD cyberspace workforce metrics to support DoD cyberspace workforce management and the requirements of DoDD 8140.01, DoDI 8140.02, Volume 1 of DoD Manual 8910.01, and this issuance.

b. Oversees work role qualification requirement, development, and management for information technology (IT), cybersecurity, and cyberspace enabler workforce elements in accordance with DoDD 8140.01, DoDI 8140.02, and this issuance.

c. Integrates the requirements of the DoDD 8140.01, DoDI 8140.02, and this issuance into the management policies, procedures, and requirements of the IT, cybersecurity, and cyberspace enabler workforce elements.

d. Coordinates:

(1) Changes and updates to this issuance to maintain a relevant and effective cyberspace workforce qualification program.

(2) The implementation and sustainment requirements of this issuance to include tools and resources (e.g., websites, data resources and integration) as directed by the CWMB.)

(3) The collection and analysis of qualification data for the IT, cybersecurity, and cyberspace enabler workforces to fulfill internal and external reporting requirements in accordance with DoDI 8140.02.

e. Establishes, under the authority of the CWMB, an approval process for updates to cyberspace workforce qualification standards, including the addition or deletion of approved qualifications.

2.2. USD(P&R).

In addition to the responsibilities in Paragraph 2.5., the USD(P&R):

a. Provides oversight and prescribes human resources guidance and supplemental products for implementing this issuance across DoD human resource offices.

b. Develops recommendations regarding the development and management of training and education qualification requirements to the CWMB for approval in accordance with DoDD 8140.01 and DoDI 8140.02.

c. Identifies authoritative manpower and personnel systems for the enterprise capture of data elements on DoD civilian employees and Service members, including contractors, required by Section 5 of this issuance.

d. Integrates cyberspace data elements into existing authoritative manpower and personnel systems in accordance with DoDD 8140.01, DoDI 8140.02, and this issuance.

e. Allocates resources for timely and continuous updates to personnel systems to support implementation of this issuance.

2.3. USD(I&S).

In addition to the responsibilities in Paragraph 2.5., the USD(I&S):

a. Oversees the development and management of intelligence (cyberspace) workforce element work roles.

b. Integrates the requirements of DoDD 8140.01, DoDI 8140.02, and this issuance into the management policies, procedures, and requirements of the intelligence (cyberspace) workforce element work roles.

c. Coordinates the collection and analysis of qualification data for the intelligence (cyberspace) workforce element to fulfill internal and external reporting requirements.

2.4. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND HEMISPHERIC AFFAIRS.

Under the authority, direction, and control of the Under Secretary of Defense for Policy, and in addition to the responsibilities in Paragraph 2.5., the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, in their role as the Principal Cyber Advisor:

a. Collaborates with the CJCS to:

(1) Provide recommendations to the CWMB for approval regarding the development and management of cyberspace effects work role qualification requirements in accordance with DoDD 8140.01, DoDI 8140.02, and this issuance.

(2) Integrate the requirements of DoDD 8140.01, DoDI 8140.02, and this issuance into the management policies, procedures, and requirements of the cyberspace effects workforce.

(3) Coordinate the collection and analysis of qualification data for the cyberspace effects workforce to fulfill internal and external reporting requirements.

b. Collaborates with DoD Component heads to support development of an integrated picture of the DoD cyberspace workforce.

2.5. OSD AND DOD COMPONENT HEADS.

The OSD and DoD Component heads collaborate with the DoD CIO, USD(P&R), USD(A&S), USD(R&E), USD(I&S), and the PCA to:

a. Provide recommendations to the CWMB for approval regarding the:

(1) Development and implementation of policies, procedures, and processes required to manage and guarantee compliance with DoDD 8140.01, DoDI 8140.02, and this issuance.

(2) Identification, coding, tracking, and reporting processes of their Component's DoD civilian employees and Service members and, as applicable, contractors and foreign nationals.

(3) Development of:

(a) Policies and procedures to manage DoD cyberspace workforce identification, tracking, data collection, and reporting requirements.

(b) DoD cyberspace workforce metrics to support DoD cyberspace workforce management and the requirements of DoDD 8140.01, DoDI 8140.02, and this issuance.

b. Oversee the maintenance of authoritative manpower and personnel system capabilities aligned to the DCWF in accordance with DoDD 8140.01, DoDI 8140.02, and this issuance.

c. Direct completion of component cyberspace workforce data collection and reporting requirements established in DoDI 8140.02, and Section 5 of this issuance.

d. Allocate resources for implementing and sustaining the cyberspace workforce qualification and management program as part of the Defense Planning, Programming, Budgeting, and Execution process.

e. Provide recommendations for updating or editing qualification requirements for each cyberspace work role through the CWMB in accordance with DoDD 8140.01, DoDI 8140.02, the CWMB Charter, and Paragraph 4.4 of this issuance.

f. Identify the office(s) of primary responsibility responsible within each Component that implements the DoD cyberspace workforce management and qualification program.

g. Report on implementation status information through the CWMB.

h. Upon the effective date of this issuance, incorporate the qualification requirements herein into new contract awards and modifications.

i. Plan for and incrementally complete the implementation requirements stated in Paragraph 4.3(a).

2.6. SECRETARIES OF THE MILITARY DEPARTMENTS AND THE COMMANDANT OF THE UNITED STATES COAST GUARD.

In addition to the responsibilities in Paragraph 2.5., the Secretaries of the Military Departments and the Commandant of the United States Coast Guard:

a. Provide recommendations to the CWMB for approval regarding the development and update of military training courses to provide qualification options as described in Section 3 of this issuance.

b. Require unit based reporting of cyberspace workforce readiness status in the Defense Readiness Reporting System in accordance with DoDD 7730.65.

2.7. CJCS.

In addition to the responsibilities in Paragraph 2.5., the CJCS:

a. Facilitates joint force development consistent with the overall responsibility of the CJCS to integrate cyberspace capabilities.

b. Coordinates with the DoD CIO, USD(P&R), USD(A&S), USD(R&E), USD(I&S), the PCA, and the OSD and DoD Components heads on qualification requirements for cyberspace work roles, as appropriate.

c. Collaborates with the PCA to:

(1) Provide recommendations to the CWMB for approval regarding the development and management of cyberspace effects work role qualification requirements in accordance with DoDD 8140.01, DoDI 8140.02, and this issuance.

(2) Integrate the requirements of DoDD 8140.01, DoDI 8140.02, and this issuance into the management policies, procedures, and requirements of the cyberspace effects workforce.

(3) Coordinate the collection and analysis of qualification data for the cyberspace effects workforce to fulfill internal and external reporting requirements.

2.8. COMMANDER, UNITED STATES CYBER COMMAND.

In addition to the responsibilities in Paragraph 2.5, the Commander, United States Cyber Command:

a. Coordinates with the DoD CIO, USD(P&R), USD(A&S), USD(R&E), USD(I&S), the PCA, and the OSD and DoD Components heads on qualification requirements for cyberspace work roles, as appropriate.

b. Establishes additional training and certification requirements for Cyberspace Operations Forces personnel to ensure combat readiness.

SECTION 3: CYBERSPACE WORKFORCE STRUCTURE AND QUALIFICATION PROGRAM

3.1. CYBERSPACE WORKFORCE STRUCTURE.

a. The DoD cyberspace workforce structure is based on work roles outlined in the DCWF. The DCWF includes work performed by the entire cyberspace workforce, to include 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 in accordance with DoDD 8140.01.

b. This structure includes:

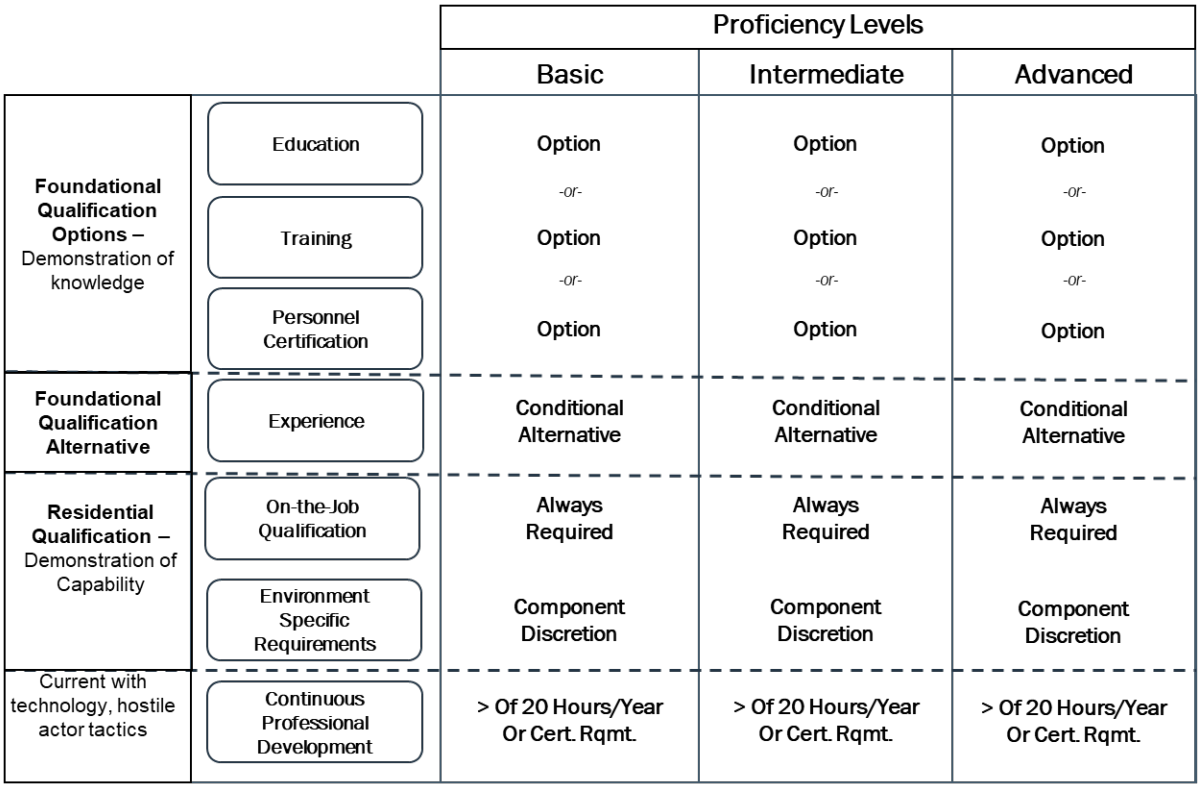
(1) DoD civilian employees and Service members assigned to positions requiring the performance of cyberspace work and coded to the DCWF with a primary and, as required, additional work role code or work role codes (up to 3 work role codes), in accordance with DoDI 8140.02.

(2) Contracted support personnel whose performance work statement requires the performance of cyberspace work. The work required should be identified by DCWF work role and proficiency level for primary and additional work roles (up to 3 work role codes) as applicable.

c. This structure differs significantly from previous workforce structures. It covers the full spectrum of cyberspace work and is based on work roles for greater specificity in identifying and qualifying the cyberspace workforce.

d. Each cyberspace work role will include an associated qualification matrix. The qualification matrix will identify the relevant options available to achieve qualification as described in this section and illustrated in Figure 1. Additional information regarding the location and management of these matrices can be found on the DoD Cyber Exchange site at: https://cyber.mil/cw/cwmp/qualifications-matrices/.

Figure 1: Sample Work Role Qualification Matrix



3.2. DOD CYBERSPACE WORKFORCE QUALIFICATION AND MANAGEMENT PROGRAM.

a. Program Overview.

(1) 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. The Program outlines qualification standards and requirements for each work role.

(a) These standards and requirements do not replace, but are used in conjunction with, OPM Qualification Standards.

(b) All training that meets the requirements of the DoD Cyberspace Operations Forces will be accepted as meeting the qualification standards and requirements of this program.

(2) 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 knowledge, skills, and abilities (KSAs) must be integrated into the qualification requirements of all cyberspace work roles regardless of workforce element alignment.

(3) Specifically, the program consists of the foundational qualification areas, residential qualification areas, and continuous professional development (CPD) outlined in Figure 1. To achieve qualification, personnel assigned to positions coded to the DCWF must meet both the foundational and resident qualification requirements outlined for each work role at the assigned proficiency levels.

(4) The program allows for options within the foundational qualification area at each proficiency level. This allows for flexibility in implementation and workforce management. To be considered, personnel must:

(a) Complete any one of the three foundational qualification options to satisfy the foundational portion of qualification.

(b) Demonstrate experience as an alternative to foundational qualification within the limits established in Paragraph 3.2.b.

(5) A component or command may dictate more stringent requirements above the options in the program.

(a) For example, a component may require two of the three foundational qualification areas be satisfied rather than just accepting one.

(b) This example or another that meets baseline standards as defined in this issuance may be applied, but the baseline standards cannot be waived.

(6) Deviations to the enterprise model shown in Figure 1, are allowed through the authority of the CWMB in accordance with the CWMB Charter.

(7) If any one area of the foundational qualification option has not been defined, or is not available for an individual work role, there will be an option between the two remaining foundational qualification areas.

(8) If qualification requirements are only available or defined for one foundational qualification area, those requirements must be satisfied to achieve qualification.

(9) When the required conditions defined in Paragraph 3.2.b. are satisfied, experience may be accepted as an alternative to the foundational qualification requirements for the scenarios described in Paragraphs 3.2.a.(7) and 3.2.a.(8).

(10) If education, training, certification, or experience requirements are defined for a specified work role, position, or occupation in regulation, statute, or other DoD policy, the optional structure of this program does not override the other requirement. The other requirement may be accepted to satisfy the foundational requirements of this issuance if they meet the standards defined in Paragraph 3.2.b.

(11) If content is undefined or does not exist for one or more foundational qualification areas for a given work role, the office of primary responsibility (OPR) as designated in

DoDD 8140.01 should evaluate and recommend qualification requirements for the undefined areas.

(12) The on-the-job qualification area of the qualification matrix must be completed to achieve qualification.

(13) CPD requirements commence upon completion of foundational and resident qualification requirements.

b. Qualification Areas.

Qualification areas establish the parameters that specific qualification requirements must meet. They provide pre-established criteria by which qualification requirements can be identified and evaluated, thereby providing consistency in the application of qualification requirements across work roles.

(1) Foundational Qualification Areas.

(a) Education.

1. At a minimum, when the education qualification area is the option chosen to meet the qualification requirements of this issuance, a secondary education diploma or equivalent (e.g., general education development) is required for all work roles at all proficiency levels.

2. Higher education and degree discipline requirements are evaluated and enacted on a role-by-role basis. When used to satisfy the foundational portion of qualification, the degree must be conferred within the past 5 years by an institution of higher education that is accredited by a nationally-recognized accreditor, unless continuous work in the relevant discipline can be demonstrated.

3. A post-secondary degree, when used to satisfy the foundational portion of qualification, must be conferred within the past 5 years by an institution of higher education that is accredited by a nationally-recognized accreditor unless continuous work in the relevant discipline can be demonstrated. In that case, the degree may have been achieved as far back as continuous work can be verified.

a. For these purposes, demonstration of continuous work should be considered documentation of employment covering any cyberspace work role with no more than 3 consecutive years lapse in cyberspace work.

b. Additionally, components should determine processes to document, review, validate, and approve continuous cyberspace work. It is recommended, but not required, that OSD and DoD Components look to the Department of Homeland Security and National Security Agency Centers of Academic Excellence when using education to meet the foundational qualification requirements.

(b) Training.

1. OSD and DoD Component cyberspace workforce training for Service members, DoD civilian employees, and contractors should be approved in accordance with relevant OSD and DoD Component training standards and should include an assessment of learning outcomes.

2. Training programs, whether one course or a defined collection of courses, must cover 70 percent of core task and KSA content of the work role appropriate for the applicable proficiency level.

3. A list of acceptable training offerings and their respective applicability to work roles and proficiency levels should be documented by OSD and DoD Components and nominated to the CWMB for inclusion in the appropriate work role qualification matrix on the DoD Cyber Exchange site at: https://cyber.mil/cw/cwmp/qualifications-matrices/.

4. All external training offerings, whether government developed or sponsored, or commercial products, require prior CWMB approval to guarantee the requirements of this section are met.

5. Approved training, when used to satisfy the foundational portion of qualification, must be completed within the past 5 years unless continuous work in the relevant discipline can be demonstrated. In that case, the training may have been completed as far back as continuous work can be verified. For these purposes, demonstration of continuous work should be considered documentation of employment covering any cyberspace work role with no more than 3 consecutive years lapse in cyberspace work.

6. The Cyber 101 course is designed as an approved training that satisfies the foundational portion of qualification for designated work roles within the cyber enabler and intelligence (cyberspace) workforce elements. Additional information can be found with the qualification matrix information for appropriate work roles at: https://cyber.mil/cw/cwmp/qualifications-matrices/.

7. All training that meets the requirements of the Cyberspace Operations Forces will be accepted as meeting the qualification standards and requirements of this issuance.

(c) Personnel Certifications.

1. Personnel certifications must be accredited to the International Organization for Standards/International Electrotechnical Commission Standard 17024 in accordance with either:

a. The National Commission for Certifying Agencies;

b. The International Organization for Standards/International Electrotechnical Commission Standard 17011; or

c. The American National Standards Institute.

2. To meet the requirements of this section, Quality Assurance of Certification Programs must adhere to Section 2015(c)(2) of Title 10, United States Code.

3. Personnel certifications must maintain relevancy through annual review and re-accreditation within 5 years in accordance with the National Commission for Certifying Agencies and International Organization for Standards/International Electrotechnical Commission 17024 timelines.

4. Personnel certifications are permitted from various sources (e.g., commercial, government, military, or academia and education) if they achieve national accreditation as described in Paragraph 3.2.

5. Personnel certification nominations will follow a process approved by and under the management of the CWMB.

a. The personnel certification will be nominated to the CWMB for alignment to a specific work role(s) and proficiency level(s). Certifications approved at a higher proficiency level also apply to lower proficiency levels within the work role.

b. If the members of the CWMB vote to proceed, the personnel certification will be forwarded for an independent third-party review to verify alignment.

c. Results will be briefed back to the CWMB.

d. A minimum of 70 percent alignment of certification content to core task and core KSA content of the applicable work role is required.

e. A formal CWMB vote is required to determine acceptance or denial as a qualification option.

(2) Alternative to Foundational Qualification Options.

The experience foundational qualification option provides a mechanism to validate and document knowledge attained through actual conduct of the tasks of a work role or work roles (i.e., experience) in a DoD environment. This option mitigates the requirement to expend additional resources on DoD employees who have already been developed to perform in their current component environment, freeing up those resources for targeted benefits such as reward or reskilling programs.

(a) Experience may be accepted in lieu of a foundational qualification option only:

1. For Federal civilian cyberspace workforce members incumbent in an IT, cybersecurity, or enabler workforce element coded position on the effective date of this issuance.

2. In the absence of qualifying education, training, or a commercial certification mapped to the work role(s) and proficiency level(s) assigned. To enable reciprocity, members who qualify through experience as an alternative to the foundational qualification options will be

able to maintain that qualification with a move in position, so long as the transition is to a position coded with the same work role and proficiency level.

3. If the workforce member is assigned to a position within the Cyberspace Operations Forces, in accordance with Paragraph 2.8 of this issuance, additional training or certification requirements may be directed by United States Cyber Command. This training shall be documented as part of residential qualification requirements in accordance with Paragraph 3.2.b.(3).

(b) Experience is only applicable as an alternative to the foundational qualification options. Further demonstration of capability through the residential qualification process will still be required to attain full qualification.

(c) Experience assessment must:

1. Be initiated through a nomination document presented by a supervisor or a senior cyberspace workforce member qualified in the subject work role. A template of the nomination document is available at https://cyber.mil/cw/cwmp/documents-library/.

2. Be evaluated at the command level by a designated evaluation team. The team should include, at minimum, two of the following personnel: cyberspace workforce program manager, information systems security manager, or a technical subject matter expert.

a. At least one member of the evaluation team must be the cyberspace workforce program manager or information systems security manager.

b. When possible, a member of the evaluation team should be qualified in the cyber work role being evaluated.

3. Leverage evaluation criteria based on work role task and KSA content, including the 70 percent core task and KSA threshold established in the foundational qualification options. Candidates must demonstrate knowledge attained through conduct of the work role.

4. Include justification for final determination (i.e. interview or documentation type) captured in the Experience Tool. The Experience Tool is available on the DoD Cyber Exchange site at: https://cyber.mil/cw/cwmp/qualifications-matrices/.

5. Final sign-off authority designated by the director or commanding officer will be documented using the DoD CIO's Specialized Cyberspace Workforce Experience certificate, available on the DoD Cyber Exchange site at: https://cyber.mil/cw/cwmp/documents-library/. This certificate must be retained in the employee's official personnel folder, and relevant cyberspace workforce tracking databases, as practicable.

(3) Resident Qualification Areas.

(a) To meet the requirements of this section, the on-the-job qualification requirements:

1. Must cover all pertinent task and KSA content of the applicable work role.

2. Include a formal period of supervised engagement for individuals, when applicable, in their designated work role and proficiency level before the individual can qualify for unsupervised work. Supervised engagement will be:

a. Direct in nature and in an organizational context at OSD and DoD Component discretion.

b. Uniform, structured, and documented.

c. At an appropriate length for the work role, proficiency level, and context.

3. Must be maintained and documented by the OSD and DoD Component.

4. May use performance-based assessments that utilize relevant, simulated environments to assess capability so long as they meet all pertinent task and KSA content.

(b) To meet the requirements of this issuance, environment-specific requirements:

1. May require training or certificates to perform a work role based on a specific operating system or environment.

2. Are at OSD and DoD Component discretion based on available tools, operating systems, and standard operating procedures.

3. Should be documented and available for reporting as required.

(4) Continuous Professional Development.

(a) To meet the requirements of this issuance, CPD:

1. Commences in the fiscal year after the employee has completed both foundational and resident qualification requirements.

2. Requires that individuals engage in a minimum of 20 hours per year of CPD or education activities to maintain and enhance competence.

a. The periodicity for reporting and completion of hours will be determined by the annual reporting cycle to be established by the CWMB in accordance with Paragraph 5.2.

b. CPD requirements remain in effect in the absence of a personnel certification, but will not excuse any continuing education requirements tied to a personnel certification.

c. Any credits achieved towards the continuing education requirement to maintain a personnel certification for the cyber work role will count towards the CPD requirement, whether or not the personnel certification meets the requirements of Paragraph 3.2.b.(1)(c).

(b) May be achieved through a variety of relevant activities including, but not limited to:

1. Completion of coursework or training;

2. Attendance at subject matter meetings, seminars, colloquia, and workshops;

3. Documented membership in professional or technical societies;

4. Cyber ranges or other related cyber exercises or virtual labs;

5. Participation in webcasts, web-based seminars, or video-link seminars;

6. OSD and DoD Component or certification body authorized mentoring activities, self-study, or e-learning;

7. Passing related professional examinations;

8. Publication of a paper, article, or book.

3.3. PROFICIENCY LEVELS.

a. The DoD Cyberspace Workforce Qualification and Management Program details qualification requirements for each DCWF work role up to three levels of proficiency. The proficiency levels:

(1) Describe the levels of a capability required to successfully perform work. This issuance does not require any connection between proficiency level and the rank or grade of the individual.

(2) Define performance expectations and include the following:

(a) Basic.

The role requires an individual to:

1. Have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance.

2. Be able to perform successfully in routine, structured situations.

(b) Intermediate.

The role requires an individual to:

1. Have extensive knowledge of basic concepts and processes and experience applying these with only periodic high-level guidance.

2. Be able to perform successfully in non-routine and sometimes complicated situations.

(c) Advanced.

The role requires an individual to:

1. Have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance.

2. Be able to provide guidance to others.

3. Be able to perform successfully in complex, unstructured situations.

b. A position may require the performance of multiple work roles at different levels of proficiency. In such cases, individuals must be qualified at the levels dictated by the requirements of the position.

SECTION 4: QUALIFICATION PROGRAM OBJECTIVES AND PROCEDURES

4.1. PROGRAM OBJECTIVES.

The Qualification Program shall:

a. Use the DCWF, along with other appropriate references, to develop a DoD cyberspace workforce with a common understanding of cyberspace concepts, principles, and applications.

b. Require that DoD personnel filling cyberspace workforce positions are qualified to perform these duties and operate in coordination with warfighters, business, and mission system owners.

c. Review and update KSAs of the DoD cyberspace workforce on a continuous basis.

d. Implement a cyberspace workforce development and sustainment process comprised of foundational (i.e., education, training, personnel certification, or experience qualification alternative); resident (i.e., on-the-job qualification and discretionary component environment specific requirements); and CPD requirements.

e. Document foundational areas to support consistency and reciprocity across the DoD. OSD and DoD Components will manage the development and implementation of qualification requirements in the resident and CPD areas outlined in Figure 1.

4.2. PROCEDURES.

a. DoD civilian employees and Service members:

(1) May temporarily perform cyberspace workforce position duties while obtaining qualification requirements under the direct observation/supervision of an appropriately qualified individual, unless the qualification requirement is waived by an OSD or DoD Component head or a delegated authority due to severe operational or personnel constraints. If such observation is not feasible, and the qualification requirement is not waived due to severe operational or personnel constraints, then the individual must be reassigned to other duties consistent with applicable law.

(2) Are considered qualified after achieving both the foundational and resident qualification requirements outlined in Section 3. DoD civilian employees and Service members must achieve:

(a) The foundational qualification requirements within 9 months of assignment to a cyberspace work role in accordance with DoDI 8140.02.

(b) The resident qualification requirements within 12 months of assignment to a cyberspace work role in accordance with DoDI 8140.02.

(3) Who are assigned to a cyberspace work role must be removed from duties associated with the work role if:

(a) They fail to achieve qualification for that cyberspace work role within stated timelines.

(b) The qualification requirements are not waived by the OSD or DoD Component head or a delegated authority.

b. Contracted support personnel must meet foundational qualification requirements upon commencement of cyberspace work in accordance with Paragraph 3.2. Contractors are not required to meet resident qualification requirements, unless the OSD or DoD Component requires it and the contract includes language to indicate this requirement and how it will be achieved.

c. OSD and DoD Component heads, or a delegated authority, may waive the qualification requirements for DoD civilian employees and Service members only under severe operational or personnel constraints.

(1) OSD and DoD Component heads:

(a) May delegate waiver authority, as appropriate, while retaining oversight of subordinate use of waiver authority.

(b) Will document, in a memorandum for the record, the justification for any granted waiver and the final plan to rectify the constraint.

(2) Waivers must include an expiration date, not to extend beyond 6 months, except in an emergency situation during a deployment to a combat environment. In this event, DoD civilian employees and Service members will make every attempt to achieve qualification without sacrifice to the mission requiring deployment. The 6-month waiver timeline will commence upon return from deployment, and the dates must be updated in all waiver documentation.

(3) Consecutive waivers for DoD civilian employees and Service members are not authorized. Waivers must be a management review item in accordance with DoDI 8500.01.

d. OSD and DoD Components must track cyberspace workforce qualifications against positions with cyberspace work role requirements in accordance with DoDI 8140.02 and this issuance.

(1) OSD and DoD civilian employees and Service members assigned to positions identified as requiring the performance of more than one cyberspace work role must achieve qualification requirements for each cyberspace work role, unless an OSD or DoD Component head or a designated authority issues a waiver.

(2) Proficiency levels may vary among cyberspace work roles.

4.3. IMPLEMENTATION.

This subsection identifies timelines for implementing this issuance across the five cyberspace workforce elements: cyberspace IT, cybersecurity, cyberspace effects, intelligence (cyberspace), and cyberspace enablers. Implementation requires in-depth planning across organizational boundaries within and across OSD and DoD Components. Standardizing skill sets will support joint assignments, reciprocity, career development, and interoperability.

a. General Requirements.

The OSD and DoD Components must:

(1) Plan for and incrementally complete these requirements:

(a) Within 2 years of the effective date of this issuance, all DoD civilian employees and Service members in cyberspace work roles under the cybersecurity workforce element must be qualified in accordance with this issuance.

(b) Within 3 years of the effective date of this issuance, all DoD civilian employees and Service members in work roles under the cyberspace IT, cyberspace effects, intelligence (cyberspace), and cyberspace enabler workforce elements must be qualified in accordance with this issuance. Thereafter, all incumbents and new hires must be trained, certified, and recertified in accordance with this issuance.

(c) OSD and DoD Components will have developed and implemented a component level program and applied a risk prioritization ensuring highest risk work roles or workforce categories are fully compliant with requirements and maintain qualification.

(d) Contractors must be qualified in accordance with this issuance at the commencement of work.

(2) Provide representation to the CWMB and Cyberspace Workforce Advisory Group as appropriate to share best practices and lessons learned from implementation activities.

b. Specific Requirements.

The DoD adopted a phased implementation timeline for this issuance to allow for accurate identification and planning of qualification requirements in accordance with DoDD 8140.01, and DoDI 8140.02.

(1) The transition to a cyberspace workforce, as indicated in this section, will include a change in reporting requirements, while enabling the DoD to meet statutory reporting requirements of DoDI 8140.02, Volumes 1-4 of DoDI 1442.02, and Public Law 113-283.

(2) Within 12 months of the effective date of this issuance, the OSD and DoD Components must:

(a) Identify all positions designated as cyberspace workforce positions in accordance with DoDI 8140.02 and Volumes 1-4 of DoDI 1442.02.

(b) Analyze all cyberspace workforce positions to ensure a proficiency level is assigned in accordance with DoDI 8140.02.

(c) Provide data on incumbent cyberspace workforce positions to the Defense Manpower Data Center (DMDC) in accordance with DoDIs 8140.02, 1336.05, 7730.54, 7730.64, and Volumes 1-4 of DoDI 1444.02. DMDC will routinely capture and format the data to support the DoD's cyberspace workforce management requirements. If an OSD and DoD Component uses an authoritative manpower and personnel system that does not exchange data with DMDC systems, the OSD and DoD Component will develop the necessary data fields to track cyberspace workforce requirements.

(d) Annually review all encumbered personnel in the personnel systems and validate their billet matches to the manpower system. Review this match annually at a minimum.

(e) Appropriately resource for cyberspace qualification requirements and workforce management requirements of DoD civilian employees and Service members. The budget plan must:

1. Implement general and specific requirements in accordance with this issuance.

2. Require authoritative manpower and personnel systems are upgraded to support cyberspace workforce management requirements as appropriate.

3. Resource training and certifying current and future members of the DoD cyberspace workforce.

4.4. GOVERNANCE.

The CWMB:

a. Is the decision body for DoD cyberspace workforce matters, as stated in its charter. As such, the CWMB designs and oversees the adjudication process for cyberspace work role and position determinations related to the program.

b. Reviews issues, identifies standards and requirements, and makes decisions, for execution and implementation by OSD and DoD Components, to guarantee the requirements of DoDD 8140.01 and DoDI 8140.02 are met.

c. Approves qualification requirements, to include DCWF requirements, for the DoD cyberspace workforce as described in Section 3.

d. Establishes and oversees the approval process for the modifications to DoD cyberspace workforce qualifications.

e. Approves updates and changes to qualification requirements for all DCWF work roles, according to the established update process for cyberspace qualification standards.

f. Coordinates with appropriate forums (e.g., Cyberspace Training Advisory Council, General Intelligence Training Advisory Committee - Cyber) on qualification matters related to training.

g. Monitors the qualification standards and requirements to provide recommendations for implementation, direct analysis, and recommends updates, as appropriate.

h. Determines cyberspace workforce qualification data collection, analysis, and reporting standards according to DoDI 8140.02 and this issuance.

i. Guarantees compliance with qualification requirements developed as described in this issuance.

4.5. COMPLIANCE.

a. Cyberspace Workforce Compliance Responsibilities.

(1) Cyberspace is a warfighting domain that requires a knowledgeable and capable cyberspace workforce to meet rapidly evolving missions. The requirements of this issuance apply to DoD civilian employees and Service members, contractors, and foreign and local nationals.

(2) This issuance implements processes and procedures necessary to standardize and improve cyberspace workforce skills to enhance mission readiness.

(3) Compliance guarantees the readiness and standardization of the civilian, military, and contractor cyberspace workforce.

b. Cyberspace Workforce Compliance Reviews.

(1) Cyberspace workforce compliance reviews are designed to capture key information regarding the implementation of this issuance. Specifically, the reviews:

(a) Monitor cyberspace workforce qualification program implementation progress.

(b) Verify cyberspace workforce qualification documentation and initiatives.

(c) Validate authoritative manpower and personnel systems' collection of appropriate workforce data.

(d) Confirm individual cyberspace workforce qualification and CPD plans are being utilized.

(e) Review cyberspace workforce training and plans and associated training budget.

(f) Confirm the cyberspace workforce data reported is valid.

(2) Cyberspace workforce compliance reviews focus on two core areas:

(a) Cyberspace workforce management.

(b) Cyberspace workforce qualification.

(3) Compliance reviews may be conducted by the following OSD and DoD Components:

(a) Inspector General of the Department of Defense.

(b) Defense Information System Agency or Command Cyber Readiness Inspection teams.

(c) United States Cyber Command-directed Command Cyber Operational Readiness Inspection teams.

SECTION 5: CYBERSPACE PERSONNEL INFORMATION MANAGEMENT

5.1. INTRODUCTION.

a. OSD and DoD Components must:

(1) Have knowledge of their cyberspace workforce position requirements; the workforce that fills these positions and their qualifications; and where these cyberspace assets are employed.

(2) Provide qualified and ready personnel when and where needed to manage the DoD cyberspace workforce effectively and efficiently.

(3) Use, to the extent possible, existing authoritative manpower and personnel systems and tools to satisfy these reporting and workforce management metrics requirements.

(4) Collect cyberspace workforce metrics at a periodicity determined by the CWMB or higher authority. The workforce metrics outlined in Paragraph 5.2 support the CWMB in current and future management of cyberspace workforce resources.

b. Cyberspace workforce metrics will be compiled in an annual report to coincide with the fiscal year.

(1) The Cyberspace Workforce Annual Report consolidates qualification and workforce management reporting requirements in accordance with DoDD 8140.01, DoDI 8140.02, this issuance, and DoDI 8510.01.

(2) The CWMB may request additional data outside of the annual report to assess program implementation or satisfy internal or external reporting requirements.

5.2. REPORTING REQUIREMENTS.

a. The CWMB coordinates the DoD Cyberspace Workforce Qualification and Management Program requirements, and guarantees that collected information supports the validation of DoD cyberspace workforce readiness. Each DoD Component must provide the DMDC with individual and position level data described in this section. This data will be used to generate the DoD Cyberspace Workforce Annual Report to support statutory and cyberspace workforce management requirements.

b. All OSD and DoD Components are required to submit data on the status of their cyberspace workforce for inclusion in the DoD Cyberspace Workforce Annual Report.

c. The CWMB will coordinate reviews of cyberspace workforce reports associated with the implementation and maintenance of the DoD qualification requirements of this issuance. In accordance with DoDD 8140.01:

(1) The DoD CIO will serve as the OPR on IT, cybersecurity, and cyberspace enabler workforce element qualification data.

(2) The PCA will serve as the OPR for cyberspace effects workforce element qualification data.

(3) The USD(I&S) will serve as the OPR for work roles and associated qualification standards for the intelligence elements of the cyberspace enabler workforce.

d. To support DoD cyberspace workforce reporting requirements, the CWMB will combine metrics from the OSD and DoD Components to assemble a consolidated DoD Cyberspace Workforce Annual Report and status. The report will include OSD and DoD Component comments regarding cyberspace workforce lessons learned, issues from the previous calendar year, and plans for the next calendar year. The report will also provide statistics for personnel performing cyberspace functions as a primary or additional duty, broken down by cyberspace work role and proficiency level.

e. Each OSD and DoD Component must guarantee that its authoritative manpower and personnel systems are properly configured, in accordance with DoDIs 7730.54, 8510.01, and Volume 1 of DoDI 1444.02, to capture the data in Paragraph 5.2.g. of this issuance. To implement DoDD 8140.01, DoDI 8140.02, and meet statutory reporting requirements, DoD Components are required to provide excerpts of the data elements in Paragraph 5.2.g. from authoritative manpower and personnel systems. These can be shared in a manual fashion (i.e., the sending of physical spreadsheets) or via automated interface.

f. DoD Components will provide updates no less frequently than annually to assist the DoD in managing the health, welfare, and maturity of the cyberspace workforce.

g. The required data elements for manpower data and personnel data should correspond to individual positions:

(1) Manpower (Position or Billet) Data.

Information about the cyberspace workforce position or billet.

(a) Position or Billet Identification Number or Unique ID.

(b) DCWF Work Role Code-Primary and associated proficiency level.

(c) DCWF Work Role Code-Additional 1 and associated proficiency level.

(d) DCWF Work Role Code-Additional 2 and associated proficiency level.

(e) Position requires designation as an IT Privileged User - Yes or No.

(f) Organization that reserves position or billet.

(2) Personnel Data.

Information about the person performing cyber work in the specified position or billet.

(a) Organization that employs person filling position or billet.

(b) Unique personnel identifier (e.g. EDI/PI).

(c) Position or Billet Identification Number or Unique ID of position held.

(d) DCWF Work Role Code and proficiency level of Position or Billet Held- Primary.

(e) DCWF Work Role Code and proficiency level of Position Held- Additional 1.

(f) DCWF Work Role Code and proficiency level of Position Held- Additional 2.

(g) IT Privileged User Designation Requirement Met- Yes or No.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CJCS	Chairman of the Joints Chiefs of Staff
CPD	continuous professional development
CWMB	Cyberspace Workforce Management Board
DCWF	DoD Cyberspace Workforce Framework
DMDC	Defense Manpower Data Center
DoD CIO	Department of Defense Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
IT	information technology
KSA	knowledge, skills, and abilities
OPM	Office of Personnel Management
OPR	office of primary responsibility
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
certification	Defined in the August 13, 2008 OPM Memorandum.
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.

cybersecurity workforce	Defined in DoDD 8140.01.
cybersecurity	Defined in Committee on National Security Systems Instruction No. 4009.
cyberspace effects	Defined in DoDD 8140.01.
cyberspace enabler	Defined in DoDD 8140.01.
cyberspace workforce	Defined in DoDD 8140.01.
cyberspace	Defined in the DoD Dictionary of Military and Associated Terms.
CWMB	Defined in DoDD 8140.01.
Defense Readiness Reporting System	Defined in DoDD 7730.65.
DoD Cyberspace Workforce Annual Report	Consolidates qualification and workforce management reporting requirements in accordance with DoDD 8140.01, DoDI 8140.02, this issuance, Section 301 note of Title 5, United States Code (also known and referred to as "the Federal Cybersecurity Workforce Assessment Act of 2015"), and DoDI 8510.01.
DCWF	Defined in DoDD 8140.01.
Federal Wage System Qualifications	Defined in https://www.opm.gov/
General Schedule Qualification Standards	Defined at https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/
information system	Defined in Committee on National Security Systems Instruction No. 4009.
intelligence workforce (cyberspace)	Defined in DoDD 8140.01.
IT	Defined in the DoD Dictionary of Military and Associated Terms and Committee on National Security Systems Instruction No. 4009.
IT workforce	Defined in DoDD 8140.01.
readiness and standardization	The qualification baseline that all cyberspace workforce members will attain, according to their assigned work role.

The American National Standards Institute	Defined at https://www.ansi.org/

REFERENCES

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 2015

DoD Cyberspace Workforce Management Board Charter, current edition[1]

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 7730.65, "Department of Defense Readiness Reporting System (DRRS)," May 11, 2015, as amended

DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020

DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010, as amended

DoD Instruction 1336.05, "Automated Extract of Active Duty Military Personnel Records," July 28, 2009, as amended

DoD Instruction 1442.02, "Personnel Actions Involving Civilian Attorneys," September 30, 2010

DoD Instruction 1444.02, Volume 1, "Data Submission Requirements for DoD Civilian Personnel: Appropriated Fund (APF) Civilians," November 5, 2013, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended

DoD Instruction 7730.54, "Reserve Components Common Personnel Data System (RCCPDS)," May 20, 2011

DoD Instruction 7730.64, "Automated Extracts of Manpower and Unit Organizational Element Files," December 11, 2004

DoD Instruction 8140.02, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements," December 21, 2021

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program" April 3, 2017, as amended

DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended

International Organization for Standards/International Electrotechnical Commission Standard 17011, 2017

International Organization for Standards/International Electrotechnical Commission Standard 17024, 2004

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Office of Personnel Management, "General Schedule Qualification Standards," current edition

[1] Available on the DoD Cyber Exchange at https://cyber.mil/cw/cwmp/documents-library/.

Office of Personnel Management Memorandum, "Fact Sheet on Certification and Certificate Programs," August 13, 2008
Public Law 113-283, "Federal Information Security Modernization Act of 2014," December 18, 2014
United States Code, Title 5, Section 301 Note (also known and referred to as "the Federal Cybersecurity Workforce Assessment Act of 2015")
United States Code, Title 10

RETURN TO TABLE OF CONTENTS

Appendix B – Security Clearance Disclosure Form

VICEROY Scholar Security Clearance Awareness & Disclosure Form

Purpose of This Form

1. Inform students about the key eligibility requirements for obtaining a U.S. Government security clearance

2. Disclose common disqualifying factors

3. Alert students that failure to obtain a clearance can significantly limit their ability to participate in internships, research roles, or employment opportunities tied to national security.

4. Encourage self-assessment and proactive engagement, so students understand their status and can raise concerns or questions early in the process.

Security Clearance Eligibility – Key Requirements

1. **U.S. Citizenship is Generally Required**
   Most national security roles require that the applicant be a U.S. citizen. Dual citizens or those with recent or strong ties to foreign nations may face additional scrutiny. Non-U.S. citizens are generally not eligible for clearances unless granted a specific exception by the federal government.

2. **Background Investigation Must Be Passed**
   A formal investigation, typically conducted by the Defense Counterintelligence and Security Agency (DCSA), is required. This process may include interviews with the applicant and people in their personal and professional network, as well as a review of documents, records, and history.

   As part of the investigation, the government evaluates key areas to determine if an individual is trustworthy, reliable, and not susceptible to coercion or undue influence. These evaluations include:
   - **Financial responsibility:** High debt, recent bankruptcies, or unpaid taxes may be seen as vulnerabilities.
   - **Criminal history:** Felonies, certain misdemeanors, or patterns of criminal behavior can negatively impact eligibility.
   - **Foreign influence and contacts:** Extensive ties to foreign individuals, entities, or governments are carefully evaluated to prevent conflicts of interest or divided loyalties.

3. **No Conflicting Allegiance to Foreign Governments**
   Applicants must demonstrate undivided loyalty to the United States. Holding foreign citizenship, serving in a foreign military, or accepting benefits from foreign governments may disqualify someone from clearance eligibility. Renouncing foreign allegiances may be necessary in some cases.

Potential Disqualifying Factors

1. **Non-U.S. Citizenship**
   Most security clearances require applicants to be U.S. citizens. Non-citizens or those with dual

citizenship may be disqualified due to concerns about loyalty, access to sensitive information, and foreign influence.

2. **Drug Use or Substance Abuse**
   While a history of drug use or substance abuse can indicate potential vulnerabilities — particularly if there are concerns about an applicant being coerced or influenced under the influence of drugs or alcohol — it is important to note that past drug use does not automatically disqualify someone from receiving a clearance. The federal government evaluates patterns of behavior, such as:

   - Recent drug use or addiction
   - Failure to comply with drug testing requirements
   - History of substance abuse, with severity and recency being important factors

   Applicants who acknowledge their past drug use, demonstrate personal growth, and show a commitment to a drug-free future have successfully obtained clearances. Full disclosure is critical, but prior mistakes do not necessarily end one's eligibility.

3. **Significant Financial Issues**
   Financial irresponsibility or instability raises concerns about an applicant's reliability and trustworthiness. Key financial issues that may disqualify an applicant include:
   a. High levels of unresolved debt (e.g., credit card debt, personal loans, unpaid taxes)
   b. Recent bankruptcy or foreclosure
   c. Failure to meet financial obligations (e.g., alimony, child support)
   d. Any financial issues that indicate a lack of judgment or a potential vulnerability to bribery or coercion may be heavily scrutinized.

4. **Criminal History**
   A criminal record, particularly one involving felonies, serious misdemeanors, or repeated violations, may be a significant barrier to obtaining a clearance. The clearance review typically considers:
   a. Type and severity of the offense (violent crimes, fraud, theft, etc.)
   b. Time elapsed since the offense (recent violations are considered more problematic)
   c. Demonstration of rehabilitation or steps taken to address criminal behavior
   d. Applicants may also face disqualification if they have any pending charges or a pattern of criminal behavior.

5. **Foreign Influence**
   Foreign influence or connections can raise questions about an applicant's ability to protect U.S. interests. This includes having significant family, financial, or personal ties to foreign governments, organizations, or individuals. Potential issues include:
   a. Close foreign family members (e.g., spouse, children, parents) who live abroad or have foreign citizenship
   b. Owning property, assets, or businesses in foreign countries
   c. Ongoing relationships with foreign nationals or entities that might create a conflict of interest or expose the applicant to foreign influence.

6. **Dishonest Conduct**
   Dishonesty, including falsification of documents, misrepresentation of facts, or lack of candor in interviews or disclosures, can result in immediate disqualification. Key behaviors include:
   a. Lying on security clearance applications or during the interview process
   b. Providing misleading or incomplete information about personal history, finances, or criminal activity
   c. Any form of deceitful conduct that undermines trust and integrity may disqualify an applicant from a clearance.

7. **Past Security Violations**
   If an individual has previously violated security protocols or failed to protect classified or sensitive information, this is a strong disqualifying factor. Examples of past security violations include:
   a. Unauthorized disclosure of classified information
   b. Mishandling of classified documents or failing to properly safeguard them
   c. Violating internal security policies (e.g., misuse of technology, unapproved communications with foreign entities)
   d. A history of security violations may indicate a lack of respect for confidentiality and national security standards, thus raising concerns about future behavior.

Student Acknowledgment

- ○ I understand most DoD/DIB roles require a U.S. security clearance.
- ○ I understand the clearance criteria and disqualifying factors.
- ○ I understand that failure to obtain a clearance will limit my eligibility for certain positions, internships, and sponsored opportunities.

Certification

I certify that I have read and understood this information. I understand that I may be excluded from clearance-required opportunities based on my background or citizenship.

Full Name: _____

Signature: _____

Date: _____

Appendix: Security Clearance Resources and Process Overview

For more information about the U.S. Government security clearance process, visit:

- DCSA Clearance Process Overview: https://www.dcsa.mil/mc/pv/mbi/gicp/

- Adjudicative Guidelines:
  - https://clearedjobs.net/security-clearance-faqs
  - https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf
  - https://www.secnav.navy.mil/dusnp/Security%20Documents/Supv_Role_in_PerSecDec2010.pdf

RETURN TO TABLE OF CONTENTS