

Program Authorization: Officer Development School (ODS) indoctrination and training of college graduates for appointment on active duty as a Special Duty Officer (Cyber Warfare Engineer (CWE)). BUPERS-317C is the community manager. The term “1840 Senior Officer” as referenced in this document is defined as the highest-ranking Active Component CWE Officer with designator 1840.

1. Program Authority: Title 10 U.S. Code section 532.
2. Cancellation: Program Authorization 121 of April 2019.
3. Quotas: As prescribed by the Deputy Chief of Naval Operations (Manpower, Personnel, Training and Education) (DCNO N1).
4. Qualifications
  - a. Citizenship: Applicants must be United States citizens.
  - b. Gender: No restrictions.
  - c. Age: Applicants must be at least 18 years old and less than 42 years old at the time of commissioning. Waivers will be considered for exceptionally qualified applicants between ages 42 and 54. Waivers will not be considered for applicants beyond age 54.
  - d. Education
    - (1) Minimum of a baccalaureate degree from an accredited institution, with a major field of study directly related to science, technology, engineering, or mathematics.
    - (2) Degrees in computer science and computer engineering are strongly preferred. Other technical majors will be considered on a case-by-case basis, which include but are not limited to: cyber operations, mathematics, information systems, software engineering, and other computer-related disciplines.
    - (3) All applicants must have substantial software development and/or computer programming coursework reflected in their college transcripts (minimum of 30 credit hours), with a minimum 3.0 grade point average preferred, but not required, in those areas.
  - e. Physical: Applicants must meet physical standards for appointment as prescribed in the Manual of the Medical Department, Chapter 15.
  - f. Duty Preference: Not applicable.
  - g. Marital Status: No restrictions.
  - h. Program Specific Requirements:

(1) Technical Skills and Abilities

(a) Substantial, demonstrated technical ability in one or more key skill areas is required, which include: reverse engineering, vulnerability analysis, red team / blue team tool development, low-level systems programming, computer forensics and exploit development. Additional consideration will be given to software engineering and computer programming expertise that includes languages, technologies, and projects relevant to cybersecurity and computer network operations. Best qualified candidates will demonstrate significant proficiency in the C programming language.

(b) Consideration will be given to substantial, demonstrated technical ability in network security, penetration testing, systems administration, artificial intelligence and machine learning. However, these skills alone do NOT constitute a sufficient basis for selection, and are NOT considered a substitute for the required technical skills as outlined in the paragraph above.

(2) Application Process

(a) In-service ODS applicants should submit an Officer package through their chain of command, while civilian ODS applicants should submit an Officer package through their recruiters. CWE/1840 must be listed as a desired community and designator. All applicants shall verify they are eligible prior to submitting a package. Upon submission, packages are received by Commander, Navy Recruiting Command (CNRC) and provided to the CWE officer community manager (OCM).

(b) The CWE OCM will conduct a professional review of all received Officer packages to ensure they are eligible and qualified for commissioning and meet basic CWE community and security requirements. Packages for qualified applicants are forwarded to the 1840 Senior Officer. Applicants whose packages do not meet standards for commissioning will be designated as non-selects. The CWE OCM will make reports of non-selects back to CNRC.

(c) The 1840 Senior Officer, or their designated representative, will conduct a technical review of all received Officer packages, which may require contact with the applicant. Applicants whose packages do not demonstrate the requisite technical skills will be designated as non-selects. The CWE OCM will make reports of non-selects back to CNRC.

(d) Applicants whose packages pass both the professional and technical review will be recommended for a skill validation and technical interview with the 1840 Senior Officer or their designated representative. If the applicant passes the skill validation and technical interview, the 1840 Senior Officer will recommend them, in writing, to the CWE OCM for selection. If the applicant does NOT pass the interview, they will be returned to the CWE OCM as non-selects. The CWE OCM will make reports of non-selects back to CNRC. Applicants who are designated non-selects upon conclusion of the interview are eligible, at the discretion of the 1840 Senior Officer, to be re-interviewed in the future for further consideration. The skill validation and technical interview cannot be waived.

(3) **Security Clearance Eligibility:** Candidates must meet the Director of National Intelligence, Intelligence Community Directive (ICD) 704 eligibility standards for access to sensitive compartmented information. Security eligibility cannot be waived.

(a) All applicants (both military and civilian) must submit a copy of a standard form-86 completed within the last two years as part of their application.

(b) Applicants who are recommended for a commission into the Active Component are required to complete an initial suitability screening with the Fleet cyber command security directorate prior to final selection as an officer candidate and will be submitted for a Top Secret clearance prior to shipping to ODS. There is no waiver for successfully completing this suitability screening.

(c) Being a dual citizen (i.e., a U.S. citizen and a citizen of another country) is not necessarily immediately disqualifying, depending on country of dual citizenship. Associated risks to national security will be determined on a case-by-case basis. Applicant is advised to refer to ICD 704 and to discuss this during their initial suitability screening with the Fleet cyber command security directorate.

5. **Waivers.** In cases where the applicant does not meet all of the qualifications referenced in section 4 above, but otherwise has an exceptional record or proven skillset, a waiver may be authorized in limited numbers. Waiver to age is specifically addressed in section 4.c above. The screening process and security clearance eligibility discussed in section 4.h are not waiverable. If a waiver is requested then follow the steps below prior to the convening of the selection board.

a. **Application Contents:** Letter with formal request from applicant on desired waiver(s).

b. **Routing:** Waiver requests routed from recruiter to CNRC, then to the CWE OCM for a recommendation concerning the waiver. Once a recommendation is received, CNRC will continue routing.

c. **Approval Authority:** CNRC.

d. **Notifying the Applicant:** CNRC will notify the applicant of waiver status.

6. **Accession Source**

a. **Civilians.**

b. Enlisted personnel of the regular Navy or Navy Reserve (active and inactive) or enlisted personnel of other armed services provided a conditional release is authorized. There is no time in service restriction for qualified applicants.

7. **Indoctrination:** Civilian and enlisted selectees will complete ODS at Officer Training Command, Newport, RI.

8. Enlistment: Not applicable.

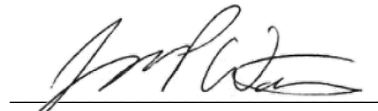
9. Constructive Entry Credit: For candidates with relevant prior military service and/or civilian work experience as outlined in enclosure (1), the 1840 Senior Officer will chair a professional review board to evaluate the candidate's record/resume and determine eligibility for constructive entry credit. Recommendations by the professional review board for accessions at a paygrade greater than Ensign/O-1 will be forwarded by the 1840 Senior Officer to the CWE OCM in writing for review and final approval.

10. Appointment: ODS candidates will be commissioned in the U.S. Navy as an Ensign 1840, or at the grade level as recommended by the 1840 Senior Officer, addressed in section 9 above, and approved by the CWE OCM.

11. Service Obligation: Selectees incur a five year active-duty obligation from date of commission. The obligation is concurrent with outstanding service obligation requirements. The obligation commences upon commissioning. The balance of service, sufficient to complete eight years total obligated service, may be served in a Ready Reserve status.

12. Pay and Allowances: Selectees are commissioned prior to attending ODS and not entitled to pay and allowances prior to commissioning.

Approved:

  
\_\_\_\_\_  
J.P. WATERS  
Rear Admiral, U.S. Navy  
Director, Military Personnel Plans  
and Policy (OPNAV N13)

Date: 9 May 22

CONSTRUCTIVE ENTRY CREDIT CRITERIA

| <b>Constructive Entry Credit Criteria for Cyber Warfare Engineer:</b>  | <b>Credit Allowable:</b>  | <b>Credited:</b> |
|--|---------------------------|------------------|
| 1. Commissioned service on active duty in an active status as an 1840.   | One year for each year.   |                  |
| 2. Computer Network Operations Development Program (CNODP) graduate.   | One year for each year.   |                  |
| 3. CNODP participant. Shall not be used in conjunction with CNODP graduate.  | One month for each month. |                  |
| <p>4. Demonstrated technical and professional experience in the following areas: vulnerability research, penetration testing, incident response, computer forensics, RF engineering, red teaming / blue teaming, exploit development, Computer Network Exploitation (CNE) focused tool development (e.g. proficiency in low-level programming languages such as C, C++, x86 assembly; proficiency in operating systems concepts such as memory management, concurrency, user-mode and kernel-mode development; mastery of security concepts such as remote code execution, shellcode development, stack and heap buffer overflows) and hardware engineering (e.g. system design, basic FPGA design and test, computer architectures, PCB design and fabrication). Enlisted experience that meets the aforementioned criteria may be considered for this credit.</p> <p>--- Applies operational and technical expertise and executes computer network exploitation, attack and defense tactics, techniques and procedures. Analyzes, plans, directs, and conducts computer network exploitation and attack. Analyzes threats, intrusions and attacks against networks. Plans and executes computer network defense response actions.</p> <p>--- Applies principles and techniques of computer science and computer engineering to research, design, develop, test, and evaluate software and firmware for computer network attack, exploitation and defense in cyberspace operations.</p> | One year for each year.   |                  |
| Sum of Credited Years of Service:  |                           |                  |
| <b>Limits and Computation of Entry Grade Credit. Entry grade credit shall be computed as follows:</b>  |                           |                  |
| A period of time of special qualification shall be counted only once.  |                           |                  |
| Qualifying period of less than one full year shall be credited proportionately to the nearest day except where noted otherwise.  |                           |                  |

|  |  |  |
|--|--|--|
| <p>Maximum entry Grade Credit. Total entry grade credit granted shall normally be limited to 15 years. After considering the recommendations of DCNO (N1), Assistant Secretary of the Navy (Manpower and Reserve Affairs) may waive the 15-year limit on a case by case basis.</p> |  |  |
|--|--|--|