Current Core Skill Requirements
Cyber Systems and Operations (CSO)
Subspecialty 6208
Curriculum# 326

Billet subspecialty coding is to be based on the minimum education/training/ experience level required for optimum performance. The following is a representative sampling of duty requirements for which this subspecialty applies:

(1) Develop, operate, manage, maintain or assess network systems and architectures at multiple security levels. Recommend and implement solutions to network problems.

(2) Make recommendations concerning military application of future cyber capabilities to enhance operations. Determine requirements from local to enterprise level, particularly with respect to integration with tactical systems and cloud computing.

(3) Assess the interoperability of hardware and software and manage acquisition processes for future network capabilities.

(4) Operate and exploit electrical and computer systems that comprise the backbone of the cyber system, and integrate advanced communication programs into military systems.

(5) Plan and implement proactive and reactive electronic warfare actions supporting the overall mission.

(6) Search for, locate, identify, penetrate, characterize, and collect intelligence from targets in cyberspace for analysis, threat recognition, planning, fusion with other sources, targeting, and conduct of future operations, and other measures short of attack, to prepare potential targets for future operations.

(7) Devise and employ measures to preserve and protect friendly/DOD cyberspace capabilities, networks and net-centric capabilities. Plan and carry out actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation.

(8) Devise and employ offensive cyber capabilities, and integrate non-kinetic with kinetic fires for optimum effect.

(9) Integrate space resources into operational planning, communications, ISR, and information operations at the operational and tactical levels. Identify vulnerabilities in the space-borne asset architecture and execute mitigating or alternative actions.

(10) Develop and input cyber-relevant requirements into research, development, and acquisition processes for space systems or unmanned/autonomous systems.

(11) Integrate unmanned/autonomous cyber resources into operational planning, for improved execution of command and control, communications, ISR, and weapon delivery.

(12) Conduct strategic, operational and tactical planning across the full range of cyberspace operations, to include Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), and DOD Global Information Grid Operations (DGO) and integration of UV/AS; integrate cyber planning into overall mission planning as part of an OPLAN/CONPLAN under both Navy and Joint commands. Provide recommendations for cyber authorities, policies, and organizational responsibilities.

(13) Employ and manipulate data management tools and processes to enable operational effectiveness.

(14) Ensure useful data is collected, processed, stored, protected, organized, made accessible, and merged with related data sources to deliver relevant information to decision makers at all levels of command.

(15) Identify requirements and solutions for improved Human Machine Interface and operational efficacy of information and decision-enabling systems and tools.

(16) Employ cyber systems to enable the commander to make operational decisions and direct forces with the utmost speed, accuracy and efficiency, such that adversaries cannot disrupt friendly actions or respond appropriately or effectively.
Cyber Systems and Operations/6208 subspecialty coding is justified when, in addition to the general criteria stated in NAVPERS 15839 series (Manual of Navy Officer Manpower and Personnel Classification) Part B, the following specific criteria are satisfied:

1. <u>Subspecialty Coding Restrictions</u>:

a. Billets assigned to: Surface Warfare, Submarine Warfare, Special Warfare, Aviation Warfare, Oceanography, Information Warfare, Information Professional, Intelligence.

2. <u>Applicable Officer Designator(s)</u>: 111X/112X/131X/132X/180X/181X/182X/183X/184X/644X/645X/743X

3. <u>Applicable Billet Designator(s)</u>: 1000-1120/1310-1322/1800-1830/1840/6640/6450/7430

4. <u>Significant Experience Criteria</u>

a. Cyber Systems and Operations/6208 S-coded <u>billets</u> are authorized when two of the following conditions are met:

(1) The duties require detailed knowledge of, or experience in, specific cyber systems, processes, management or leadership.

(2) Appropriate training on specific cyber systems, processes, or management is available and accessible to qualified Officers prior to assignment to the billets.

(3) Specific community career track requirements/milestones include distinct follow-on billets requiring cyber expertise.

b. Cyber systems and Operations/6208 S-coded Officers are authorized when:

(1) The Officer has filled a B, S, R, P, or Q coded billet for more than 18 months and has no subspecialty code in the field.

(2) FITREP justifies that s/he has accomplished the task(s) associated with the billets above for more than 18 months.

(3) Discrete incremental training received has provided the set of required skills associated with the billets above.

c. Cyber Systems and Operations/6208 R-coded billets are authorized when, in addition to the requirement for S-coded billets, the billet must be filled by Officers having filled a previous 6208-coded billet. A requirement for familiarity or experience in the specific duties, as through service in a previous billet, should characterize these billets.

d. Cyber Systems and Operations/6208 R-coded Officers are authorized when:

(1) The Officer has filled one B, S, R, P, Q coded billet for more than 18 months and has an S subspecialty code.

(2) Two FITREPs justify that s/he has accomplished the task(s) indicated above for more than 18 months.

5. Baccalaureate Criteria

a. Cyber Systems and Operations/6208 E-coded billets are authorized but limited to billets coded for O1-O3, where a strong background in cyber is warranted but generally not available through graduate education or experience.

b. Cyber Systems and Operations/6208 E-coded Officers are authorized when they have received a baccalaureate degree in one of the following areas:

(1) Cyber Systems or Cyber Security

(2) Computer Science or Computer Engineering

(3) Information systems or Network Engineering

(4) Other degrees with strong correlation to the 6208 ESR, by petition.

6. Elective Level Criteria

a. Cyber Systems and Operations/6208 H-coded billets are authorized for:

(1) Billets requiring expertise in Cyber where a master's level of knowledge is desirable but not essential for optimum performance.

7. Functional Education Criteria

a. Cyber Systems and Operations/6208 G-coded Officers are authorized when:

(1) An Officer has not completed all required ESRs (e.g., not completed a thesis or capstone/practicum at NPS).

(2) An Officer attends a civilian institution and completes two thirds or greater of the ESRs.

b. Cyber Systems and Operations/6208 F-coded Officers are authorized when:

(1) An Officer has a G code and has done a tour in a master's degree billet or higher.

8. Master's Criteria

a. Cyber Systems and Operations/6208 P-coded billets are authorized when the billet requires performance at least three of the sixteen above-listed duty requirements.

b. Cyber Systems and Operations/6208 P-coded Officers are authorized when:

(1) The Officer completes the Cyber Systems and Operations master's degree at NPS. Full subspecialty will not be given if a thesis or capstone/practicum is not completed. Officers graduating without meeting this requirement will instead receive the F subspecialty code. Utilization and obligations are still required.

(2) The Officer completes a master's degree at an accredited institution of higher learning that satisfies all 6208 ESRs.

c. Cyber Systems and Operations/6208 Q-coded billets are authorized when the billet requires:

(1) All requirements of the P code and detailed knowledge of, or experience in, specific cyber systems, processes, management, or leadership.

d. Cyber Systems and Operations/6208 Q-coded Officers are authorized when:

(1) The Officer completes the Cyber Systems and Operations/6208 ESR, either at NPS or another accredited institution, and having done at least 18 months in a master's degree coded billet or higher. The Officer must have a P-code prior to a Q-coded tour.

(2) F coded Officers cannot obtain Q codes. They will be authorized G codes.

9. Post Masters

a. Cyber Systems and Operations/6208 N-coded billets are not authorized.

b. Cyber Systems and Operations/6208 N-coded Officers are not authorized.

c. Cyber Systems and Operations/6208 M-coded billets are not authorized.

d. Cyber Systems and Operations/6208 M-coded Officers are not authorized.

10. Doctorate Criteria

a. Cyber Systems and Operations/6208 D-coded billets are authorized when the billet requires:

(1) Detailed knowledge beyond that attainable through master's degree or other pre-doctoral programs.

(2) Research.

b. Cyber Systems and Operations/6208 D-coded Officers are authorized when:

(1) They complete the Cyber Systems and Operations PhD program.

(2) They complete a PhD program at another accredited institution of higher learning that meets the 6208 ESRs.

c. Cyber Systems and Operations/6208 C-coded billets are authorized when the billet requires:

(1) Supervision of research or instruction as part of a master's degree program or higher.

d. Cyber Systems and Operations/6208 C-coded Officers are authorized when:

(2) The Officer holds a 6208D code and has done at least 18-months in a D-coded billet.

11. Major Area Sponsor and Subject Matter Experts:

- Major Area Sponsor POC: LCDR William Nesbitt, OPNAV N2/N6C1, 703-604-6293.
- Subject Matter Expert POC: Mr. Joseph Sullivan, Navy Information Dominance Forces, 757-471-6722.

APPROVED: Jan E Tighe
FCC/C10F (Curriculum Sponsor)
18 JUN15
Date

APPROVED:
OPNAV N2/N6 (MAS)
13 JUL 2015
Date

APPROVED:
OPNAV N12 (TFMTERD)
22 FEB 2016
Date