PROPOSED 2018-20 CORE SKILL REQUIREMENTS
Network Operations and Technology
Subspecialty: 6209
Curriculum: 386

Billet subspecialty coding is to be based on the minimum education/training/experience level required for optimum performance. Network Operations and Technology/6209 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. Description of (Core Skill Requirements) CSR Competencies. The listed CSRs are a set of quantifiable skills, traits and experiences that a subspecialist must possess to perform acceptably in a coded billet for Network Operations and Technology/6209.

a. CSR-1: Operate the network as an agile warfighting system. Develop, operate, defend, manage, maintain, or assess network systems and architectures at multiple security levels, to include the application of authorized cross-domain solutions to allow safe and effective portability of data between those security levels. Recommend and implement solutions to network problems relevant to military operations.

b. CSR-2: Make recommendations concerning military application of future information warfare capabilities to enhance operations and enhance efficiency of operational support functions. This includes making recommendations on tools and processes for predictive analysis of threats to the networks based on indications and warning to preemptively pace or achieve advantage over adversary actions. Determine requirements from local to enterprise level.

c. CSR-3: Assess the interoperability of hardware and software, and data to support acquisition processes and the economics of future network capabilities, and integration of new capabilities with legacy infrastructure. Develop systems engineering principles to ensure optimal integration and operation of systems of systems

d. CSR-4: Integrate advanced Information Warfare policy, protocol and procedures into military systems.

e. CSR-5: Devise and employ cybersecurity measures to preserve and protect friendly warfighting, networks and capabilities, to include Command and Control (C2) and information, control, combat, and navigation systems. Recommend tools, processes, and policies that will help preemptively identify potential threats and counter them. Plan and carry out actions that protect and defend warfighting systems by ensuring confidentiality, integrity, and availability.

f. CSR-6: Optimize C2 system configurations to assure lethality in the operational environment, and codify and execute pre-planned responses to enable continued operations in a contested environment. Recommend tools, processes, and procedures that proactively identify potential threats to warfighting systems so action can be taken prior to adversary action to degrade or deny efficacy of capabilities.

g. CSR-7: Integrate Space capabilities into operational planning, communications, Intelligence, Surveillance, and Reconnaissance (ISR), and information operations at the operational and tactical levels of war. Identify vulnerabilities and understand adversary threat capabilities in space-based architectures and execute mitigating or alternative actions.

h. CSR-8: Develop and input information warfare requirements into research, development, acquisition, and operations processes for space systems or unmanned/autonomous systems (UV/AS).

i. CSR-9: Integrate unmanned/autonomous (UV/AS) information warfare resources into operational planning, for improved execution of C2, communications, ISR, and weapon delivery. Identify friendly and adversary vulnerabilities in the unmanned/autonomous vehicle asset architecture and execute mitigating or alternative actions.

j. CSR-10: Conduct strategic, operational and tactical planning for Defensive Cyberspace Operations (DCO), DOD information networks (DODIN) operations, and Space operations. Integrate courses of action into overall mission planning as part of Joint campaign plans. Provide recommendations for innovative naval use of capabilities, authorities, policies, and organizational responsibilities.

k. CSR-11: Employ data management and analysis strategies and advanced data science methods to enable operational effectiveness and decision-making processes. Ensure useful data are collected, processed, stored, protected, organized, and made accessible to deliver information to decision makers, at the speed of relevance, at all levels of command.

l. CSR-12: Employ and optimize Electromagnetic Maneuver Warfare to include spectrum management, counter-ISR, frequency planning and allocation, and threat mitigation frameworks against adversary action.

m. CSR-13: Employ information warfare 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. Leverage artificial intelligence, machine learning, data science, cloud, and automation technologies to enhance decision making.

n. CSR-14: Enable standardized exchange of information between tactical units and higher echelons to deliver collective battlespace awareness and a synchronized, tailorable common operational picture.

2. Applicable Officer Designator(s)

a. 111X/112X/113X/12XX/131X/132X/15XX/18XX/23XX/31XX/51XX

3. Applicable Billet Designator

a. 1000-1130/1200/1310-1322/1500/1800-1850/2300/3100/5100

4. Educational and Significant Experience Criteria.

a. Coded billets are authorized when the functions of the billet include the CSR competencies listed above (in paragraph 1). For additional clarification regarding definition of suffixes, refer to the NAVPERS 15839I, Vol 1. (Note: 'Proven' requires at least 18-month experience tour in subspecialty coded billet or billet using the CSR of a related subspecialty.)

b. Subspecialty Code Suffixes Authorized. Authorized suffixes should be annotated "X" for yes; unauthorized suffixes should be left blank. If any additional clarification is required for the code, annotate 1, 2, etc., in the notes column and add a Note below the table.

Subspecialty Code Suffixes Authorized				
Billet	**Officer**	**Suffix**	**Definition**	**Notes**
		C	Proven Doctor of Philosophy	
		D	Doctor of Philosophy	
	X	F	Proven Master's Degree that does not meet all ESRs	1
	X	G	Master's Degree that does not meet all ESRs	2
X		H	Master's Degree desired, not required	3
		L	Certificate degree at the Master's level	
		M	Proven Post Master's Degree graduate education	
		N	Post Master's Degree graduate education	
X	X	P	Master's Degree in approved Navy subspecialty	4
X	X	Q	Proven Master's Degree	5
X	X	R	Proven Significant Experience	6
X	X	S	Significant Experience obtained through OJT	7

Note 1:

a. Network Operations and Technology/6209 F-coded officers are authorized when:

1. An officer has not completed all required ESR (not completed a thesis at NPS).

2. An officer attends a Civilian Institution and completes two thirds or greater of the ESR.

Note 2:

b. Network Operations and Technology/6209 G-coded officers are authorized when:

1. An officer has an F code and has done a tour in a master's degree billet or higher.

Note 3:

b. Network Operations and Technology/6209 H-coded Billets are authorized for:

1. Billets requiring expertise in the duty requirements as described above where a master's level of knowledge is desirable but not essential for optimum performance.

Note 4:

c. Network Operations and Technology/6209 P-coded Billets are authorized when the billet requires the following:

1. Primary duties requiring the CSRs.

d. Network Operations and Technology/6209 P-coded officers are authorized when:

1. The officer completes Network Operations and Technology master's degree at NPS. Full Subspecialty will not be given if a thesis or capstone project is not completed. The officer will 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 the 6209 ESRs.

Note 5:

c. Network Operations and Technology/6209 Q-coded billets are authorized when the billet requires:

1. All requirements of the P code and experience in the duty requirements as described above as through filling a P-coded billet.

d. Network Operations and Technology/6209 Q-coded officers are authorized when:

1. They complete Network Operations and Technology/6209 ESR, either at NPS or another accredited institution, and have done at least 18 months in a master's degree coded billet or higher – Must have a P code prior to the Q-coded tour.

2. F-coded officers cannot obtain Q codes. They will be authorized G codes.

Note 6:

c. Network Operations and Technology/6209 R-coded billets are authorized justified when, in addition to the requirement for S-coded billets, the billet must be filled by officers having filled a previous 6209-coded billet. Leadership, management, planning or programming of specific duties through familiarity or experience, as through service in a previous billet, should characterize these billets.

d. Network Operations and Technology/6209 R-coded officers are authorized when:

1. The officer has filled one B, S, R, P, Q coded billets for more than 18 months and has an S subspecialty code.

2. Two FITREPs justify that he/she has accomplished the task(s) indicated above for more than 18 months. This in the case the S code was gained as in paragraph 4.b.3 and has not filled a B, S, R, P, or Q coded billet.

Note 7:

c. Network Operations and Technology/6209 S-coded billets are authorized when the following conditions are met:

1. The duties require detailed knowledge of, or experience in, information systems or networks as described above.

2. Appropriate training on specific information systems or networks is available and accessible to qualified officers prior to assignment to the billets.

d. Network Operations and Technology/6209 S-coded officers are authorized when:

1. The officer has filled a B, S, R, P, Q, H coded billet for more than 18 months and has no Subspecialty Code in this field.

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

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

5. Subspecialty Code/Curriculum Sponsor, Major Area Sponsor, and Subject Matter Experts

a. Subspecialty Code/Curriculum Sponsor: VADM Timothy White, Commander, U.S. Fleet Cyber Command/Commander, U.S. TENTH Fleet

b. Major Area Sponsor: VADM Matthew Kohler, DCNO, Information Warfare (OPNAV N2N6)

c. Subject Matter Expert: CAPT Michael Vernazza, Chief of Staff, U.S. Fleet Cyber Command/U.S. TENTH Fleet

APPROVED:	FLTCYBERCOM/C10F (Curriculum Sponsor)	17OCT18 [DATE]
APPROVED:	OPNAV N2N6 (MAS)	17DEC18 [DATE]
APPROVED:	Director, OPNAV N12	30 April 2019 [DATE]