PROPOSED CORE SKILL REQUIREMENTS
Network Operations and Technology
NWOT 6209
Curriculum #386

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) Employ the military network as operational platform for information, an agile warfighting system. Develop, operate, 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.

(2) Make recommendations concerning military application of future cyber 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 network based on indications and warning to preemptively thwart adversary actions. Determine requirements from local to enterprise level.

(3) Assess the interoperability of hardware and software and manage acquisition processes for future network capabilities and integration of new capabilities with legacy infrastructure.

(4) Operate and exploit computer network and communications systems that comprise the backbone of the operational platform for information, and integrate advanced communications programs, policy, protocol and procedures into military systems.

(5) Devise and employ measures to preserve and protect friendly/DOD cyberspace capabilities, networks and net-centric capabilities. Recommend tools, processes and policies that will help preemptively identify potential threats and counter them. Plan and carry out actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation.

(6) Optimize Command and Control system configurations to align with changes in the operational environment, and codify and execute pre-planned responses to enable continued operations in a communications-degraded environment. Recommend tools, processes and procedures that proactively identify potential threats to communications systems so action can be taken prior to adversary action to degrade or deny efficacy of systems.

(7)   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.

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

(9)   Integrate unmanned/autonomous (UV/AS) cyber resources into operational planning, for improved execution of command and control, communications, ISR, and weapon delivery. Identify vulnerabilities in the unmanned/autonomous vehicle asset architecture and execute mitigating or alternative actions.

(10)   Conduct strategic, operational and tactical planning for Defensive Cyber Operations (DCO), 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 innovative use of capabilities, cyber authorities, policies, and organizational responsibilities.

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

(12) Ensure useful data are collected, processed, stored, protected, organized, made accessible, and merged with related data sources to deliver relevant information and knowledge to decision makers, at optimum time and format, and at all levels of command.

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

(14) 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.

(15) Empower standardized exchange of information between tactical units and higher echelons to deliver collective battlespace awareness and a synchronized, tailorable common operational picture.

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

   a. Billets assigned to: Surface Warfare, Submarine Warfare, Special Warfare, Human Resources, Aviation Warfare, Aerospace Engineering Duty, Aviation Maintenance Duty, Information Dominance Corps, Medical Service Corps, Supply Corps, and Civil Engineering Corps.

2. <u>Applicable Officer Designator(s)</u>:
   111X/112X/113X/12XX/131X/132X/15XX/18XX/23XX/31XX/51XX/644X/645X/743X

3. <u>Applicable Billet Designator (s)</u>: 1000-1130/1200/1310-1322/1500/1800-1830/1840/2300/3100/5100/6440/6450/7430

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

   a. Network Operations and Technology/6209 S-coded <u>Billets</u> 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.

   b. Network Operations and Technology/6209 S-coded <u>Officers</u> 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) FITREP justifies that s/he 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.

   c. Network Operations and Technology/6209 R-coded <u>Billets</u> 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 <u>Officers</u> 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 s/he 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.

5. Baccalaureate Criteria

a. Network Operations and Technology/6209 E-coded Billets are *authorized but limited to billets codes for O1-O3, where a strong background in information systems and networks is warranted but generally not available through graduate education or experience.*

b. Network Operations and Technology/6209 E-coded Officers are *authorized/justified* when they have received a baccalaureate degree in one of the following areas:

(1) Computer Science or Computer Engineering
(2) Information Systems or Network Engineering
(3) Other degrees with strong correlation to the 6209 ESRs, by petition.

6. Elective Level Criteria

a. 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.

7. Functional Education Criteria

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.

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 masters degree billet or higher.

8. <u>Masters Criteria for *Network Operations and Technology/6209*</u>

a. Network Operations and Technology/6209 P-coded <u>Billets</u> are *authorized* when the billet requires the following:

(1) Primary duties requiring the CSRs.

b. Network Operations and Technology/6209 P-coded <u>Officers</u> 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.

c. Network Operations and Technology/6209 Q-coded <u>Billets</u> 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 <u>Officers</u> are *authorized* when:

(2) 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.

(3) F-coded officers cannot obtain Q codes. They will be authorized G codes.

9. <u>Post-Masters</u>

a. Network Operations and Technology/6209 N-coded <u>Billets</u> are not *authorized*.

b. Network Operations and Technology/6209 N-Coded <u>Officers</u> are *not authorized*.

c. Network Operations and Technology/6209 M-coded <u>Billets</u> *are not authorized*.

d. Network Operations and Technology/6209 M-coded <u>Officers</u> *are not authorized*.

10. Doctorate Criteria

    a. Network Operations and Technology/6209 D-coded Billets are *not authorized.*

    b. Network Operations and Technology/6209 D-coded Officers are *not authorized.*

    c. Network Operations and Technology/6209 C-coded Billets are not *authorized.*

    d. Network Operations and Technology/6209 C-coded Officers are *not authorized.*

11. Core Skill Requirements have been coordinated with the Budget Submitting Offices (BSO) responsible for the billets identified to be re-coded.

BSO	COMMAND	POC	Date
02	Central Operating & Program Support Division (PERS-73)	Apryle Saahir apryle.saahir@navy.mil	15 Apr 13
11	Field Support Activity (01M)	Russell Copon russell.copon@navy.mil	30 Apr 13
15	Office of Naval Intelligence (ONI)	Phil Anderson phillip.anderson@navy.mil	30 Apr 13
18	Chief, Bureau of Medicine and Surgery (BUMED)	Kevin Magnusson kevin.magnusson@med.navy.mil	23 May 13
22	Chief of Naval Personnel (CNP)	Jim Long james.a.long@navy.mil	30 Apr 13
27	Commandant of the Marine Corps	Greg Baker greg.l.baker@usmc.mil	5 May 13
28	Joint Chiefs of Staff	Robert Ford robert.m.ford18.civ@mail.mil	30 Apr 13
33	Commander, Military Sealift Command	Isagani E. Penaranda isagani.penaranda@navy.mil	30 Apr 13
39	Commander, Space and Naval Warfare Systems Command	Daniel Montgomery daniel.montgomery1.ctr@navy.mil	30 Apr 13
44	DIA	Phil Anderson phillip.anderson@navy.mil	30 Apr 13
60	Commander, U.S. Fleet Forces	Sherri Smith sherri.smith1@navy.mil	23 Apr 13

70	Commander, U.S. Pacific Fleet	LT Andrew Gates andrew.r.gates@navy.mil	5 Apr 13
75	U.S. Transportation Command	LCDR Bob Reddy rajashaker.reddy@navy.mil	30 Apr 13
76	Chief of Naval Education and Training	Deborah Lloyd deborah.lloyd@navy.mil	30 Apr 13

12. Sponsor and Subject Matter Experts

Sponsor:___Katherine Flattery_____, ___OPNAV N2/N6C___,

Subject Matter Expert: ___Ralph Stephens/LCDR___, NCF,

APPROVED: [signature]   4/21/2013
                SPONSOR'S SIGNATURE   DATE

Director Education and Training (N15) Approved:

_____   _____
         SIGNATURE   DATE