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 18839 series (Manual of Navy Officer Manpower and Personnel Classification) Part B, the following specific criteria are satisfied:

1. Description of 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, 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.

   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 network based on indications and warning to preemptively thwart 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 for 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 measures to preserve and protect friendly warfighting, networks and capabilities, to include 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 availability, integrity, authentication, confidentiality and non-repudiation.

Enclosure (3)
f. CSR-6: Optimize Command and Control system configurations to align with changes in the operational environment, and modify and execute pre-planned responses to enable continued operations in a denied-degraded 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 systems.

g. CSR-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.

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

i. CSR-9: Integrate unmanned/autonomous (UAV/AS) information warfare resources into operational planning, for improved execution of C2, communications, ISR, and weapon delivery. Identify 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 Cyber Operations (DCO), DOD information networks (DODIN) operations and integration of UAV/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.

k. CSR-11: Employ knowledge management, data management strategies, and analytics to enable operational effectiveness and decision-making processes. 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.

l. CSR-12: Identify requirements and solutions for improved Human Machine Interface and operational efficacy of information and decision-enabling systems and tools.

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.

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

2. **Applicable Officer Designator(s)**
   a. 11XX/12XX/13XX/12XX/131X/131X/15XX/18XX/23XX/31XX/51XX

3. **Applicable Billet Designator**
   a. 1000-1150/1200/1310-1322/1500/1800-1890/2300/3100/5100

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 NAVPER 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.

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

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).

3 Enclosure (3)
2. An Officer attends a Civilian Institution and completes two thirds or greater of the ESR.

Note 2:
  a. Network Operations and Technology/6209 Q-coded Officers are authorized when:
     1. An Officer has an F code and has done a tour in a masters degree billet or higher.

Note 3:
  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.

Note 4:
  a. Network Operations and Technology/6209 P-coded Billets are authorized when the billet requires the following:
     1. Primary duties requiring the CSRs.
  b. 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 2 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:
  a. 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.
  b. 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. P-coded officers cannot obtain Q codes. They will be authorized G codes.

Note 6:
  a. 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.

b. 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 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.

Note 7:
   a. 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.

b. 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. 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.

5. Major Area Sponsor and Subject Matter Experts

   a. Major Area Sponsor: VADM Jan Tighe, DCNO, Information Warfare (OPNAV N2/N6)

   b. Subject Matter Expert: Mr. John Hope, NAVIFOR N1

   APPROVED: [Signature] 12/29/16
   CYBERCOM/C10R (Curric Sponsor) [DATE]

   APPROVED: [Signature] 2/25/17
   OPNAV N2/N6 (N2S) [DATE]

   APPROVED: [Signature] 3/20/2017
   Director, OPNAV N12 [DATE]