OPNAV INSTRUCTION 5500.66

From: Chief of Naval Operations

Subj: SECURITY COORDINATION BOARD

Ref: (a) SECNAVINST 5500.36

Encl: (1) Security Coordination Board Charter
(2) OPNAV Security Role Matrix

1. **Purpose.** With the increasing complexity and broad range of challenging security issues, the Security Coordination Board (SCB) provides a forum for stakeholders who are accountable and responsible for Navy security to coordinate and integrate cross-functional security issues. This instruction designates a Navy Security Enterprise (NSE) senior executive, per reference (a), and establishes the SCB. The SCB will be the senior-level governance body for the integration and policy coordination of the NSE.

2. **Scope and Applicability.** This instruction applies to all Office of the Chief of Naval Operations (OPNAV) and appropriate echelon 2 commands and activities. Governance is applicable to all appropriate security-related strategies, policies, missions, and activities in the Navy enterprise, including mission assurance, force protection, cyber security, personnel security, and chemical, biological, radiological, nuclear, and high-explosive (CBRNE) defense.

3. **Responsibilities**

   a. The NSE consists of a federated collection of leaders across the OPNAV staff, Navy Installations Command, U.S. Fleet Forces Command, U.S. Pacific Fleet, and U.S. 10th Fleet. Each has varying security mission roles, including responsibility for policy development and execution; accountability for accomplishment of actions and activities within a security mission; coordination; and information. The SCB is the centralized body that will provide integration and coordination across the NSE as outlined in enclosure (1). The appropriate security roles -- Responsible, Accountable, Coordinate, and Inform -- assigned by governing instructions or agreed upon by SCB members and distributed across the NSE are identified in the OPNAV security role matrix in enclosure (2).

   b. The Vice Director, Navy Staff (VDNS) is designated as the NSE senior executive and will serve as the primary point of contact for external security stakeholders.

4. **Records Management.** Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy (SECNAV) Manual 5210.1 of January 2012.
5. **Review and Effective Date.** Per OPNAVINST 5215.17A, Director, Navy Staff (DNS) will review this instruction annually on the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 5 years, unless revised or cancelled in the interim, and will be reissued by the 5-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

![Signature]

K. M. DONEGAN  
Director, Navy Staff

Releasability and distribution:  
This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, [http://doni.documentservices.dla.mil](http://doni.documentservices.dla.mil)
SECURITY COORDINATION BOARD CHARTER

1. Purpose

   a. The Security Coordination Board (SCB) will be the senior-level governance body for the integration and policy coordination of the Navy Security Enterprise (NSE). It will provide a forum for stakeholders who are accountable and responsible for Navy security to coordinate and integrate cross-functional security issues.

   b. Additionally, it may:

      (1) advise the Chief of Naval Operations (CNO) on security policy and training, provide recommendations on key policy decisions and opportunities for standardization and improved effectiveness and efficiency, and facilitate cross-functional security policy coordination;

      (2) commission reviews and in-depth studies of security issues and, based on the results, make recommendations for developing or improving policies, processes, procedures, and products to address pervasive, enduring, or emerging security challenges; and

      (3) review resource investments and priorities and recommend changes to the NSE for submission to the CNO, through the NSE senior executive.

2. Authorities. Deliberations of the SCB may influence security policy or resourcing; however, decision authority will remain with the responsible offices identified in enclosure (2).

3. Membership

   a. The voting membership of the NSE SCB will consist of:

      (1) DNS, who will serve as chair;

      (2) VDNS, who herein is designated as the NSE senior executive;

      (3) Deputy Chief of Naval Operations for Manpower, Personnel, Training, and Education (CNO N1);

      (4) Deputy Chief of Naval Operations for Information Warfare (CNO N2N6);

      (5) Deputy Chief of Naval Operations for Operations, Plans, and Strategy (CNO N3N5);

      (6) Deputy Chief of Naval Operations for Readiness and Logistics (CNO N4);
(7) Deputy Chief of Naval Operations for Integration of Capabilities and Resources (CNO N8);

(8) Deputy Chief of Naval Operations for Warfare Systems (CNO N9);

(9) Director, Special Programs Division (N9SP);

(10) Chief of Navy Reserve (CNO N095);

(11) Chief of Information (CHINFO) (CNO N09C);

(12) Judge Advocate General (JAG) of the Navy (CNO N09J);

(13) Deputy Director, Naval Nuclear Propulsion Program (CNO N00N);

(14) Commander, Navy Installations Command;

(15) Commander, U.S. 10th Fleet;

(16) Deputy Commander, U.S. Fleet Forces Command; and

(17) Deputy Commander, U.S. Pacific Fleet.

b. The chair may invite representatives as appropriate to participate as non-voting members of the NSE SCB.

c. If additional voting members are needed, a recommendation may be submitted to the NSE SCB for approval.

4. Meetings. The NSE SCB must meet no less than semiannually and as required at the call of the chair. The chair will set the agenda with the input from the members.

5. Subgroups and Working Groups

   a. The NSE SCB may be informed by standing subgroups or ad-hoc working groups and may establish standing subgroups or ad-hoc working groups as deemed necessary. Each group must have a charter or specific tasking document. Meeting minutes must be maintained and agreed to by the members of the subgroup or working group and action items must be tracked. Copies of minutes and action items must be provided to the designated executive secretary for tracking on behalf of the NSE SCB. Reports of progress or action must be provided to the NSE SCB as requested, but no less than annually.
b. The integrated capabilities requirements review board (ICRRB) is established as a standing subgroup under the NSE SCB.

(1) The co-chairs for the ICRRB will be O-6 or GS-15 level representatives from CNO (N3N5) (afloat antiterrorism/force protection (AT/FP) policy) and Director, Shore Readiness (OPNAV N46) (ashore AT/FP policy and resource sponsor).

(2) Within 30 days of approval of the SCB charter, the ICRRB co-chairs must submit working group charters to the SCB for approval.

6. **Administration**

a. The VDNS will designate an executive secretary who must arrange meetings; prepare, coordinate, and publish minutes; track action items; and perform other duties as the chair or NSE SCB may assign.

b. The NSE SCB will establish procedures for its operation and that of the subgroups or working groups, as needed.
## OPNAV Security Role Matrix

### OPNAV Security

<table>
<thead>
<tr>
<th>Security Function</th>
<th>N1</th>
<th>N2N6</th>
<th>N3N5</th>
<th>N4</th>
<th>N8</th>
<th>N9</th>
<th>N093</th>
<th>N095</th>
<th>N097</th>
<th>N09F</th>
<th>DNS</th>
<th>N09G NAV</th>
<th>IG</th>
<th>N09J NAV</th>
<th>NCIS</th>
<th>N09J JAG</th>
<th>N09C CHINFO</th>
<th>OPR</th>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPNAV Security</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>I_a</td>
<td>A</td>
<td>A</td>
<td>A, C_a</td>
<td>A</td>
<td>DNS</td>
<td>OPNAV-M 5510.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

28 Aug 2017

### Mission Assurance

<table>
<thead>
<tr>
<th>Mission Assurance</th>
<th>C</th>
<th>A</th>
<th>A</th>
<th>R</th>
<th>C_a</th>
<th>C_a</th>
<th>A</th>
<th>C_a</th>
<th>I_a</th>
<th>I_a</th>
<th>C_a</th>
<th>A</th>
<th>I_a</th>
<th>C_a</th>
<th>N4</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPNAVINST 3502.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Will include Critical Infrastructure Protection (SECNAVINST 3501.1C)

### Insider Threat Program

<table>
<thead>
<tr>
<th>Insider Threat Program</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>I_a</th>
<th>A</th>
<th>C</th>
<th>A</th>
<th>R</th>
<th>C_a</th>
<th>A</th>
<th>A</th>
<th>A, C_a</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OPNAVINST 5510.165A</td>
<td></td>
</tr>
</tbody>
</table>

1 Oct 2015

### Continuity of Operations (COOP)

| Continuity of Operations (COOP) | A  | A    | R^

1 | A    | A    | A    | A    | A    | A    | R^

2 | C_a  | A    | A    | A, C_a | A    | C_a  | A    |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>OPNAVINST 3030.5B</td>
<td>N3N5^2</td>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. CNO (N3N5) is the Navywide and Department of the Navy (DON) Headquarters (HQ) OPR for COOP policy, execution, operations, exercises, and training
2. DNS is the DON HQ OPR for COOP Information Technology (IT) and program funding

### Force Protection

<table>
<thead>
<tr>
<th>Force Protection</th>
<th>I_a</th>
<th>R</th>
<th>I_a</th>
<th>I_a</th>
<th>A</th>
<th>C_a</th>
<th>I_a</th>
<th>I_a</th>
<th>I_a</th>
<th>I_a</th>
<th>C_a</th>
<th>N314</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPNAVINST 3380.5A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

19 Dec 2014

### Navy Installation Emergency Management Program

<table>
<thead>
<tr>
<th>Navy Installation Emergency Management Program</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>R</th>
<th>A</th>
<th>A</th>
<th>C</th>
<th>C</th>
<th>A</th>
<th>I_a</th>
<th>I_a</th>
<th>C</th>
<th>C</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPNAVINST 3440.17A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 Aug 2014

### Physical Security and Law Enforcement Program

| Physical Security and Law Enforcement Program | C  | C_a | R1 | R2 | A    | C_a | I   | C   | C   | I_a  | C_a  | A    | A    | C   | I   | N4 |
|------------------------------------------------|----|-----|----|----|------|-----|-----|-----|-----|------|------|------|-----|-----|----|
| OPNAVINST 5530.14E                             |    |     |    |    |      |     |     |     |     |      |      |     |     |     |    |

1. CNO (N3N5) provides overarching antiterrorism (AT) policy and strategic oversight of the Navy Security Program and will annually assess the effectiveness of current policies and standards
2. CNO (N4) has the primary responsibility for the formulation and dissemination of Navy Security Program policies and standards ashore

### Notes

a. Security role requested (not assigned in governing instructions)
b. References (b) and (c) re-align security responsibilities from NCIS to DUSN(P)
<table>
<thead>
<tr>
<th>Security Function</th>
<th>N1</th>
<th>N2N6</th>
<th>N3N5</th>
<th>N4</th>
<th>N8</th>
<th>N9</th>
<th>N093</th>
<th>N095</th>
<th>N097</th>
<th>N09F</th>
<th>DNS</th>
<th>N00N</th>
<th>N09G NAV IG</th>
<th>N09N</th>
<th>NCIS</th>
<th>N09J JAG</th>
<th>N09C CHINFO</th>
<th>OPR</th>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navy Antiterrorism Program</td>
<td>A</td>
<td>A</td>
<td>R&lt;sup&gt;1&lt;/sup&gt;</td>
<td>C&lt;sup&gt;2&lt;/sup&gt;, A</td>
<td>A</td>
<td>A&lt;sup&gt;3&lt;/sup&gt;</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>A</td>
<td>A</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C</td>
<td>N3N5</td>
<td>OPNAVINST F3300.53C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small Arms Training and Qualification</td>
<td>C</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>R&lt;sup&gt;1&lt;/sup&gt;</td>
<td>A</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>A</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I</td>
<td>N4&lt;sup&gt;1&lt;/sup&gt;</td>
<td>OPNAVINST 3591.1G</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security of Conventional Arms, Ammunition, and Explosives</td>
<td>I</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>R&lt;sup&gt;1&lt;/sup&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>N09N&lt;sup&gt;1&lt;/sup&gt;</td>
<td>OPNAVINST 5530.13C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defense Support of Civil Authorities</td>
<td>C</td>
<td>R</td>
<td>A</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>A</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>N31</td>
<td>OPNAVINST 3440.16E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Security</td>
<td>C</td>
<td>R&lt;sub&gt;a&lt;/sub&gt;</td>
<td>A&lt;sup&gt;2&lt;/sup&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sup&gt;3&lt;/sup&gt;</td>
<td>R&lt;sup&gt;3&lt;/sup&gt;C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>I&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>A</td>
<td>A&lt;sub&gt;2&lt;/sub&gt;C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>C&lt;sub&gt;a&lt;/sub&gt;</td>
<td>N6</td>
<td>OPNAVINST 5239.1C</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Footnotes:
- a. Security role requested (not assigned in governing instructions)
- b. Refs (b) and (c) re-align security responsibilities from NCIS to DUSN(P)

1. CNO (N3N5) must be responsible for strategic oversight of Navy AT policy, both ashore and afloat; develop AT strategy; provide program implementing guidance; identify and quantify the degree of risk to be assumed in the AT mission area; review and evaluate the Navy AT Program; and develop and manage the Navy AT Strategic Plan.
2. CNO (N4) is responsible for ashore AT policy. Also assigned in OPNAVINST 5450.352
3. CNO (N9) (from OPNAVINST 5450.352) will coordinate, with other Services and agencies, antiterrorism/force protection (AT/FP) for the Navy and all chemical, biological, radiological, and nuclear matters afloat and ashore.

1. Pending update shifts OPR from OPNAV (N314 Afloat Force Protection) to CNO (N4)
2. Pending update shifts OPR from CNO (N09N) to CNO (N4)
3. Navy Information Assurance (IA) Program to be replaced by Navy Cybersecurity Program
4. CNO (N2N6) (from OPNAVINST 5450.353) the NIA CIO ensures execution of Navy SCI IA practices that protect and defend information technology assets, oversight, and validation of the Federal Information Security Modernization Act (FISMA) compliance and reporting, execution of designated CIO authorization authorities, to include appropriate naval intelligence enterprise risk management, and approval National Intelligence Program (NIP) information technology purchase requests
5. CNO (N8) (from OPNAVINST 5450.352) will maintain responsibility for the management of the Navy SAPCO and for implementing DON SAPCO policies and procedures for the execution management, oversight, administration, security, information assurance, and records management for Navy special access programs and other special access programs with Navy equities. 2017 OPNAV re-organization moved SAPCO responsibility to CNO (N9)
## OPNAV Security Role Matrix

<table>
<thead>
<tr>
<th>Security Function</th>
<th>OPNAV Organizational Element</th>
<th>N1</th>
<th>N2N6</th>
<th>N3N5</th>
<th>N4</th>
<th>N8</th>
<th>N9</th>
<th>N093</th>
<th>N095</th>
<th>N097</th>
<th>N09F</th>
<th>DNS</th>
<th>N00N</th>
<th>N09G NAV IG</th>
<th>N09N</th>
<th>NCIS</th>
<th>N09 JAG</th>
<th>N09C CHINFO</th>
<th>OPR</th>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navy Cybersecurity Program(^1,2)</td>
<td>C</td>
<td>R, A(^3)</td>
<td>I(_a)</td>
<td>A</td>
<td>A(^4), A</td>
<td>C(_a)</td>
<td>I(_a)</td>
<td>I(_a)</td>
<td>I(_a)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Navy Cybersecurity Program to replace Navy IA Program
2. Will include Navy Industrial Base Data Protection
3. CNO (N2N6) (from OPNAVINST 5450.353) the NIA CIO ensures execution of Navy SCI IA practices that protect and defend information technology assets, oversight, and validation of FISMA compliance and reporting, execution of designated CIO authorization authorities, to include appropriate naval intelligence enterprise risk management, and approval NIP Information Technology Purchase Requests
4. CNO (N8) (from OPNAVINST 5450.352) will maintain responsibility for the management of the Navy SAPCO and for implementing DON SAPCO policies and procedures for the execution management, oversight, administration, security, information assurance, and records management for Navy special access programs and other special access programs with Navy equities. FY17 OPNAV re-organization moves SAPCO responsibility to CNO (N9)

<table>
<thead>
<tr>
<th>Operations Security(^1)</th>
<th>A</th>
<th>R</th>
<th>I(_a)</th>
<th>I(_a)</th>
<th>C(_a)</th>
<th>C(_a)</th>
<th>I(_a)</th>
<th>I(_a)</th>
<th>I(_a)</th>
<th>A</th>
<th>C(_a)</th>
<th>A</th>
<th>A(_b)C(_a)</th>
<th>C(_a)</th>
<th>C</th>
<th>N2N6</th>
<th>OPNAVINST 3432.1A</th>
</tr>
</thead>
</table>
1. Update pending | | | | | | | | | | | | | | | | | 4 Aug 2011 |

| Information Security | A | I\(_a\) | I\(_a\) | A | I\(_a\) | I\(_a\) | I\(_a\) | I\(_a\) | | R\(_{a,A}\) | C\(_a\) | R\(_b\)C\(_a\) | C\(_a\) | N09G\(^c\) | | | | | | | |
|----------------------|---|------|------|---|------|------|------|------|---|------|---|------|---|---|-----|-----------|
1. DNS agreed to assume OPR for OPNAV | | | | | | | | | | | | | | | | | 6 Oct 2006 |

| Sensitive Compartmented Information (SCI) Security\(^1\) | R, A\(^2\) | I\(_a\) | I\(_a\) | C\(_a\) | R\(_{a,C}\), C | C\(_a\) | I\(_a\) | I\(_a\) | I\(_a\) | C\(_a\) | C\(_a\) | DoDM 5105.21 |
|--------------------------|---|------|------|------|------|------|------|------|------|---|------|---|---|-----|-----------|
1. New NIA SCI Cybersecurity instruction pending (see note 2)  
2. CNO (N2N6) (from OPNAVINST 5450.353) the NIA CIO ensures execution of Navy SCI IA practices that protect and defend information technology assets, oversight, and validation of FISMA compliance and reporting, execution of designated CIO authorization authorities, to include appropriate naval intelligence enterprise risk management, and approval NIP Information Technology Purchase Requests  
3. CNO (N8) (from OPNAVINST 5450.352) will maintain responsibility for the management of the Navy SAPCO and for implementing DON SAPCO policies and procedures for the execution management, oversight, administration, security, information assurance, and records management for Navy special access programs and other special access programs with Navy equities. FY17 OPNAV re-organization moves SAPCO responsibility to DCNO (N9)

---

Footnotes:

- a. Security role requested (not assigned in governing instructions)
- b. Refs (b) and (c) re-align security responsibilities from NCIS to DUSN(P)

Enclosure (2)
## OPNAV Security Role Matrix

<table>
<thead>
<tr>
<th>Security Function</th>
<th>N1</th>
<th>N2</th>
<th>N3</th>
<th>N4</th>
<th>N8</th>
<th>N9</th>
<th>N09</th>
<th>N07</th>
<th>N09F</th>
<th>N00N</th>
<th>N09G</th>
<th>IG</th>
<th>NCIS</th>
<th>N09J</th>
<th>JAG</th>
<th>CHINFO</th>
<th>OPR</th>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel Security</td>
<td>$A_2$</td>
<td>$A, C^3$</td>
<td>$I_a$</td>
<td>$I$</td>
<td>$A$</td>
<td>$A_a$</td>
<td>$C_a$</td>
<td>$C_a$</td>
<td>$C_a$</td>
<td>$C_a$</td>
<td>$R_b C_a$</td>
<td>$C_a$</td>
<td>$N09N_3^b$</td>
<td>SECNAVINST 5510.30B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel Identity Protection Program$^1$</td>
<td>$R^2$</td>
<td>$C_a$</td>
<td>$C_a$</td>
<td>$C_a$</td>
<td>$C_a$</td>
<td>$I_a$</td>
<td>$C_a$</td>
<td>$I_a$</td>
<td>$A$</td>
<td>$I_a$</td>
<td>$C_a$</td>
<td>$A$</td>
<td>$C_a$</td>
<td>$A$</td>
<td>DNS</td>
<td>SECNAVINST 5211.5E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Program</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$C$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$R^1$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$A, C_a$</td>
<td>$A$</td>
<td>DNS</td>
<td>SECNAVINST 5500.37</td>
<td></td>
</tr>
<tr>
<td>Identity Activities$^{1,2}$</td>
<td>$A$</td>
<td>$A$</td>
<td>$A$</td>
<td>$A$</td>
<td>$A$</td>
<td>$C_a$</td>
<td>$A$</td>
<td>$A$</td>
<td>$A$</td>
<td>$C_a$</td>
<td>$A$</td>
<td>$C_a$</td>
<td>$A$</td>
<td>$C_a$</td>
<td>$A$</td>
<td>DNS</td>
<td>SECNAVINST 5211.5E</td>
<td></td>
</tr>
<tr>
<td>Sex Offender Tracking, Assignment, and Access Restrictions within the Navy</td>
<td>$R$</td>
<td>$I_a$</td>
<td>$C$</td>
<td>$C$</td>
<td>$I_a$</td>
<td>$I_a$</td>
<td>$C_a$</td>
<td>$N135^1$</td>
<td>$OPNAVINST 1752.3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Footnotes:

a. Security role requested (not assigned in governing instructions)
b. Refs (b) and (c) re-align security responsibilities from NCIS to DUSN(P)
<table>
<thead>
<tr>
<th>Organizational Element</th>
<th>N1</th>
<th>N2N6</th>
<th>N3N5</th>
<th>N4</th>
<th>N8</th>
<th>N9</th>
<th>N093</th>
<th>N095</th>
<th>N097</th>
<th>N09F</th>
<th>DNS</th>
<th>N00N</th>
<th>N09G NAV</th>
<th>N09 IG</th>
<th>N09N</th>
<th>NCIS</th>
<th>N09J JAG</th>
<th>N09C CHINFO</th>
<th>OPR</th>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Function</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBRNE</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>I_a</td>
<td>I_a</td>
<td>I_a</td>
<td>C_a</td>
<td>N9</td>
<td>OPNAV 3400.10H</td>
<td>17 May 2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemical, Biological, Radiological, and Nuclear Defense Requirements Supporting Operational Fleet Readiness</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>C^1</td>
<td>A</td>
<td>C</td>
<td>I_a</td>
<td>I_a</td>
<td>I_a</td>
<td>C_a</td>
<td>DNS</td>
<td>OPNAVINST 8120.1</td>
<td>27 Oct 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nuclear Weapons Security</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>C^1</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>A, C_a</td>
<td>A</td>
<td>N9</td>
<td>OPNAV 3440.15C</td>
<td>23 Oct 2012</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nuclear Weapon Incident Response Management</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>C^1</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>C_a</td>
<td>A</td>
<td>N4</td>
<td>OPNAVINST 5530.16A</td>
<td>11 May 2011</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Standards For Safeguarding Biological Select Agents &amp; Toxins</td>
<td>R</td>
<td>C^1</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>A</td>
<td>C_a</td>
<td>I</td>
<td>N00N</td>
<td>OPNAV 5210.16</td>
<td>21 Sep 1978</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Footnotes:
- a. Security role requested (not assigned in governing instructions)
- b. Refs (b) and (c) re-align security responsibilities from NCIS to DUSNP
## OPNAV Security Role Matrix

<table>
<thead>
<tr>
<th>Security Function</th>
<th>OPNAV Organizational Element</th>
<th>N1</th>
<th>N2N6</th>
<th>N3N5</th>
<th>N4</th>
<th>N8</th>
<th>N9</th>
<th>N093</th>
<th>N095</th>
<th>N097</th>
<th>N09F</th>
<th>DNS</th>
<th>N00N</th>
<th>N09G NAV IG</th>
<th>N09N</th>
<th>NCIS</th>
<th>N09J JAG</th>
<th>N09C CHINFO</th>
<th>OPR</th>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safeguarding Nuclear Command and Control Extremely Sensitive Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguarding of Naval Nuclear Propulsion Information</td>
<td></td>
<td>I_a</td>
<td>I_a</td>
<td>C_a</td>
<td>I_a</td>
<td>A</td>
<td>R</td>
<td>I_a</td>
<td>C_a</td>
<td>N00N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OPNAVINST N9210.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pandemic Influenza Policy</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>C^1</td>
<td>A</td>
<td>A</td>
<td>C_a</td>
<td>I_a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OPNAVINST 3500.41</td>
<td></td>
</tr>
<tr>
<td>CWMD Policy</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>A^1</td>
<td>A</td>
<td>A, C^2</td>
<td>A</td>
<td>I</td>
<td>I_a</td>
<td>A^3 C_a</td>
<td>C_a</td>
<td>N3N5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OPNAVINST 3400.11A</td>
</tr>
</tbody>
</table>

1. Includes Unclassified and classified portions

1. CNO (N9) (from OPNAVINST 5450.352) will coordinate, with other Services and agencies, AT/FP for the Navy and all chemical, biological, radiological, and nuclear matters afloat and ashore

1. Also, CNO (N4) (from OPNAVINST 5450.352) will pursue interagency and international coordination to present and protect Navy environmental, radiological protection, energy, and compatible use interests

2. CNO (N9) (from OPNAVINST 5450.352) will coordinate, with other Services and agencies, AT/FP for the Navy and all chemical, biological, radiological, and nuclear matters afloat and ashore

3. CNO (N09N) (from OPNAVINST 5450.352) will manage matters involving criminal investigations, counterintelligence, technical surveillance countermeasures, protective service operations, and terrorism investigations and operations. Manage domestic and international law enforcement and counterintelligence relations

Footnotes:

a. Security role requested (not assigned in governing instructions)
b. Refs (b) and (c) re-align security responsibilities from NCIS to DUSN(P)

Enclosure (2)
# OPNAV Security Role Matrix

<table>
<thead>
<tr>
<th>Security Function</th>
<th>N1</th>
<th>N2N6</th>
<th>N3N5</th>
<th>N4</th>
<th>N8</th>
<th>N9</th>
<th>N093</th>
<th>N095</th>
<th>N097</th>
<th>N09F</th>
<th>DNS</th>
<th>N00N</th>
<th>N09G NAV IG</th>
<th>N09N</th>
<th>NCIS</th>
<th>N09J JAG</th>
<th>N09C CHINFO</th>
<th>OPR</th>
<th>INSTRUCTION</th>
</tr>
</thead>
</table>

**Security Roles:**
- R - Responsibility
- A - Accountable
- C - Coordinate/Consult
- I - Informed

**Security Role Definitions:**
- **Responsibility** = Office of Primary Responsibility (OPR) for policy and/or ensuring a mission / function / task is accomplished
- **Accountable** = Office accountable to OPR, or assigned by other OPNAV / SECNAV directives, to accomplish a mission / function / task
- **Coordinate / Consult** = Office with whom the OPR or Accountable office must coordinate / consult with in order to modify policy or accomplish a mission / function / task
- **Inform** = Office that must be informed of policy changes or matters involving accomplishment of a mission / function / task

**Acronyms:**
- CHINFO = Chief of Information
- CIO = Chief Information Officer
- CWMD = Countering Weapons of Mass Destruction
- DNS = Director, Navy Staff
- DUSN(P) = Deputy Under Secretary of the Navy (Policy)
- FOIA = Freedom Of Information Act
- JAG = Judge Advocate General
- NAV IG = Naval Inspector General
- NCIS = Naval Criminal Investigative Service
- NIA = Naval Intelligence Activity
- OPR = Office of Primary Responsibility
- PA = Public Affairs
- SAPCO = Special Access Program Central Office
- SCI = Special Compartmented Information

---

**Footnotes:**
- a. Security role requested (not assigned in governing instructions)
- b. Refs (b) and (c) re-align security responsibilities from NCIS to DUSN(P)