NSTC INSTRUCTION 3070.2

From: Commander, Naval Service Training Command

Subj: OPERATIONS SECURITY PROGRAM

Ref: (a) DODMAN 5205_02 Series (OPSEC)  
(b) SECNAVINST 3070.1 Series (OPSEC)  
(c) OPNAVINST 3432.1 Series (OPSEC)  
(d) NETCINST 3070.1 Series (OPSEC)  
(e) NSTCINST 2100.1 Series (Telecommunication)  
(f) NSTCINST 5720.1 Series (Web Use Policy)  
(g) NSTCINST 5720.2 Series (Public Affairs)  
(h) NSTCINST 5211.1 Series (Privacy Act)  
(i) NSTC INST 5230.1 Series (IT Governance)

Encl: (1) Critical Information List (CIL)  
(2) NSTC OPSEC Self-Assessment Tool  
(3) Waiver Request Template


2. Applicability. This guidance is applicable to all assigned NSTC Staff.

3. Background. The Secretary of the Navy (SECNAV) has reaffirmed all units must follow Operations Security Program (OPSEC) practices in their daily military operations. The practice of OPSEC enables mission success by preventing inadvertent compromise of sensitive or unclassified activities, capabilities, or intentions at the strategic, operational, and tactical levels.

4. OPSEC Policies. The following OPSEC policies are hereby instituted:

   a. Critical Information Policy. Enclosure (1) defines information that must be protected. This is not an exhaustive list, and should be amended as situations warrant.

   b. Email Policy. Per reference (f), digital signatures and encryption techniques shall be used on Non-secure Internet Protocol Router Network (NIPRNET) emails that contain the following:

      (1) Sensitive but unclassified information;
(2) All items listed in enclosure (1);

(3) Personally Identifiable Information (PII);

(4) Payroll, contracts, finance, logistics, personnel management, and proprietary information; and

(5) Any official record requiring authentication.

c. **Shredder Policy.** All documents containing data listed under 7(c) shall be shredded using a cross-cut-style shredder. All classified paper must be destroyed.

d. **Web Use Policy.** Web policy should be followed in accordance with reference (f).

e. **Social Media Policy.** Do not allow unknown or untrusted persons to have access to Personally Identifiable, nor Critical Information without approval for public release per reference (f).

f. **Personal Electronic Device (PED) Policy.** PEDs may be used to conduct NSTC business, but shall not be connected to Navy networks per reference (i).

5. **Responsibilities.** All NSTC personnel shall exercise OPSEC in the daily execution of assigned duties, complete required OPSEC Training upon indoctrination and annually thereafter as directed, and be familiar with the contents of enclosure (1). Additional responsibilities include:

a. **Commander, NSTC is overall responsible for the OPSEC Program and shall designate an OPSEC Program Manager to ensure strict adherence to references (a) through (d).**
b. The OPSEC Program Manager manages the OPSEC Program per references (a) through (d) and is responsible for maintaining this instruction. Additional responsibilities include:

   (1) Act as the Commander’s representative to ensure OPSEC measures are in place and practiced during all command activities;

   (2) Ensure all hands are aware of the contents of enclosure (1);

   (3) Complete the computer-based training, OPSEC Fundamentals Course (OPSE-1301), or approved equivalent, and the OPSEC Program Manager's Practitioner's Course (OPSE-2500), or an approved equivalent course, available on the Interagency OPSEC Support Staff website (https://www.iad.gov/ioss/). Additional higher-level OPSEC training will be conducted as necessary;

   (4) Advise the Commander and Department Heads/Directors on the status of the OPSEC Program;

   (5) Conduct a Formal Review of the OPSEC Program prior to turnover and annually per enclosure (2). Provide the results to the Commander via the Chief of Staff;

   (6) Promote OPSEC awareness throughout the command via posters, special briefings, and other such techniques;

   (7) Attend and participate in OPSEC Working Group (WG) meetings with other external agencies as appropriate;

   (8) Propose and train a replacement OPSEC Program Manager prior to detachment from the command; and

   (9) Conduct a Formal Review of the OPSEC Process using enclosure (2).

c. The Public Affairs Officer shall review and approve articles and documents for release to the public per reference (f).

d. Department Directors shall ensure OPSEC is considered in all activities and operations for which they are responsible and ensure personnel in their department complete all required training.

e. OPSEC Working Group meetings shall be conducted annually. The OPSEC Working Group shall be chaired by the OPSEC Program Manager. Details on the OPSEC Working Group Meeting shall be routed to CNSTC via the Chief of Staff. Additionally, OPSEC WG members shall:

   (1) Assist the OPSEC Program Manager in conducting OPSEC training, annual assessments, surveys, awareness campaigns, and other OPSEC tasks at NSTC; and
(2) Notify the OPSEC Program Manager of recommendations to meet the intent of the OPSEC program or potential OPSEC concerns.

f. Contracting Officer Representative. NSTC lacks contracting authority and is dependent upon the issuing contracting officer for inclusion of applicable clauses. Requiring Activity shall review all Statements of Work and/or Performance Work Statements for OPSEC requirements per reference (a).

6. **Review.** The following shall be conducted annually by the OPSEC Program Manager:

   a. Verify references (a) through (d) are still valid;
   
   b. Conduct a Formal Review of the command’s OPSEC Program per enclosure (2);
   
   c. Chair an OPSEC Working Group Meeting and route the minutes to CNSTC for review;
   
   d. Review enclosure (1) and (2), and update if necessary; and
   
   e. Review this instruction, and update if necessary.

7. **Records Management.** Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 January 2012.

8. **Review and Effective Date.** Per OPNAVINST 5215.17A, NSTC will review this instruction annually on the anniversary of its effective date to ensure palpability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction.

M. D. BERNACCHI

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Naval Service Training Command issuance website, http://www.netc.navy.mil/nstc/NSTC_Directives/instructions.html.
A necessary condition for maintaining essential secrecy is protection of critical information ensuring that in addition to traditional security measures, NSTC maintains a heightened awareness of potential threats of adversaries taking advantage of publicly available information and other detectable unclassified activities to derive indicators of U.S. intentions, capabilities, operations, and activities. The NSTC Critical Information Listing (CIL) below is not all-inclusive and should be amended for specific operations and activities.

DO NOT DISCUSS, OR TALK AROUND, CRITICAL INFORMATION OVER UNSECURED TELEPHONE LINES OR UNCLASSIFIED E-MAIL. USE YOUR SECURE PHONE AND NETWORKS. DIGITALLY SIGN/ENCRYPT EMAILS! EXAMPLES INCLUDE:

- Command, control, communications, and intelligence architecture.
- Detailed installation maps/site photography/building plans.
- Sensitive joint training and experimentation issues affecting command, services, and agencies.
- VIP/distinguished visitor schedules, travel itineraries, etc.
- User names and passwords.
- Access/identification cards.
- Personal identification information.
- Entry/exit (security) procedures.
- Address and phone lists.
- Budget information.

ALWAYS PRACTICE OPSEC. REMEMBER THAT THE ADVERSARY MAY BE LISTENING. THINK LIKE THE WOLF.

APRIL 2017

Enclosure (1)
<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 Jul 18</td>
<td></td>
</tr>
</tbody>
</table>

**Enclosures (2)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Notes**

- Please ensure all documents are submitted by the end of the week.
- Meeting with Team A scheduled for Tuesday at 10 AM.
- Report due by Friday.

---

**Attachments**

- Email for Team B
- Monthly report

---

**Exhibits**

- Chart 1: Project Timeline
- Chart 2: Revenue Comparison

---

**References**

- Document 1: Company Policies
- Document 2: Client Feedback

---

**Signatures**

- [Signature]
- [Signature]

---
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Text 1</td>
</tr>
<tr>
<td>2</td>
<td>Text 2</td>
</tr>
<tr>
<td>3</td>
<td>Text 3</td>
</tr>
<tr>
<td>4</td>
<td>Text 4</td>
</tr>
<tr>
<td>5</td>
<td>Text 5</td>
</tr>
</tbody>
</table>

**Table:**

- **Column 1:** Item
- **Column 2:** Description
From: Commanding Officer, XXXX  
To: OPNAV N2/N6F31, USN  
Via: ISIC  

Subj: WAIVER REQUEST FOR COMMAND OPERATIONS SECURITY PROGRAM MANAGER  

Ref:  
(a) SECNAVINST 3070.2, 5 May 2016  
(b) ALNAV 072-16, 13 Dec 2016  

1. Per reference (a) the OPSEC Program Manager is required to be an O-3 or above or civilians GS-12 or higher. Reference (b) automatically grants a waiver of this requirement if program managers are warfare qualified Information Warfare officers CWO2/above at commands below the Echelon II level.  

2. This paragraph is your reason for requesting the waiver. (Due to the small size of the command, Command XXXX does not have the manpower to support this requirement, non-operational mission.)  

3. Respectfully request the requirements set forth in the references (a) and (b) be waived. (Command) OPSEC Program Manager will be CPO/LTjg XXXX.

CO signature