DEPARTMENT OF THE NAVY
NAVAL SERVICE TRAINING COMMAND
2601A PAUL JONES STREET
GREAT LAKES, ILLINOIS 60088-2845

NSTCNST 3070.2B
N00
1 Jun 2021

NSTC STAFF INSTRUCTION 3070.2B

From: Commander, Naval Services Training Command

Subj: OPERATIONS SECURITY PROGRAM

Ref: (a) DoD Directive 5205.02E of 20 June 2012
(b) DoDM 5205.02, DoD Operations Security Program Manual of 3 November 2008
(c) DoD Instruction 8550.01 of 11 September 2012
(d) JP 3-13.3, Operations Security, 6 January 2016
(e) SECNAVINST 3070.2A
(f) NTTP 3-13.3M

Encl: (1) NSTC Critical Information and Indicators List
(2) OPSEC Decision Flowchart for Article Reviews
(3) NAVAL Services Training Command (NSTC) Staff Operations Security (OPSEC) Training Requirements

1. Purpose. To establish and maintain an Operational Security (OPSEC) program at Naval Service Training Command (NSTC) as required by references (a) through (f).

2. Cancellation. NSTCINST 3070.2A.

3. Applicability. All military, civilian, and contracted staff assigned to NSTC Great Lakes.

4. Background. The Department of Defense (DoD) has reaffirmed all units must follow OPSEC practices in their daily military operations. The practice of OPSEC enables mission success by preventing inadvertent compromise of sensitive or unclassified activities, capabilities, intent, as well as operational, and tactical levels.

a. The Department of Navy states in reference (e) that OPSEC is a critical process for all Navy activities.

b. At the command level, OPSEC processes provide commanders with the ability to identify critical information, current vulnerabilities, risks due to its vulnerabilities, and countermeasure decision criteria to mitigate risks.

5. Discussion. The mission of NSTC includes providing assigned shore-based education and training for the five services including both Active and Reserve component personnel, other DoD elements, and other personnel from Nation-state and Coalition partners.

6. Policies and Measures. The following OPSEC policies and measures are hereby instituted in order to protect NSTC's critical information:

a. Establish and implement the best OPSEC practices, procedures, processes, and guidance to enable sustained superior performance and cost-effective protection of NSTC's critical information (i.e., personnel, operations, technology, future initiatives, and sustainment).

b. In order to run an effective OPSEC program, enclosure (1) has been developed to determine the types of information to be protected, and it will be reviewed and updated annually or when critical information changes. It is not an exhaustive list and should be amended as situations warrant.

c. Per reference (c), authorized users of unclassified DoD networks shall comply with all laws, policies, regulations, and guidance concerning communication and the appropriate control of DoD information.

d. Digital signatures and encryption techniques, per reference (c), as applicable, shall be used on all non-secure Internet Protocol Router Network emails that contain:

(1) Sensitive but unclassified information or any items stated in enclosure (1).

(2) Personally Identifiable Information.

(3) Payroll, contracts, finance, logistics, personnel management, and proprietary information.

(4) Operational information regarding status, readiness, location, or operational use of forces or equipment.

(5) Any official record requiring authentication.

e. Establish and maintain an effective OPSEC Working Group (WG) with representatives from all key command components, departments, or functions. The WG shall include a representative where applicable for:

(1) Security.

(2) N005 Flag Administration.

(3) Public Affairs.

(4) N6 Information Technology.

(5) Additional members as designated by Chief of Staff.

f. Enforce a 100 percent shred policy for the destruction of all office-generated paper. This policy applies to items generated by NSTC personnel and those received from outside sources.

NOTE: Newspapers, magazines, commercial wrappers, and packing materials are exempt from this policy only after the address label has been removed and shredded to the greatest extent possible. Dispose of food wrappers and food-like items in appropriate containers.

(1) Destruction/disposal of office paper is authorized by:

(a) Using the designated cross-cut shredders residing in common areas.

(b) Using the blue or gray shred bins with the single-top slot and padlocked (some bins also have chains in addition to the padlock) throughout the building per their exterior labeling instructions for UNCLASSIFIED/CUI information. Contact department OPSEC Representatives for locations or what information shall be disposed in them if in doubt.

(2) All classified paper must be destroyed. All NSTC personnel will complete OPSEC training, as outlined in reference (e), within 60 days of reporting, and annually thereafter. Enclosure (3) outlines the minimum OPSEC training.

7. Responsibilities.

a. Commander, NSTC, via the Chief of Staff

(1) Establish NSTC's OPSEC Program per reference (e) and ensure strict adherence to proper OPSEC measures.

(2) Per reference (e), appoint, in writing, an O-3/GS-12 (or above) to serve as the Command's OPSEC Program Manager and ensure they receive appropriate and periodic OPSEC policy and doctrine training. Per reference (e), the Program Manager should be expected to serve in the role for a minimum of 18 months.

b. OPSEC Program Manager

(1) The Command OPSEC Program Manager acts as the focal point for all OPSEC matters and maintains a thorough knowledge of NSTC operations and familiarity with NETC plans and procedures.

(2) Ensure proper OPSEC measures are in place and the OPSEC process is practiced during all Command activities/operations.

(3) Develop OPSEC policies and procedures as required. Conduct an annual review of OPSEC procedures to assist in the improvement of the OPSEC Program.

(4) Develop/review enclosure (1) annually, identify the critical information that requires protection, and ensure it is provided to the entire workforce and posted both conspicuously in workspaces and online via NSTC Central.

(5) Complete the computer-based training, OPSEC Fundamentals Course (OPSE-1301), the OPSEC Analysis Course (OPSE-2380),

and the OPSEC Program Management Course (OPSE2390), or approved equivalent courses, available on the Interagency OPSEC Support Staff website (https://www.iad.gov/ioss/). Additional higher-level OPSEC training will be conducted as necessary.

(6) Chair the OPSEC WG and provide direction, guidance, and training. The OPSEC WG will meet minimally on a quarterly basis to discuss generic and specific OPSEC issues relevant to the Command, and as necessary to meet trigger/emerging tasking.

(7) Coordinate with the NSTC Security Manager to ensure personnel receive OPSEC indoctrination on arrival. Ensure NSTC Security Manager is using the most current and authorized OPSEC course to provide training.

(8) Advise the Commander and Division Directors/Special Assistants (DD/SAs) on the status of NSTC OPSEC program plans, developments, problems, and proposed solutions.

(9) Conduct an initial baseline, and thereafter, annual OPSEC assessments and surveys, and provide the results to the Commander.

(10) Promote OPSEC awareness throughout NSTC via posters special briefings, and other such techniques.

(11) In coordination with the NSTC Security Manager, ensure all command personnel complete annual OPSEC awareness training.

(12) Attend and participate in OPSEC WG meetings with other external agencies as appropriate.

(13) Assist the NSTC Office of the Inspector General (IG) during Assist Visits.

(14) As directed by higher authority, compile an OPSEC report based on self-assessments and surveys the Chief of Naval Personnel’s OPSEC Program Manager.

(15) Ensure OPSEC requirements, including training requirements, are identified/listed in unclassified and classified contracts awarded in support of NSTC.

(16) Contract related security requirements will be coordinated with the executing contracting office. The Contracting Officer and the requiring subject matter expert will determine the applicable contract language and clauses in conjunction with the Security/OPSEC managers.

c. NSTC DD/SAs

(1) It is highly encouraged to have both a primary and alternate OPSEC WG member to represent all divisions/branches under DD/SA cognizance for a period of one calendar year at which time rotation is also highly-encouraged. For smaller DD/SA codes, combining with other codes is preferred.

(2) Ensure OPSEC is considered in all activities and operations for which they are responsible.

(3) Ensure all designated WG members complete the computer-based training, OPSEC Fundamentals Course (OPSE-1301), or an approved equivalent, within 30 days of their appointment.

d. NSTC Security Manager. Provide and track completion of indoctrination and annual OPSEC training.

e. OPSEC WG:

(1) Review NSTC's organizational mission and objectives to identify potentially critical information and indicators for each division/branch and at the Command level.

(2) Recommend countermeasures against vulnerabilities to critical information and indicators.

(3) Remain actively engaged and assist the OPSEC Program Manager in conducting OPSEC training, annual assessments, surveys, awareness campaigns, and other OPSEC tasks at NSTC.

(4) Ensure that OPSEC measures are included in respective Department/Division daily routine and that enclosure (1) is posted conspicuously and available to all division employees.

(5) Provide necessary liaison to other OPSEC WG members in the accomplishment of the command's OPSEC program.

(6) Complete the computer-based training, OPSEC Fundamentals Course (OPSE-1301), or an approved equivalent, within 30 days of appointment.

(7) Provide all new members of the command with Family Outreach OPSEC training and encourage members to share the training with their dependents.

f. Contracting Officer Representatives. Complete the Defense Acquisitions University (DAU) OPSEC Contract Requirements course (DAU CLC 107) or the OPSEC Fundamentals Course (OPSE-1301) within 30 days of appointment.

g. All NSTC personnel:

(1) Exercise OPSEC procedures in the daily execution of assigned duties and abide by OPSEC policies and procedures.

(2) Complete initial OPSEC training within 60 days of in-processing.

(3) Complete annual OPSEC refresher training.

(4) Notify department OPSEC Representative or the Command OPSEC Program Manager of recommendations for the OPSEC Program or potential OPSEC concerns.

(5) Notify the Chief of Staff via the OPSEC Program Manager of all violations of command OPSEC policy. Members who violate this policy shall receive additional OPSEC training, and additional measures may be taken based on the severity of the offense.

8. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manuel 5210.1 of September 2019.

9. Review and Effective Date. Per OPNAVINST 5215.17A, OPSEC Manager will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

JENNIFER S. COUTURE

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, https://www.netc.navy.mil/Commands/Naval-Service-Training-Command/NSTC-Directives/

NAVAL SERVICE TRAINING COMMAND CRITICAL INFORMATION LIST

A necessary condition for maintaining essential secrecy is protection of critical information Ensuring that 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:

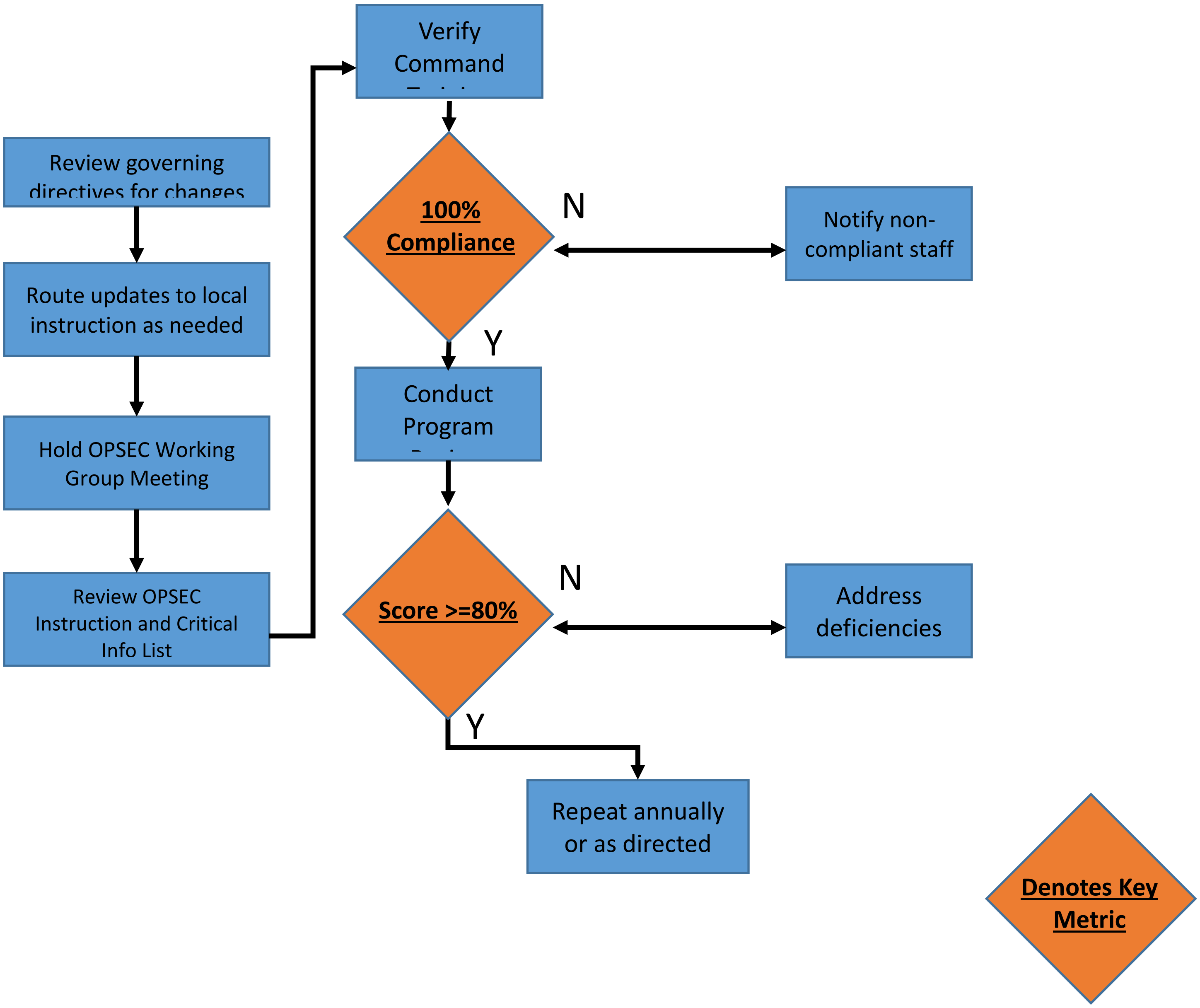
- Command, control, communications, and intelligence architecture.
- Detailed installation maps/site photography/building plans.
- Sensitive joint training and experimentation issues affecting command, services, and agencies
- VIP/distinguished visitor schedules travel itineraries, etc.
- User names and passwords.
- Access/identification information.
- 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.

March 2021

DECISION FLOWCHART for ensuring adequate OPSEC Program Management.

TITLE: Operational Security (OPSEC)
PURPOSE: To define the procedures for ensuring adequate OPSEC Program Management
PROCESS OWNER: Daniel L Rose, (847) 688-7510, Ext. 247, Daniel.l.Rose@navy.mil
GOVERNING DIRECTIVES: SECNAVINST 3070.2A, NETCINST 3070.1C, DODM 5205-02, NTTP 3-13.3M, OPNAVINST 3432.1
Date: 3 Mar 21
For Official Use Only


Review governing directives for changes
Route updates to local instruction as needed
Hold OPSEC Working Group Meeting
Review OPSEC Instruction and Critical Info List
Verify Command
100% Compliance
N
Notify non-compliant staff
Y
Conduct Program
Score >=80%
N
Address deficiencies
Y
Repeat annually or as directed
Denotes Key Metric

NAVAL SERVICE TRAINING COMMAND (NSTC) STAFF OPERATIONS SECURITY (OPSEC) TRAINING REQUIREMENTS

1. The following minimum OPSEC training will be provided to all NSTC staff members:

a. Basic OPSEC Orientation. Upon reporting aboard, all personnel (military, civilian, and contractors) will be provided basic OPSEC orientation training to accomplish the following objectives:

(1) Foster appreciation of the advantages of secrecy, and the harm from a lack of secrecy in military mission accomplishment and capabilities.

(2) Show the role of secrecy in gaining the initiative, attaining surprise, achieving superiority, and maintaining security against hostile action.

(3) Gain an understanding of the OPSEC concept, how it originated and evolved, and its relationship to other security programs.

(4) Gain a general understanding of the hostile intelligence threat and the OPSEC measures used to counter the threat. Focus on hostile espionage spotting and assessing techniques, terrorists, gathering of targeting intelligence, criminal/saboteur/special purpose forces gathering of physical security penetration intelligence, and OPSEC measures to counter these threats.

b. Annual Staff OPSEC Training. OPSEC training will be completed annually by all staff members. Division Training Representatives are responsible for tracking and reporting to the NSTC Security Manager annual completion of OPSEC refresher training. Annual refresher training is authorized using one of the following three methods:

(1) Uncle Sam's OPSEC, NIOC-USOPSEC-3.0 (or current version), available on the Navy eLearning website: https://www.lms.prod.nel.training.navy.mil/.

(2) OPSEC Application (APP): An all-in-one OPSEC APP is available for personnel devices (i.e., tablets/smartphones), which provides OPSEC resources and OPSEC training courses. Users can download the OPSEC APP from the Apple store and Google Play Store at no cost.

(3) In-person OPSEC training may be provided upon request and facilitated by the departmental OPSEC WG
representative, OPSEC Program Manager, or Security Manager.

c. Continuing OPSEC Awareness. Continuing OPSEC awareness information will be disseminated through the following means:

(1) Posters, plan of the week/NSTC Newsletter notes, distribution of case studies, notes on hostile intelligence, special briefings, and other such techniques as warranted.

(2) Publishing information on special intelligence threats and OPSEC measures pertinent to particular command functions and concerned personnel.

(3) As appropriate, briefing and training on subjects which require special OPSEC measures.