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

NSTCINST 3070.2A
N00
9 Apr 2020

NSTC INSTRUCTION 3070.2A

From: Commander, Naval Services Training Command

Subj: OPERATIONS SECURITY PROGRAM

Ref: (a) SECNAVINST 3070.2A
(b) NETCINST 3070.1B
(c) DoDM 5205.02, DoD Operations Security Program Manual of 3 November 2008
(d) NTTP 3-13.3M
(e) OPNAVINST 3432.1A

1. Purpose. To establish guidance for conducting a Level II Operational Security (OPSEC) program at Naval Service Training Command (NSTC) as required by references (a) through (e).

2. Cancellation. NSTCINST 3070.2.

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

4. Roles and Responsibilities. All NSTC personnel shall exercise OPSEC in the daily execution of assigned duties, complete required OPSEC Training upon reporting and annually thereafter as directed, and familiarize themselves with the contents of enclosures (2) and (3). Specific responsibilities follow.

a. Commander, Naval Service Training Command (CNSTC). CNSTC is overall responsible for the OPSEC Program. CNSTC shall:

(1) Take all OPSEC measures required to prevent disclosure of critical information and maintain essential secrecy.

(2) Establish, resource, and maintain an effective OPSEC program.

(3) Designate an OPSEC Program Manager pursuant to reference (a).

b. OPSEC Program Manager (OPSEC-PM). The OPSEC-PM manages the OPSEC Program as prescribed in references (a) through (e). The OPSEC-PM shall:

(1) Within 30 days of designation, complete the computer-based training OPSEC Fundamentals Course OPSE-1301. Within 90 days of designation, complete the in-person OPSEC Program Management Course OPSE-2390. Registration for both courses is through the Interagency OPSEC Support Staff (IOSS) website, https://www.iad.gov/ioss/.

(2) Advise CNSTC on all OPSEC matters.

(3) Ensure that initial and annual refresher training on OPSEC is provided to all employees and contractors at the local command.

(4) Maintain the Essential Elements of Friendly Information (EEFI), and Critical Information and Indicators List (CIIL).

(5) Conduct annual OPSEC Program assessments using the review standards in reference

(a) Report completion of this assessment to the NETC OPSEC-PM.

(6) Hold an annual Command OPSEC Working Group meeting.

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

(8) Participate in installation- and domain-wide OPSEC planning, training, or coordination when such events are available.

(9) Review this instruction annually or as directed and recommend changes as required.

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

d. Department Directors shall:

(1) Ensure OPSEC is considered in all activities and operations for which they are responsible and ensure personnel in their department complete all required training.

(2) Attend, or assign an appropriate representative to attend, the annual OPSEC Working Group meeting.

e. 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).

5. <u>Policy</u>

a. The OPSEC-PM shall maintain an essential elements of friendly information (EEFI) and critical information and indicators list (CIIL).

(1) The EEFI are developed by the OPSEC-PM using enclosure (1). EEFI are the key pieces of information adversaries will likely inquire about regarding our intentions, capabilities, and activities. EEFI serve as the basis from which the CIIL is developed.

(a) The OPSEC-PM shall maintain a copy of the NSTC-specific EEFI in the OPSEC folder of the share drive and in the OPSEC program binder.

(b) The OPSEC-PM shall provide the EEFI for review during the annual OPSEC Working Group meeting.

(2) The CIIL is developed using enclosure (2). This worksheet is intended to guide the OPSEC-PM and OWG members in developing the NSTC CIIL from the EEFI. Reference (d) contains the most up to date version of this worksheet and provides direction in its use.

(a) The CIIL defines information which must be protected to ensure that our EEFI are safeguarded.

(b) The OPSEC-PM shall provide the CIIL to Department Directors.

(c) Department Directors shall provide the CIIL to personnel in their departments when:

1. The individual initially reports. This may be accomplished by having the individual check in with the OPSEC-PM.

2. A revised CIIL is received from the OPSEC-PM

b. The OPSEC Working Group (OWG) is established to assist the OPSEC-PM in their responsibilities.

(1) Reference (a) mandates that the OWG include representative from security, AT/FP, critical infrastructure protection, public affairs, information assurance, and FOIA. Accordingly, the OWG shall consist of a representative from each of the following departments or special programs:

(a) N005 Flag Administration

(b) N4 Logistics

(c) N6 Information Technology

(d) Public Affairs Officer

(e) Physical Security Office

(f) Additional members as designated by the Chief of Staff

(2) OWG members shall:

(a) Assist the OPSEC-PM in planning OPSEC training, annual assessments, surveys, awareness campaigns, and other OPSEC tasks at NSTC.

(b) Notify the OPSEC-PM of recommendations to meet the intent of the OPSEC program or potential OPSEC concerns.

(c) Provide input upon request for the annual self-assessment conducted by the OPSEC-PM.

(d) Be active participants during outside inspections of the NSTC OPSEC Program.

(3) OWG members are advised to develop a baseline understanding of the OPSEC Program through the computer-based training OPSEC Fundamentals Course (OPSE-1301) available on https://www.iad.gov/ioss/. This website is CAC-enabled and requires registration.

c. The OPSEC-PM shall facilitate an annual meeting consisting of the OWG and representatives from each department not represented in the OWG. During this meeting, participants shall ensure that NSTC's EEFI and CIIL are current and applicable to the command, and that the five-step OPSEC process is being applied across the command.

d. The five-step OPSEC process, described in reference (d), is continuous and interactive. It uses established EEFI as a basis for our CIIL. The elements of this process are:

(1) Identification of critical information and its indicators.

(2) Analysis of threats.

(3) Analysis of vulnerabilities.

(4) Assessment of risks.

(5) Application of appropriate countermeasures.

e. The OPSEC-PM shall promote the active participation and involvement of all personnel in the OPSEC program.

(1) Free physical awareness products available from the IOSS website, https://www.iad.gov/ioss/. Products include magnets, posters, calendars, and DVDs.

(2) All-hands reminders, digital fliers, or educational materials may be delivered via command email distros.

6. Essential Elements of Friendly Information (EEFI) Guidelines

a. These guidelines are intended to assit the OPSEC-PM and OWG members in developing the EEFI for NSTC. The actual EEFI are maintained by the OPSEC-PM and may be made available to any member of the command, but should not be made publically available. This precludes their inclusion in this instruction.

(1) Information that reveals the specific capability of an organization.

(2) Information that reveals a weakness or a compromise of a specific operation.

(3) Knowledge about specific measures used to protect a mission or operation.

(4) Information that reveals a security weakness of a unit or activity.

(5) Material about special installation projects, dates, and locations.

(6) Essential personnel privacy information, to include chain of command.

7. Critical Information and Indicators List (CIIL) Worksheet

a. The CIIL shall encompass only information deemed vital to an adversary. It is not necessary to include all sensitive or classified information at the command.

b. The CIIL may include the following types of information:

(1) Sensitive but classified information.

(2) Personally Identifiable Information (PII).

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

(4) Additional items as determined by the OWG and OPSEC-PM.

c. The CIIL is maintained by the OPSEC-PM. Copies of the CIIL are available upon request.

d. Secure all working documents containing information on the CIIL at the end of your workday. Dispose of documents containing information on the CIIL by depositing in labeled shred boxes located in Building 1 or by using a cross-cut shredder.

e. Do not post information from the CIIL to publicly accessible website, including public-facing .mil websites. If the website does not require your CAC or other government-provided credentials to log-in, any information posted could be collected by an adversary.

f. Do not post information from the CIIL to any social media platform.

g. Before releasing information on the CIIL outside of NSTC, consider if the information is necessary to accomplish the tasking at hand.

8. Review. The OPSEC-PM shall review this instruction for currency and accuracy annually following the OWG meeting.

MILTON J. SANDS III

Release 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