



DEPARTMENT OF THE NAVY

NAVAL EDUCATION AND TRAINING CENTER
61 CAPODANNO DRIVE
NEWPORT RHODE ISLAND 02841-1522

IN REPLY REFER TO:
NETCNPTINST 3070.1A
Code 23
17 AUG 95

NETCNPT INSTRUCTION 3070.1A

From: Commander

Subj: OPERATIONS SECURITY (OPSEC) PLAN

Ref: (a) SECNAVINST 3070.1A
(b) CNETINST 3070.1B
(c) CNETINST 5450.43C

1. Purpose. To establish an OPSEC Plan for the Naval Education and Training Center (NETC).
2. Cancellation. NETCNPTINST 3070.1.
3. Policy. OPSEC awareness will be integrated into the daily routine of each staff member.
4. Background. OPSEC, as outlined in references (a) and (b), was established to prevent the disclosure of classified and sensitive information to unauthorized sources. It is intended to ensure that personnel, both military and civilian, are aware of all ways in which sensitive information may be obtained by actual or potential enemies. The function of OPSEC at NETC is to safeguard intelligence information by staff education, identify vulnerable areas, and limit access to sensitive information susceptible to hostile exploitation.
5. Discussion. The mission of the Naval Education and Training Center (NETC), as stated in reference (c), is to administer those schools from which qualified officers are prepared for military service; train international officers and officer candidates, as required; train U.S. Navy enlisted; provide appropriate logistic support for tenant and support activities, including fleet units; and perform such other functions as directed by higher authority. This instruction establishes policy and assigns responsibility for implementing the NETC Operations Security (OPSEC) Plan to accomplish this mission.
6. Responsibilities
 - a. The Commander shall:
 - (1) Establish an OPSEC program, including planning, training, techniques, and methodologies.

(2) Assign a command OPSEC Officer to provide management, review, and inspection of the OPSEC program.

b. The OPSEC Officer. The Command Security Manager shall act as the Command OPSEC Officer and shall:

(1) Execute and coordinate all facets of the NETC OPSEC program.

(2) Update this plan, as necessary, to ensure all OPSEC objectives are met.

(3) Establish and chair a command OPSEC Committee.

(4) Develop and execute an OPSEC Training and Awareness Program for all assigned personnel (civilian and military).

(5) Provide training and guidance to OPSEC coordinators assigned by department directors and special assistants.

(6) Maintain liaison with appropriate intelligence communities to keep abreast of threat assessment to the command.

(7) Ensure OPSEC surveys are conducted as specified in this plan.

(8) Solicit and incorporate inputs to this plan from OPSEC coordinators regarding sensitive projects and/or programs or classified/sensitive information.

c. Department Directors and Special Assistants shall:

(1) Appoint an OPSEC coordinator for their organization.

(2) Provide technical support, as required, to carry out this OPSEC plan.

(3) Ensure all personnel comply with provisions of this plan.

d. The Automatic Data Processing (ADP) Security Officer shall:

(1) Provide ADP security assistance to the OPSEC Officer and department OPSEC coordinators, as required.

(2) Serve as a member on the OPSEC Committee.

e. Department/Special Assistant OPSEC Coordinators shall:

(1) Ensure all personnel in their departments are trained in OPSEC, as required by this instruction.

(2) Provide assistance to the OPSEC Officer.

(3) Monitor their departments for possible vulnerabilities that could be exploited by an adversary. Formal vulnerability assessments (VA) shall be completed by each department/special assistant OPSEC coordinator as part of the command VA program.

(4) Provide input to the OPSEC Officer on those events, projects or programs within their departments which contain classified, sensitive and/or unclassified information and are not sufficiently covered by this OPSEC plan.

(5) Serve as members of the OPSEC Committee.

(6) Training Program. For OPSEC to be effective, all personnel must understand the concept of OPSEC and be able to apply that knowledge and awareness. The primary way to accomplish this is through training. The NETC OPSEC Training and Awareness Program will consist of the following subdivisions:

a. Basic Orientation. Each individual (military/civilian) newly assigned to NETC will receive an OPSEC brief as part of the required Command Orientation Program. This brief will occur within 30 days of reporting on board and will address:

(1) The definition and purpose of OPSEC.

(2) Why OPSEC was originated, into what it has evolved, and its relationship to other security programs.

(3) The intelligence-gathering capabilities of hostile agencies.

(4) OPSEC measures to counterthreats.

(5) The employee's role in OPSEC.

b. Department Training. Department and special assistant OPSEC coordinators will ensure that personnel assigned to their departments attend formal training. OPSEC training will be scheduled by the OPSEC Officer annually.

c. Continuing Awareness. An ongoing OPSEC awareness program will be provided for all personnel. Utilizing a multimedia approach, it will incorporate:

- (1) Lectures. (Notes 1, and 2)
- (2) Posters. (Note 3)
- (3) Plan of the Day notes. (Note 4)
- (4) Navalog articles. (Note 4)

Notes:

- 1. Provided at Command Orientation.
- 2. Scheduled annually by the OPSEC Officer.
- 3. Will be acquired by the OPSEC Officer and distributed to department/special assistant OPSEC coordinators.
- 4. Submitted at least quarterly by the OPSEC Officer.

d. Contractor Briefs. The Defense Investigative Service has the primary responsibility for implementing an OPSEC program within the Department of Defense. Each NETC department director and special assistant will ensure OPSEC is practiced in their relationships with contractors conducting business for their department. Complete security of classified/sensitive information is the goal.

7. OPSEC Monitoring. In order to ensure the preservation of essential security through OPSEC, the command will periodically examine its OPSEC posture by conducting the following surveys:

a. Informal Internal Survey. At least semiannually, the department/special assistant OPSEC coordinator will conduct an informal survey of their department, discussing with assigned personnel the OPSEC program, determining the "state of health" of their area of responsibility from a security viewpoint. They will observe internal security practices and procedures, and make a written report to the OPSEC Officer with a copy to their department director/special assistant.

b. Formal External Surveys. Initiated by the Commander, the OPSEC Officer will conduct an unannounced formal survey of selected departments and special assistants. This will include a review of training, OPSEC awareness, administrative practices and procedures, and ensure appropriate services are being conducted.

The OPSEC Officer will make a formal report of findings to the Commander and appropriate department directors.

c. Vulnerability Assessments/Management Control Review (VA/MCR). Each department director and special assistant will ensure vulnerability assessments are conducted for their areas of responsibility with an eye toward OPSEC. In those areas where problems or possible problems exist, a management control review will be conducted. OPSEC, when possible, will be considered when reviewing or updating VA/MCR's.

8. Command OPSEC Committee. The OPSEC Committee will be composed of the OPSEC Officer, the ADP Security Officer and department/special assistant OPSEC coordinators. The OPSEC Officer will be responsible for ensuring the committee meets at least once semiannually and will be responsible for:

a. Providing advice and direction on OPSEC policy and implementation programs.

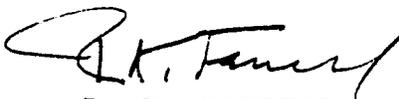
b. Evaluating command operations and activities which might require OPSEC review.

c. Determining the adequacy of the command OPSEC training and awareness program.

d. Reviewing current NETC policy and, if required, develop or update procedures and concepts for the improvement of OPSEC.

e. Preparing semiannual minutes for the Commander on the status of OPSEC.

9. Essential Elements of Friendly Information (EEFI). Essential elements of friendly information are those key questions about military capabilities likely to be asked by opposing planners and decision makers. They are critical facts about friendly operations and activities which reveal sensitive detail about capabilities and require protection from hostile intelligence collection and exploitation. EEFI can include classified, sensitive, and unclassified information. Appendix E is a list of EEFI's that apply to NETC. This list is also provided to assist in development of individual OPSEC plans.



R. K. FARRELL

Distribution
Lists A,B,C,D,E,F,G,and H

APPENDIX A

THREATS

1. The following are the general threats the command may face and corresponding OPSEC measures which may be of value:

a. The first general threat is theft. Hostile intelligence organizations, disaffected personnel, and criminals observe physical security practices to find vulnerabilities they can exploit to steal documents or material of value.

b. The second general threat is posed by intelligence organizations and criminals gathering personal data (indebtedness, weakness in character) on personnel assigned to NETC. Entrapment or recruitment of our personnel, (military and civilians), is possibly the single most dangerous threat to NETC's OPSEC success.

c. The third and most common threat is that of our personnel introducing information via statements, press releases, conversations, articles, letters and other such actions. Hostile intelligence organizations train their personnel in techniques of eliciting information during conversations (face-to-face and telephonic) by obtaining command newsletters, plans of the day, instructions, manuals and other readily available sources.

APPENDIX B

VULNERABILITIES

The following is a list of vulnerabilities known to be common to NETC. This list is provided to ensure all personnel are aware of its contents and to assist individuals in preparing a more detailed OPSEC plan where required.

1. Telephone Security. The telephone is an integral part of everyone's office. The handset of a telephone acts as a microphone, picking up and transmitting both electronic signals and normal volume conversations. These can be covertly monitored even when the receiver is on the hook. Furthermore, it is not uncommon for people to talk about sensitive information on unsecure telephones using "homemade" codes.
2. Communication Links. The transmission of sensitive information via radio telephone offers the adversary an excellent opportunity to exploit information. All personnel must be aware and alert to ensure information passed and received does not contain sensitive information. Appendix E will be used to assist with this determination.
3. Automatic Data Processing Security. Ambiguous and conflicting statements contained on Department of Defense and individual service's ADP security programs can lead to misinterpretation of requirements and result in questionable security procedures. Continuous involvement by the ADP Security Office is vital to the OPSEC program. Supervisors of work centers using ADP equipment are responsible for understanding and enforcing the ADP Security and OPSEC programs. They will further ensure assigned personnel attend required training in these areas.
4. Industrial OPSEC Program. A significant proportion of the support at NETC is provided by contractors. It is vital that the contractor have an effective internal industrial OPSEC program in place before sensitive data is developed by, or provided to, that contractor.
5. Public Affairs Officer. There is little specific guidance available to the information specialists who typically release information to the public. A sensitivity to OPSEC principles is important within the public affairs function. Any questions regarding sensitivity of any information may be confirmed or established by the OPSEC Officer.

6. Planning for System Installation (TEMPEST). Early consideration of TEMPEST requirements and involvement by the IRM Division is important prior to purchasing and installing any ADP equipment or system. TEMPEST and ADP security considerations are required when submitting an Abbreviated System Decision Paper (ASDP).

7. Increased Enforcement Capability (TEMPEST). Changing or re-locating previously TEMPEST certified systems, or replacing certain components without proper notification, violates the control designs, increasing the risk of compromising the security of the system used to process or transmit classified data. Any alteration or movement of a TEMPEST certified system of any type must be coordinated with the ADP Security Officer.

8. New Construction. The inclusion of security issues and consultation with security personnel is not always considered during new construction planning for government facilities. The OPSEC Officer and Security Officer must be included in initial preliminary planning of proposed facilities.

9. Carelessness. Trash receptacles can be lucrative sources of information. Sensitive operations can be disclosed by the improper disposal of sensitive paper waste such as unclassified messages or plans of the day.

10. Awareness. Lack of awareness of the hostile intelligence threat to NETC may cause employees to become careless in regard to their security responsibilities. Strict compliance with the OPSEC training and awareness program will ensure personnel are continually up to date on the potential of hostile intelligence threats.

11. Information Security Vulnerabilities. Some of the most common activities which, by their nature, could cause NETC personnel to be vulnerable to OPSEC violations are:

a. Failure to ensure that classified information is furnished or disclosed to only authorized persons.

b. Failure to provide a security review for security implications, or classification considerations, may result in inadvertent disclosure of classified information.

c. Assigning uncleared personnel to duties that may provide them the opportunity for access to classified information.

d. Failure to follow security classification guidelines on proper classification of data.

- e. Failure to ensure that NETC visitors are not exposed to classified information for which they may not have a need-to-know.
- f. Failure to maintain proper security at classified meetings and conferences.
- g. Failure to store classified information in approved security containers.
- h. Dissemination of classified or sensitive, unclassified data to personnel without the need-to-know.
- i. Failure to follow published security guidance or regulations.
- j. Failure to follow classification management procedures.
- k. Failure to properly protect classified and sensitive, unclassified hardware.

12. Physical Security Vulnerabilities. Even though the annual physical security survey is designed to identify and eliminate these vulnerabilities, personnel must be aware that the following actions are considered a breakdown of the NETC OPSEC program:

- a. Failure to maintain or enforce access controls into designated restricted areas.
- b. Failure to maintain strict lock-and-key accountability to facilities that contain a security interest.
- c. Failure to follow procedures for test and maintenance of intrusion detection system.
- d. Failure to follow established procedures in the control and movement of vehicles entering or leaving restricted areas.
- e. Failure to maintain a positive system of package, material, and property movement control into or out of security areas.
- f. Failure to comply with the physical security standards applicable to designated security areas.
- g. Failure to use authorized locking devices in accordance with the sensitivity of the item being protected.

13. Data Processing Facilities. Information stored in a computer system is vulnerable to a wide variety of hazards. The security controls must be based not only on security objectives, but also on all the vulnerabilities of the application. The following are examples that should be considered.

a. Human error could result in the accidental destruction, disclosure, or modification of sensitive and classified computer-based information. Incorrect, inconsistent, or unreasonable data may be accepted as valid for processing. It is also conceivable that computer facilities could be unsecured because of the failure to observe written security policy and instructions.

b. Individuals could process classified and sensitive data on ADP equipment which has not been approved or accredited for such operations through the intentional or inadvertent disregard of existing policy.

c. Computer transmission could be intercepted for the unauthorized disclosure of sensitive data.

d. Natural disasters, such as fire, flood, and electrical failures, could disrupt computer operations and result in the destruction of data and equipment; the possibility of human injury also exists.

e. Persons with unauthorized dial-in access may obtain access to the system, especially when remote dial-in-access is allowed.

f. Failure to downgrade or declassify ADP systems and admittance of facilities requiring maintenance.

g. Failure to properly secure computer facilities during nonoperational hours. Software containing classified or sensitive material should be stored in a locked security container appropriate to the classification level of material being safeguarded.

APPENDIX C

SAMPLE OPSEC PLAN

DATE:

OPSEC ANNEX TO: (enter program/event/project/department name)

Ref: (a) NETCNPTINST 3070.1A
(b) (other applicable references)

1. General. This annex provides guidance for the security planning and conduct of operations in support of: (define briefly the project/program, activity purpose, objective and classification).

2. Responsible for OPSEC. (Identify the project/program, activity, OPSEC POC and POC overall responsible for security.)

3. Hostile Intelligence Threats and Vulnerabilities. (Identify hostile intelligence threats or refer to NETC OPSEC Plan for description of hostile threats. If additional hostile intelligence factors are involved, identify here.)

a. Human Intelligence (HUMINT) Threat. (Identify HUMINT threats which your program/project will be exposed.)

b. Signal Intelligence (SIGINT) Threat. Outline in general terms all hostile communications intelligence (COMINT) and electronic intelligence (ELINT) capabilities which are a threat to the project/program.)

c. Imagery. (Outline hostile photo intelligence (PHOTINT), radar and sensory capabilities that are a threat to the project/program.)

d. Electronic Warfare (WE) Threat. (Provide an assessment of hostile EW capabilities and potential impact on the project/program.)

4. OPSEC Programs (countermeasures). (Outline the OPSEC and related measures taken to counter the threats described in paragraph 3 above. Appendices may be prepared if an exceptionally detailed description of one or more of these countermeasures is required. Otherwise, briefly describe countermeasures taken in the following areas):

a. Physical Security.

b. Information Security.

NETCNPTINST 3070.1A
17 AUG 95

- c. Signal Security.
- d. Intelligence.
- e. Others.

5. Essential Elements of Friendly Information. (List the specific aspects of the project/program which must be withheld from the enemy.)

6. A copy of (project/program name) classification guide, dated _____, is attached.

APPENDIX D

CONTRACTOR OPSEC

1. OPSEC measures are required of contractors when administrative, technical and physical actions they might execute could result in sensitive information being made available to them or outside sources.
2. The existence of the above situation must be determined prior to issuance of request for proposals (RFP's) or contract. To accomplish this, an OPSEC estimate will be prepared when a requirement to issue an RFP or contract involving classified or sensitive information is identified.
3. Care must be taken not to confuse requirements for OPSEC measures with requirements for information, physical, communications, or personnel security contained in industrial security regulations. These measures are required automatically of all contractors executing classified contracts.
4. A contract that requires the use of OPSEC measures may result in classification requirements and OPSEC being added to other existing or future support contractors if:
 - a. An indication of when and where certain activities will occur (i.e; tests, evaluations, meetings, etc.) can be targeted as a place, time or way of obtaining sensitive information.
 - b. The taking or distribution of photographs indicates classified features or approaches.
 - c. The publishing of ads, status reports or brochures reveals possible sensitive Department of Defense (DOD) information.
5. To ensure uniformity in the way OPSEC requirements are presented throughout the DOD, the following guidance will be followed:
 - a. Guidance will be appended to basic RFP's or contracts and labeled: "OPSEC REQUIREMENTS."
 - b. OPSEC guidance will include:
 - (1) Essential elements of friendly information pertinent to contractual activities.

NETCNPTINST 3070.1A
17 AUG 95

(2) Essential secrecy to be maintained, advantages expected from secrecy and a statement of harm if adversaries derive accurate estimates.

(3) OPSEC measures:

(a) Controls over technical and physical actions, in addition to encryption and TEMPEST, to keep indicators from appearing in detectable activities, such as electromagnetic or acoustic emissions and observable physical matters.

(b) Covers or other deceptions to explain harmless indicators that will result from actions necessary to execute contracts.

APPENDIX E

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI)

The following is a compilation of EEFI's that may have application to the type of classified or sensitive, unclassified activities conducted at NETC. This list is also intended to assist those activities with special projects or programs in developing their own EEFI list:

- . Weapons, sonar, communication, launcher, electronic, combat control descriptions, characteristics, capabilities, effectiveness and limitations.
- . Ship and aircraft operational employment schedules.
- . Operational predictions.
- . Sensitive test programs, concepts and philosophies that reveal military application.
- . Drawings and plans of sensitive equipment.
- . Lessor plans of capability and application of specific warfare areas.
- . Objective and defensive tactics.
- . Expert opinions as to the effectiveness of DOD systems.
- . Unclassified foreign and domestic open literature collections.
- 0. Specific nicknames or project members.
- 1. Background information or technological breakthroughs.
- 2. Date, time, location and name of platform where special equipment will be installed.
- 3. Information concerning protective measures (alarms, guards, patrol, etc.) being installed or applied to sensitive areas or programs.
- 4. Staffing requirements or responsibilities of key individuals that would indicate the nature, progress or status of a special program/event.

NETCNPTINST 3070.1A
17 AUG 95

15. Official travel plans, including itineraries, routes, purpose, etc., of certain key military personnel.

16. Disclosure of NETC capabilities or limitations.

17. Personnel reports, including manpower counts, shortages and hiring/firing actions.

18. Security plans, surveys and inspection reports.