



DEPARTMENT OF THE NAVY

NAVAL TRAINING CENTER  
2601A PAUL JONES ST  
GREAT LAKES, ILLINOIS 60088-2845

NTCGLAKESINST 5511.4G  
N3  
MAY 06 1999

NTC GREAT LAKES (SIMPLEX) INSTRUCTION 5511.4G

Subj: INFORMATION AND PERSONNEL SECURITY PROCEDURES FOR  
NAVAL TRAINING CENTER (NTC) STAFF

Ref: (a) OPNAVINST 5510.1H

Encl: (1) NTC Great Lakes Orientation Brief

1. Purpose. To establish procedures and assign responsibility for the implementation of the Information and Personnel Security Program at NTC Great Lakes.
2. Cancellation. NTCGLAKESINST 5511.4F. This instruction has been substantially revised and should be reviewed in its entirety.
3. Policy. All departments of NTC, Great Lakes (Simplex) shall become familiar with the Information and Personnel Security Procedures Program and its requirements. Creation and retention of classified material shall be minimized.
4. Procedures. In accordance with reference (a), the following procedures are established to minimize the creation and retention of classified material as well as to maintain control of classified material.

a. Incoming Classified Material

(1) Only the Security Manager, and/or Assistant Security Manager may accept incoming classified material.

(2) All incoming classified material will be given to the Assistant Security Manager for review. Classified material that is received as Registered Mail will be signed for by the Assistant Security Manager who will retain the material and a copy of the registered mail signature receipt. The Assistant Security Manager is responsible for the logging and distribution of all classified material. Upon receipt of classified material, the Assistant Security Manager will fill out an individual log control sheet (OPNAV 5216/20) assigning a control number for each and every piece of material using a basic number system. Log control sheets with essential information and a cover sheet indicating the level of classification will be placed on the documents. All classified material will then be delivered to the Chief of Staff, Operations via the Assistant Chief of Staff, Base Operations (N3) who will recommend distribution, retention and/or destruction. All classified material will then be returned to the Security Manager for appropriate handling as follows:

(a) Distribution. Distribution will be made by the Assistant Security Manager who will ensure routing is properly recorded on the log control sheet and will then personally deliver. All personnel in receipt of classified material will sign for custody of the

document(s) and will return all classified material to the command Security Manager or Assistant Security Manager for stowage. When classified information is no longer needed by the department/special assistant who has temporary daily custody, the material is to be returned to the Security Manager for retention or destruction.

(b) Retention. When classified material is identified for retention, the Assistant Security Manager will mark the log control sheet with the word "Retain" and will store in the classified safe. A copy of the log control sheet will be kept in a separate binder. Log control sheets should only use the unclassified title of material.

(c) Destruction. When classified material is marked for destruction, the Assistant Security Manager will stamp the log control sheet "Destroy" and retain a copy of log control sheet as a Record of Destruction. Witnesses will sign and date the control sheet upon destruction. No other destruction record is necessary.

b. Storage of Classified Documents

(1) Secret and Confidential material shall be stored in the command classified containers located in Room 237, Bldg 1.

(2) The Original Log Control Sheet (OPNAV 5216/20) and all other administrative records shall be stored in a separate container.

c. Outgoing Classified Correspondence. All classified outgoing correspondence will be under the direct control of the Security Manager. All drafts/working copies and typewriter ribbons shall be safeguarded (locked up) and destroyed when the correspondence is complete. All correspondence will be completed by using typewriters (not word processors.) All outgoing correspondence shall be controlled the same as incoming correspondence with regard to assignment of control numbers.

d. Routing/Checking Out Classified Material. Classified material will be hand carried only to those personnel who have access and a clear "need to know". All material will have signature receipts. When material is removed from its document folder, a signed record of check-out shall be placed in the folder.

e. Procedures for Incoming/Outgoing Personnel

(1) Incoming Personnel

(a) Reporting staff personnel who have no need for a security clearance require no action other than a review of OPNAV 5520/20 as part of orientation. (See enclosure (1)).

(b) Reporting staff personnel who have no previous security clearance/access, no record of a past security investigation and are filling a billet that requires a security clearance, must have a security investigation initiated immediately.

(c) Reporting staff personnel who have previous security clearances and are placed in a billet requiring a security clearance may be granted an Interim Clearance for 180 days until a final security clearance is granted by DONCAF. Additionally, they must review enclosure (1). In order to obtain a final clearance, an OPNAV 5510/413 must be completed and forwarded to DONCAF. If final clearance is not received five months after submission of OPNAV 5510/413 a tracer should be forwarded to DONCAF.

(2) Outgoing Personnel

(a) Outgoing personnel who are leaving the U.S. Naval Service via retirement/resignation/discharge who have had a previous security clearance and/or access must complete an OPNAV 5511/14 Security Termination Statement. This statement is placed in the service member's official record.

(b) Outgoing personnel who have no record of a security investigation/clearance or previous access and who are reporting to a billet identified in the member's orders as requiring a security clearance will require an appropriate level investigation be initiated prior to leaving the command with results forwarded to receiving command. Procedures are outlined in reference (a).

(3) Personnel Assigned TAD. Personnel assigned TAD requiring a secret clearance shall have their clearance indicated on TAD orders or have their clearance forwarded in accordance with reference (a).

f. Emergency Destruction Plan. This instruction addresses the requirement to safeguard and to destroy, in the event of hostile elements or a natural disaster, all classified information held in the command. All messages, regardless of security classification, will be designated for destruction as authorized in paragraph 17-6 of reference (a). Storage of classified material is in two locations: Building 1, Room 237 and Room 229 and Building 5, Retention Center. The threat or compromise of classified material is therefore minimal and the following emergency destruction procedures are considered adequate to prevent any loss or compromise of classified material.

(1) Authorization for Destruction. Emergency destruction will commence when directed by Commander, Naval Training Center (CNTC) or higher authority.

(2) Responsible Personnel. The safeguarding of classified information and the destruction thereof is the direct responsibility of the command designated Security Manager and may be delegated to the Assistant Security Manager.

(3) Procedures

(a) Minimal Storage Policy. In order to reduce the amount of classified material to a bare minimum, routine destruction is performed on an "as needed" basis. There is rarely any need to retain secret documents, and in the majority of cases a determination is made to immediately destroy. They are logged in and placed in a separate folder within the safe to await destruction as soon as possible (ASAP).

(b) To aid in the minimal storage policy an annual clean out day will be held on the first Tuesday of each June.

(c) Emergency Destruction. In the event of a natural disaster or civil disturbance, and when CNTC determines that sufficient protection cannot be provided for classified information in Buildings 1 and 5, all classified material will be evacuated to Building 1127 (Recruit Training Command). In the event that the emergency does not allow adequate time to transfer material to Building 1127, the shredder will be used in Room 237 to implement emergency procedures for destruction of all classified documents. In the event the Security Manager cannot be recalled for emergency destruction/evacuation, the CDO can obtain the safe combination for Building 1 Room 237 from the Assistant Security Manager. Alternate sites for emergency destruction of documents include Naval Criminal Investigative Service (Building 2). It should be noted that these sites are identified as destruction sites for all base elements. Established priorities could preclude timely destruction at these sites. Shredding in Building 1 should be considered the most practical alternative.

(d) Priority. In the event of emergency destruction the following priorities will be followed:

Priority One - Secret Material

Priority Two - Confidential Material

Priority Three - Unclassified Messages

(e) Drills. Emergency drills coordinated by the Security Manager will be conducted and documented annually to ensure that personnel are familiar with the plan and locations of safe and destruction equipment.

(f) Several security violations can result in the loss, compromise or possible compromise of classified information. Security violations are also caused by a failure to adhere to security regulations but does not result in a loss, compromise or possible compromise.

1. Loss, compromise or possible compromise.

(a) Discovery. Upon discovery of a loss, compromise or possible compromise the individual shall report to the Security Manager or Command Duty Officer after normal working hours. The Security Manager or Command Duty Officer shall notify NCIS and the Chief of Staff, Operations.

(b) Preliminary Inquiry. If NTC is the custodian of the loss, compromise or possible compromise the Security Manager shall initiate a preliminary inquiry within 72 hours.

2. Other Security Violations. Violations of security regulations other than those involving the loss, compromise or possible compromise of classified material will be investigated and corrected by the Chief of Staff, Operations. A Security Discrepancy Notice (OPNAV 5511/51) may be used.

(a) Unsecured Containers. If a container containing classified material is found unlocked in the absence of assigned personnel, the incident will be reported immediately to the Security Manager, Assistant Security Manager, or the Command Duty Officer. The container will be guarded until the duty officer or Security Manager arrives at the location of the unlocked container. The duty officer or Security Manager will then inspect the classified material involved, lock the container, and make a security violation report to the Chief of Staff, Operations. A Preliminary Inquiry shall be initiated.

(b) Improper Transmission. Upon receipt of classified material that has been improperly mailed, shipped, addressed, packaged, handled or transmitted, the Security Manager shall determine whether the material has been subjected to compromise. If circumstances indicate the classified material has been compromised, the Security Manager shall notify the sending command. When circumstances indicate the information was not

compromised, the Security Manager shall report the violation to the sending command using OPNAV 5511/51 (Security Discrepancy Notice).

5. Responsibilities

a. The Chief of Staff, Operations is responsible for the Information Security Program within this command. The Security Manager acts as his advisor and is his direct representative in all matters pertaining to the program.

b. NTC Security Manager is to be designated by CNTC, in writing, and is responsible for the following:

(1) Ensuring the requirements of reference (a) are met.

(2) Granting clearance and access to classified material, on a "need to know" basis.

(3) Coordinating control of incoming/outgoing classified material.

(4) Providing security briefings to personnel with access to classified material as required/needed.

(5) Storing all classified material in the security container maintained by the Assistant Security Manager. All classified material must be returned to the Security Manager prior to close of business each day.

(6) Conducting quarterly inventories and purging all non-essential classified material maintained by.

(7) Changing safe combinations, in accordance with reference (a).

(8) Conducting and coordinating annual emergency destruction drills.

## 6. Action

a. The CNTC shall designate, in writing, the Security Manager and Assistant Security Manager.

b. Security Manager:

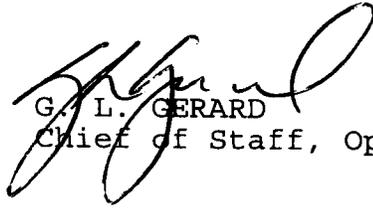
(1) Shall hold a mandatory security awareness briefing in June of each year for all NTC personnel regardless of whether they have clearance or not.

(2) Will be responsible for orientation (enclosure (1))

of each staff member upon check-in and will check out all staff members in regard to security status.

(3) Shall carry out provisions of this instruction and responsibilities as outlined in reference (a). All classified material shall be under his/her control.

7. Forms. All related forms are available through normal supply channels.



G. L. GERARD  
Chief of Staff, Operations

Distribution:  
NTCGLAKESINST 5216.5M  
LIST I

SECURITY ORIENTATION BRIEFING

The material presented in this enclosure has been abstracted for you from the U. S. Navy Security Manual (OPNAVINST 5510.1.1) and The Guide for Security Orientation Education and Training (ONI-63-2). The central aim of this program is "SECURITY-MINDEDNESS" in other words, impressing upon you the continuing importance of certain fundamental habits of security.

First, it must be pointed out that all personnel associated with the Naval Service, in any manner whatsoever, have a personal responsibility for maintaining the security of any classified matter of which they have knowledge. All persons have the obligation of controlling their own words and their own actions at all times and in all places. All such personnel, yourself included, are also requested to report to the proper authorities anything which might actually, or even possibly, reveal the improper release of classified information to persons not authorized to possess it. Careful and unceasing attention to this responsibility is an essential part of the services demanded of every individual by the United States Government.

"CLASSIFIED INFORMATION" is any official information, which must be safeguarded for the interests of national security. There are three basic categories of classified information:

1. Confidential.
2. Secret.
3. Top Secret.

Information, official or otherwise, is not classified unless it requires protective safeguarding in the interests of the security of the United States or its allies.

"For Official Use Only (FOUO)" is another term used within the Naval Establishment to indicate information that requires protection from unlawful dissemination. Such information, though not meeting the requirements for classified material, is of such a nature that it should not have unrestricted public dissemination -- like much of the information contained in your service record.

This information must be handled with the same respect that classified information deserves. It must be strongly emphasized that the unauthorized disclosure of any such information will not be tolerated.

U. S. ESPIONAGE LAWS

As part of your security briefing, you are required to read certain Criminal Statutes of the United States Code relating to defense information. Specifically, these are Sections 793, 794, 795, 796, 797, and 1001; Title 18, United States Code, and UCMJ Art. 106a. In these statutes, you are informed as to those acts which committed advertently or inadvertently are punishable by law. These statutes are found at the end of OPNAVINST 5510.1H; but, to assist you in remembering them, they are summarized as follows:

1. Communicating or giving to unauthorized persons any information relating to the National Defense.
2. Permitting such information in your custody to be stolen or destroyed through your own gross negligence.
3. Failing to report to your superior the known loss or destruction of such information.
4. Hiding or shielding any person whom you believe, or suspect, has taken, communicated to unauthorized persons, or lost such information; or who permitted any such information to be stolen or destroyed.
5. Making defective, in any manner, an article or material which is to be used for, or is in any way connected to, the National defense.
6. Damaging or destroying any building, property, or equipment used in connection with the National defense.
7. Taking, stealing, or damaging any property which is being made for, or which belongs to, the government.
8. Photographing or making any map or sketch of anything relating to, or which belongs to, the government.
9. Disobeying any order or regulation published by the Secretary of Defense, or his designated representative, which relates to the security or protection of any National defense plants.
10. Reproducing, publishing, selling, or giving away photographs, sketches, pictures, maps, or graphical representation of any military installation or equipment.

11. Possession of classified material, or material which would be detrimental to the United States except in the proper work area. This includes taking classified material to an individual's home without proper authorization.

12. Knowingly and willfully falsifying or concealing material facts.

13. Making false, fictitious, or fraudulent statements or representations.

That's the lot of them -- and just to show that Uncle Sam isn't kidding around, the culprit can be fined (not more than) \$10,000.00, or imprisoned (not more than) ten (10) years, or both, and shall, moreover, be thereafter ineligible to hold any office or place of honor, profit, or trust created by the Constitution or the laws of the United States. Think about it! That's a lot of "life, liberty, and pursuit of happiness" down the drain!

SECURITY MINDEDNESS - IT'S UP TO YOU!

While on duty, you, as a member of the Naval Service, are responsible for such security responsibilities in your office or space as may be assigned by your supervisor. You may not delegate this responsibility.

It is also your responsibility to safeguard classified information from unauthorized disclosure. This may be accomplished by constant reference to the clearance status and need-to-know requirement on the part of those persons being given access to the classified information under your control.

Classified information may only be disclosed to other individuals in the course of official activity after you have determined the clearance status of the other party, and then after determining that the person to be given access to the classified information concerned has an official "need to know", which necessitates such access. This procedure may often be relaxed somewhat if the person is known to you and is involved in a day-to-day working relationship with the material concerned. Once again, it is emphasized that the basic responsibility for safeguarding the security of classified information rests with each individual having knowledge of such information.

Even the most casual examination of the off-duty security obligations of all personnel of the Naval establishment reveals limitations upon the freedom of choice and action

by such employees in the conduct of their private lives. Discretion should be exercised when participating in public activities in which such participation would reflect adversely upon the Naval establishment. This is particularly true in cases where matters of National security are involved. An opinion, either expressed or implied, by a member of the Naval establishment may mistakenly be interpreted as the official position of the Navy in such matters. Participation in activities such as these must be avoided so as not to focus undesirable attention on military and Naval operations and its personnel. Nothing herein, however, should be construed as preventing Department of the Navy personnel from participation in elections, or local politics, as long as the activities do not violate the provisions of the Hatch Act, which governs political activity by government employees.

Another limitation is that which pertains to the keeping of personal diaries. No classified matter pertaining to the Department of Defense may be mentioned directly, indirectly, or by suggestion in personal diaries.

While the observation of these and other limitations are a part of the service for which you are being paid, a very real form of compensation is the justifiable pride and satisfaction which you are entitled to feel as the result of your unique contribution to the national security.

Discussion of classified aspects of your work should not be carried on at any military or civilian social gathering, even though all personnel present are cleared. Furthermore, classified material shall not be removed from the confines of the station, or from any activity, except when specifically authorized.

THE "I DON'T KNOW" HABIT -- "NEED TO KNOW" POLICY ONLY

Extreme care should be exercised with members of your family or your friends. They are not cleared. They have no "need to know", and, lastly, they have not been indoctrinated in the necessary safeguards required for the security V classified information. Develop the habit of saying, "I don't know." They will respect your desire to keep quiet. Only when you pretend to know something will your friends and family question you to satisfy their natural curiosities. Developing the habit of saying, "I don't know" is one of your best weapons in guarding against loose talk. It is not possible to provide each individual with a complete list of "do's and don'ts" as far as

security is concerned. However, there are two rules of thumb which will usually help in answering the questions: "Should I do this?" or "Should I say this?"

Rule 1: Could spies or traitors possibly learn anything from this?

Rule 2: Could this possibly help spies or traitors verify something that they already have ideas about or have guessed?

If there is the slightest possibility that the answer to either of these two questions might be "Yes", "Probably", or even "Possibly", the action should not be taken, or the statement should not be made. Remember: One of the personal restrictions that working with classified material requires of an individual is that conduct and speech must always be guarded.

It should be brought out that the goal of any good security education program is to teach military personnel the point that whenever and however a topic comes up which has even the most remote bearing on classified information, they shall automatically become alert, watchful, and on their guard against security slips.

#### THE TELEPHONE IS STRICTLY UNCLAS

Of particular importance is security and the telephone. A telephone has no security! There is a strict prohibition against discussing any classified information over the telephone. This is especially important because of the fact that a high proportion of Department of Defense telephone conversations are being transmitted through microwave transmitters, and such conversations can be easily and surreptitiously recorded and analyzed. The types of situations to be avoided when talking on the telephone are:

1. Allowing classified information to slip into conversations through carelessness.
2. Disclosure of classified information in order to expedite the completion of a "rush" project.
3. Use of codes, double talk, or attempts to talk around classified information. It should be noted that private codes and "talking around" classified matters present no real protection against the abilities of a trained analyst.

For example, you've all heard of wire taps: Whether legal, or not, they exist. Remember -- A telephone has no security!!

EVERYONE IS A POTENTIAL TARGET FOR ENEMY AGENTS!

ESPIONAGE. In novels, movies, and TV thrillers, espionage is generally shown as an exciting and fascinating theme. Often, the most adventurous and gripping stories are based on real-life incidents. However, these fictional or dramatized espionage stories seek only to entertain us. The real espionage operations by enemies of the United States has a far more serious purpose -- to destroy us. Every Navy employee is a potential target of espionage activities. The reason is that he either knows something that an enemy agent would like to know, or is regarded as a possible means of obtaining such information.

All Navy personnel must know how to recognize and defend themselves against possible attempts at espionage. They should also know exactly what to do if they suspect that such an attempt is being made to involve them or get information from them. More specifically, some of these attempts are as follows:

1. Attempts by representatives or citizens of communist controlled countries to cultivate friendships or to place personnel under obligation.
2. Attempts by representatives or citizens of foreign governments to:
  - a. Cultivate a friendship to the extent of placing them under obligation, which they would not normally be able to reciprocate, or by money payment or bribery to obtain information of intelligence value.
  - b. Obtain information of intelligence value through observation, collection of documents, or by personal contact.
  - c. Coerce personnel by blackmail, by threats against or promises of assistance to relatives living under their control, especially those in a communist country.
  - d. Appeal to personnel on a racial, nationalistic, or ideological basis.
  - e. Exploit personnel who may be disaffected or in personal difficulties.

f. Intimidate, harass, entrap, discredit, search, spy on, or recruit for intelligence purposes personnel traveling in communist countries.

g. Induce personnel to defect, or to induce those who fled from communist countries to redefect.

3. Attempts by Department of the Navy personnel to provide unauthorized services, information, or documents to anyone believed to be in contact with a foreign-intelligence service.

4. Attempts by persons living in communist countries to obtain information of intelligence value from personnel by correspondence (including pen-pal correspondence), questionnaires, ham-radio activity, Naval cachets (request to service postal covers), or other forms of communication.

5. If you ever have reason to believe that you are the target of any of the above-listed attempts at espionage, remembering and sticking to a few simple rules may actually save your life. Here they are:

a. Do not show that you are suspicious. Any marked or sudden change in your manner will alert an experienced agent. If you have been cordial and friendly before, do not switch suddenly to a distant or hostile attitude.

b. As soon as possible, tell the Security Manager or your Department Head or other proper authority about your suspicions. Do not tell anyone else.

c. The Security Manager will promptly report the incident to the proper authorities. These authorities may ask you to help in handling the case. If so, do only what they tell you no more, no less.

d. Do not try to investigate or "crack" the case yourself. This is a complicated job for trained professionals.

No matter how big or important an enemy agents mission might be, he/she usually gets his information piece-by-piece, item-by-item. In order to do this, he/she is always looking for individuals who will supply the bits and pieces because of carelessness, ignorance, weakness, or outright disloyalty.

Some employees whose regular duties do not involve the handling of classified duties, are inclined to think that they don't know anything of value to enemy agents. This is a serious error. To

repeat: Every employee knows something that an enemy would like to know.

It follows then, that all Navy personnel have a personal responsibility to defend the Naval Service and their country against espionage. This responsibility can be set by adhering strictly to a few simple habits of thinking and acting, on duty and off:

1. Be security conscious "every day" 24 hours a day.
2. Know and strictly observe all regulations affecting your duties, regarding the proper handling of classified papers and materials.
3. Never discuss classified information
  - a. with unauthorized persons.
  - b. over a telephone.
  - c. in any place where you might be overheard.
4. Always remember that a person's clearance for a certain category of classified information does not entitle him or her to knowledge of everything in that category. It only authorizes access to information he/she needs to know in order to perform his duties.
5. Avoid any kind of public or private conduct that enemy agents might use as blackmail against you.
6. Be cautious in all new friendships, especially if they develop out of strange and unexplained circumstances.
7. Avoid groundless or foolish suspicions. But -- if you feel there are good grounds for suspicion, report them immediately to your Commanding Officer, or other proper authority. Tell no one else.
8. Never attempt any "counterintelligence" work on your own. This is a complex and highly dangerous job that only trained experts can handle successfully.

BE SECURITY CONSCIOUS

In summary, the secure handling of vital defense information is essential to the accomplishment of the mission of the Navy. Security is, therefore, a crucial part of the responsibility of each individual, military, or civilian, in the Department of the Navy.

Effective security also requires that the handling of classified materials be managed in an efficient manner. Good management practices are of paramount importance in obtaining effective security control. If security needs are to be met, constant attention must be given to the way in which classified material is handled. Be continuously security minded!

Always remember that the Government of the United States is a freely chosen institution of the American people. As an American citizen and member of the Armed Forces, your unshakable faith and trust in your country and your service are essential to their strength. That same faith and trust are your strongest armor against the insidious and deceptive activities of enemy agents.

AN ENEMY AGENT IS INTERESTED IN ALMOST ALL AREAS OF MILITARY LIFE!

STATEMENT OF UNDERSTANDING

I have read and understand the NTC Great Lakes orientation brief contained in NTCGLAKESINST 5511.4F (Information and Personnel Security Procedures for NTC).

\_\_\_\_\_  
DATE

\_\_\_\_\_  
SIGNATURE