



DEPARTMENT OF THE NAVY  
JOINT BASE PEARL HARBOR-HICKAM  
850 TICONDEROGA ST STE 100  
PEARL HARBOR HI 96660-5102

JBPHHINST 5205.2  
JB00  
30 Jan 15

JOINT BASE PEARL HARBOR-HICKAM INSTRUCTION 5205.2

From: Commander, Joint Base Pearl Harbor-Hickam

Subj: JOINT BASE PEARL HARBOR-HICKAM OPERATIONS SECURITY PROGRAM

Ref: (a) DoD Directive 5205.02  
(b) DoD 5205.02-M  
(c) OPNAVINST 3432.1  
(d) ALNAV 056/10

Encl: (1) Information Security/OPSEC Indoctrination Briefing

1. Purpose. To provide supplemental guidance per references (a) through (d) and standardized procedures for the implementation of a quality Operations Security (OPSEC) Program within Joint Base Pearl Harbor-Hickam (JBPHH).

2. Scope. This instruction applies to all JBPHH and installation personnel. This instruction does not replace but is to be used in conjunction with references (a) through (d).

3. Background. References (a) through (d) provide policy guidance for the effective management of the Department of Defense (DOD) and Department of the Navy (DON) OPSEC Program.

a. OPSEC is a critical process for all Navy activities. The Department of Defense (DoD) and the Department of the Navy (DoN) has reaffirmed OPSEC practices must be followed in the daily application of military operations. The practice of OPSEC enables mission success by preventing inadvertent compromise of sensitive or classified activities, capabilities, or intentions at the tactical, operational and strategic levels. OPSEC processes provide JBPHH with the ability to identify critical information (CI), current vulnerabilities, risks due to its vulnerabilities, and countermeasure decision criteria to mitigate risks.

b. OPSEC is a core competency within information operations (IO). OPSEC processes provide an integrated conduit for protecting CI while disrupting, denying and degrading the adversary's attempts to gain an advantage. Proper utilization of OPSEC planning, tracking and execution provides an increased probability of success by preventing the timely aggregation and analysis of CI required for the adversary to disrupt friendly actions.

c. OPSEC is identified as one of three key components for achieving operational surprise. The other two components are security programs (physical security, personnel security, information systems security) and counterintelligence. The important distinction between OPSEC and the others is that OPSEC is an operations function, not a security function. As a function of operations, OPSEC belongs in daily activity planning and must continually be revisited as JBPHH's mission and plans continually transform.

d. Properly applied, OPSEC contributes directly to operational effectiveness by preventing CI such as the Navy's recruiting strategy from being obtained by adversaries. Excessive OPSEC countermeasures can degrade operational effectiveness by interfering with the required activities such as coordination, training and logistical support. The OPSEC process recognizes that risk is inherent to all military activities. Proper use of the OPSEC process will achieve a balance, maximizing information security, while minimizing the impact on operations and planning requirements. Each operation must be evaluated by JBPHH and the OPSEC planner to determine the most effective countermeasures for implementation as balanced against operational requirements, timelines and budget.

#### 4. Discussion

a. The goal is to establish and implement the best OPSEC policies, procedures, processes and guidance to enable sustained superior performance and cost effective protection of CI, people, operations, technology and sustainment. JBPHH shall institute and manage an OPSEC program relevant to protect the mission and resources. OPSEC shall be considered across the entire spectrum of JBPHH. OPSEC, Security, and Information Assurance programs shall be closely coordinated to account for force protection and the security of information and activities.

#### 5. Command Management/Responsibility

a. JBPHH Chief Staff Officer (CSO)/Installation Commanding Officer (ICO) are responsible for effective management and execution of the ISPS outlined in references (a) thru (d).

b. OPSEC Program Manager (OPM) is to be designated in writing and serves as CSO/ICO's principle advisor and direct representative in matters pertaining to OPSEC. The OPM will have insight to the full scope of the command's mission to properly manage the OPSEC program. The OPSEC Program Manager shall:

- (1) Be designated in writing.

(2) Have a SECRET clearance in order to have access to the Secure Internet Protocol Router Network (SIPRNET).

(3) Complete core competency OPSEC training and execute the applicable requirements in references (a) through (c), and will be a dedicated, qualified OPSEC individual assigned to develop and manage the OPSEC program.

(4) Establish a formal OPSEC Program per references (a) through (d) that incorporates the principles and practice of OPSEC focused on command involvement, planning, assessments, surveys, training, education, threat, resourcing and awareness. Coordinate and administer the JBPHH OPSEC program and provide oversight regarding the execution of Navy OPSEC policy, doctrine, instruction and organizational program implementation.

(5) Establish an account with the Operations Security Collaboration Architecture (OSCAR) program on SIPRNET. This program was developed as an interactive tool for conducting an OPSEC assessment and incorporates intelligence information with user-supplied settings that reflect the current command environment. Assessment results can provide the commander with a snapshot of the unit's current OPSEC posture (e.g., susceptibility to open-source adversary intelligence collection). Use of OSCAR annually will satisfy the annual assessment requirements as set forth in reference (a).

Pertinent Web sites

OSCAR: <https://oscar.dtic.smil.mil/oscar>.

OSCAR registration:

<https://register.dtic.smil.mil/wobin/WebObjects/RegLite?SiteID=OSCAR>.

(6) Determine command CI per references (a) through (c). CI that has been fully coordinated within JBPHH and approved will be visible and used by all personnel at JBPHH to identify information requiring application of OPSEC measures.

(7) Ensure contract requirements properly reflect OPSEC responsibilities and that these responsibilities are included in contracts when applicable per references (a) and (b).

(8) Conduct annual OPSEC self-assessments and surveys per references (a) through (c). Report completion of an assessment to BUPERS' OPSEC program manager and the Navy OPSEC Support Team (NOST).

JBPHHINST 5205.2  
JB00  
JAN 30 2015

The NOST is a subordinate element of Navy Information Operations Command (NIOC).

(9) Maintain a turnover binder and ensure OPSEC programs and plans are exercised or evaluated through regular assessments.

(10) Generate and submit an annual OPSEC program status report to BUPERS' program manager no later than 1 November each year. The report format is listed in table 1 of reference (c).

(11) Provide OPSEC orientation and awareness training to assigned personnel. Ensure OPSEC awareness training is conducted at least annually.

(12) Supplement the Program Review Checklist and OPSEC Assessment and Survey requirements listed in reference (b) with JBPHH specific guidance if needed.

(13) Ensure contracts and acquisition agreements include OPSEC guidance (e.g., mandatory policies and measures) related to programmatic information that may be publicly released. The systems commands will conduct a regular review of information released in the public forum (e.g., Web sites) to ensure compliance with ALNAV 056/10.

(14) Conduct regular reviews of publicly accessible processes and information on contractor and government sites to determine if the aggregation of information for major programs constitutes an OPSEC disclosure.

(15) Evaluate technological capabilities and solutions to reduce OPSEC vulnerabilities, prevent unclassified CI exploitation, employ aggregate OPSEC analysis, and generate relevant, cost effective countermeasures.

(16) Submit at least one suitable Navy candidate for the annual national OPSEC awards program to IOSS no later than 1 December of each year. Instructions for submitting the awards packages are located on the IOSS Web site:  
<https://www.iad.gov/ioss/department/national-opsec-awards-10021.cfm>.

(17) Act as JBPHH's representative regarding OPSEC matters.

(18) Maintain the central point of contact for JBPHH OPSEC program concerns.

c. Assistant OPSEC Program Manager. May be assigned per the requirements of reference (a), and take direction from the OPM in

JB00  
JAN 30 2015

providing support to the OPSEC program. The Assistant OPSEC Program Manager assists the OPSEC Program Manager in implementing the JBPHH OPSEC Program. The Assistant shares all responsibilities and requirements as the Manager. Assistants may be assigned as needed.

d. Human Resources - Government Civilians. OPSEC is a requirement throughout the hiring process and when a program's CI or associated indicators are subject to adversary exploitation or unacceptable risk per references (a) and (b). JBPHH shall impose OPSEC measures by:

(1) Determining what OPSEC measures and requirements are essential to protect CI for job advertisement.

(2) Establishing procedures to verify Position Descriptions (PDs) properly reflect OPSEC responsibilities and ensuring those responsibilities are included in the PD. CI should be determined using references (a) through (c).

(3) Ensuring publicly released documents do not reveal CI or indicators of CI. OPSEC program managers should review the PD prior to public release.

e. Human Resources - Contractors. OPSEC is a requirement throughout the contract acquisition process and when a program's CI or associated indicators are subject to adversary exploitation or unacceptable risk per references (a) and (b). Additionally, ensure and verify that contractors supporting DoD activities use OPSEC to protect CI for specified contracts and subcontracts. JBPHH shall impose OPSEC measures as contractual requirements by:

(1) Determining what OPSEC measures and requirements are essential to protect CI for specific contracts.

(2) Identifying those OPSEC measures in their requirements documents.

(3) Ensuring the GCA identifies those OPSEC measures and requirements in the resulting solicitations and contracts.

(4) Establishing procedures to verify contract requirements properly reflect OPSEC responsibilities and ensuring those responsibilities are included in contracts determined to have CI. CI should be determined using references (a) through (c).

(5) Ensuring publicly released documents and statements of work (SOW) do not reveal CI or indicators of CI. If OPSEC planning is

necessary in a contract, reflect the OPSEC requirements in the SOW. OPSEC program managers should review the SOW prior to public release.

f. Public Affairs. Unclassified, publicly available media and Web sites present a potential risk to personnel, assets and operations if inappropriate information is published on Web sites. Public Affairs Officer shall review command products for the following concerns:

(1) Unclassified, publicly available web sites shall not include classified material, "For Official Use Only" information, proprietary information, or information that could enable the recipient to infer this type of information. Personnel are reminded that all government information must be approved by the Public Affairs Officer for public release prior to posting to any Internet site.

(2) Unclassified, publicly available web sites shall not display personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers, or e-mail addresses which contain the individual's name. General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable. The names, telephone numbers, and personalized, official e-mail addresses of command or activity public affairs personnel and or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories. Guidelines for official Internet posts can be found in reference (d).

(3) Public affairs is an important tool in garnering public support, fostering community relations and helping with the success of Navy recruiting. Public knowledge of military operations is inevitable because of advanced technology and instant media coverage. Therefore, publicly accessible information must be considered from an adversary's perspective prior to publication where media attention is expected or desired. The need for OPSEC should not be used as an excuse to deny non-CI to the public.

(4) The use of social media for Navy Recruiting is growing tremendously, supported by initiatives from the administration, directives from government leaders and demands from the public. This situation presents both opportunity and risk. Navy personnel are encouraged to responsibly engage in the use of social media and social networking sites in an unofficial and personal capacity. Guidelines and recommendations for using social media technologies in a manner that minimizes the risk are located in <https://www.chinfo.navy.mil/socialmedia.html>, and the Chief

JBPHHINST 5205.2

JB00

JAN 30 2015

Information Office Guidelines for Secure Use of Social Media by Federal Departments and Agencies, version 1.0 (<http://www.doncio.navy.mil/Download.aspx?AttachID=1105>). If personnel have any questions regarding the appropriateness of information they intend to place on social media sites, they should contact the Command OPSEC Program Manager and Command Public Affairs Officer.

6. Action. The OPSEC Program Manager shall review and update this instruction as needed.



S. KEEVE

Distribution: <https://g2.cnic.navy.mil/tscnrh/JOINTBASEPEARLHARBOR-HICKAMHI/JBPHH%20Instructions/Forms/Instructions.aspx>



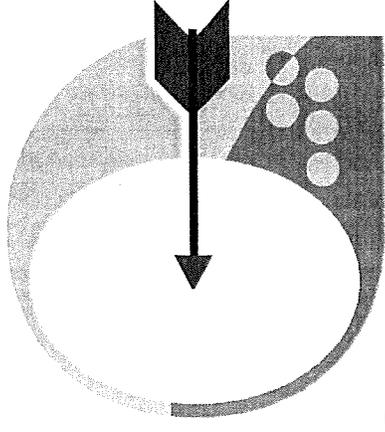
# Introduction to Operations Security (OPSEC)



Joint Base Pearl Harbor-Hickam

# Objective

- Understand the core of Operations Security (OPSEC)
- Define & identify targets and threats
- Establish countermeasures
- Identify the Critical Information Commandments
- Decipher the value of information



# What is OPSEC...?



- Have you ever taken precautions against

Someone...

- ...breaking into your house while you're on vacation?
- ...stealing your purse?
- ...stealing packages from your car while your shopping?
- ...fraudulently using your credit card?

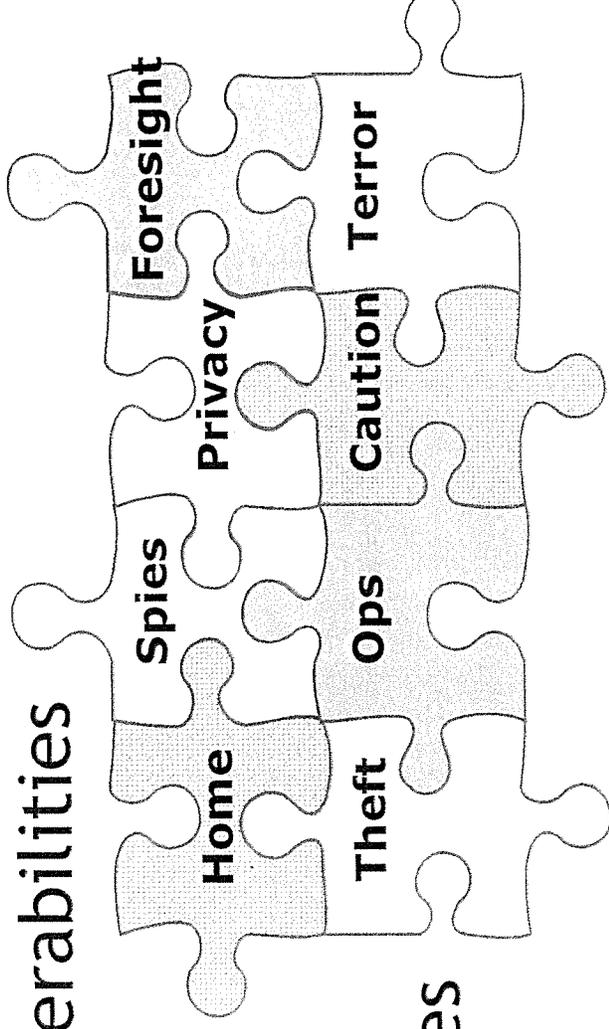
**Then you have used OPSEC!**

# What is OPSEC...?

- OPSEC is a risk management instrument that enables a manager or commander to view an operation or activity from the perspective of an adversary. It is a process of identifying, analyzing and controlling critical information.

# What is OPSEC...?

- Identify Critical Information
- Analyze Threats
- Discover Vulnerabilities
- Assess Risks
- Develop Countermeasures



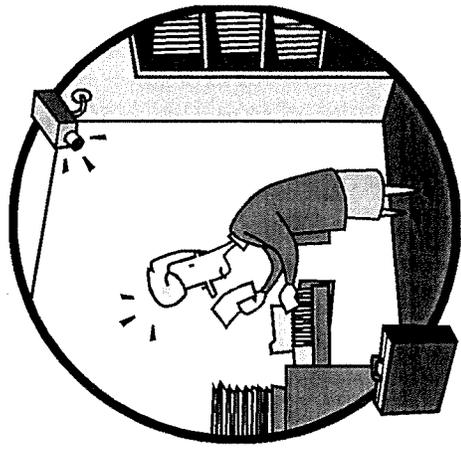
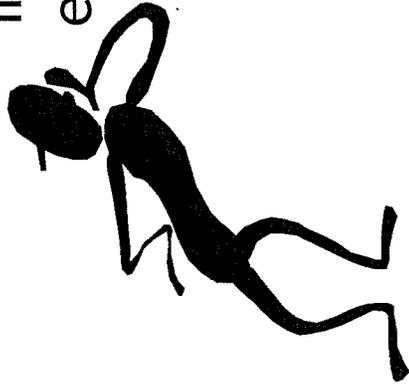
# What is OPSEC...?

- Identify Critical Information:

- Credit card numbers, travel dates, itineraries, passwords, patterns, changes in patterns, inspection results, information base systems, etc..

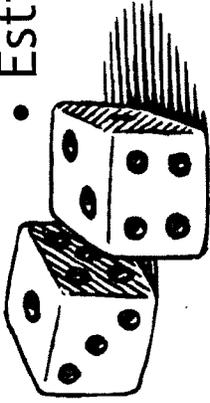
- Analyze Threat:

- Adversaries, Intelligence agencies - Open source information, corporate/state sponsored spies, eavesdropping, photographing, etc...



# What is OPSEC...?

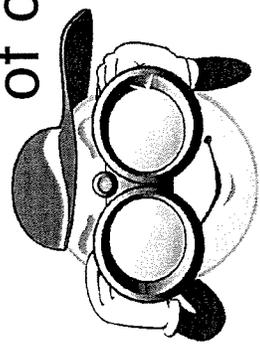
- Discover Vulnerabilities:
  - Flow of information, operations, timing of events, how an adversary would acquire the information, etc...
  - How would the loss of such data impact the organization?
- Assess Risks:
  - Estimated loss \$ x impact of risk x likelihood of risk = \$
  - Does the solution outweigh the loss?



# How Do I Identify Threats & Vulnerabilities...?



- Take note of suspicious behavior
  - HUMINT- “Task our students in the US with collecting information on the security of the facility where they are doing research. Then we’ll use one of our special teams to steal the chip.”



If you see something, say something

- Be consistent with the testing of systems
  - There is always room for improvement

# Critical Information Commandments...

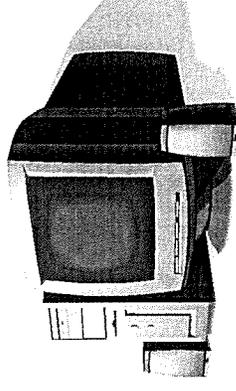
1. Thou must protect the information that the adversary needs to accomplish his mission.
2. Thou shall not try to protect everything.
3. Consider who thy adversaries are and what information they require to inflict harm to you.

# Critical Information Commandments...

4. Thou shall consult all sources of information to determine what thine enemies know about you.
5. Once thou has determined what information is critical, thou shall determine if that information is associated with thine activities.

# What Information Should I Protect...?

- Tactical information concerning intentions
- Scientific information regarding new technologies
- Military capabilities
- Commercial information on new technologies



## SECURITY BRIEF

1. Classified Information is any information or material that if allowed unauthorized disclosure could result in exceptional grave damage, serious damage, or could be prejudicial to the defense interests of the nation.
2. Access to classified information will be limited to the extent possible, to the minimum number of persons necessary to accomplish the mission, and will be based on need-to-know. Additionally, the level of the classification and the amount of information authorized for access will be limited to the minimum level and amount required to perform assigned duties.
3. A security clearance is a privilege, not a right. When you accept the privilege of access to classified information, you are also accepting the responsibilities that accompany this privilege. This is a lifelong responsibility
4. Need-to-know is the determination by an authorized holder of classified information that access to the information is required by another appropriately cleared individual in order to perform official duties.
5. Classified information is protected by concealing its contents from unauthorized disclosure. Classified material has to be stored, protected and used in secure areas.
  - a. Proper stowage will be according to classification. SECNAV M-5510.36 Para 10-19 records of destruction are not required for secret and confidential information except for special types of classified information, command policy may vary in different areas.
6. Any and all classified material must be marked to show the level of classification.
7. If you *find* unattended material that appears to be classified, notify someone, i.e., LPO, LCPO, Division Officer, etc., cover the material, do not scrutinize it. Turn it over to properly cleared personnel. If in fact this is a breach of security NCIS will be notified.
8. Classified material has to be protected during any type of transfer from one area or command to another in such a manner as not to disclose its content. Examples: transfer of classified material from one office space to another, a classified cover sheet must be utilized. When delivering or picking up classified information or Naval messages, 2 opaque containers must be used such as one manila envelope containing the information inside another manila envelope. The material inside a manila envelope carried in an attaché or briefcase. Carry your own; the servicing facility may not furnish them. Intermediate stops are not authorized, i.e., no chow; no gas. Do not handle classified material as normal information, if its content were for public viewing it would not be considered classified.
9. Classified material also has to be destroyed by authorized means, i.e., burning, shredding or mulching by authorized personnel following proper procedures. If you are involved in this evolution you will be thoroughly briefed on destruction policies.
10. Any breach of security must be reported, however insignificant it may seem. Keep in mind, if you use friendship; the buddy system, or any other reason as an excuse to keep from reporting a compromise or violation you and the party concerned have gained the right to join the 10X10 Club, \$10,000 and ten years of your life making little rocks out of big rocks in the red hot Kansas sun.
11. Any contact in any form with any citizen of a Communist controlled or hostile country must also be reported to NCIS or to your security manager. Contact means any form or encounter, association or communication including contact in person or by radio, telephone or letter or other forms of communications for social, official, private or any other reason.

12. Any attempt by an unauthorized person to solicit classified information must be reported. If you are financially embarrassed, living a disrupted life or have access to classified material, you become a prime target. Report to NCIS or your supervisor, give all details possible and do not discuss your finding thereafter with any unauthorized personnel.

13. All personnel granted eligibility for a security clearance by an adjudicating authority (DoD Central Adjudication Facility) are subject to continuous evaluation and are required to report to the security manager any information that could potentially affect an individual's eligibility to include oneself or others.

a. Standards of Conduct - The Guidelines

- 1) To maintain access, you must recognize and avoid behavior that might jeopardize your clearance.
- 2) Recognize behaviors in yourself or others that may need to be reported to your security officer and may signal that you or a co-worker may need assistance.
- 3) **Early intervention** is often the key to quick, effective resolution of problems without harming you or the organization.

b. Financial Considerations - Possible Red Flags

- 1) Don't pay your bills
- 2) Living or spending beyond your means
- 3) Don't file tax returns, tax evasion
- 4) Calls at work from creditors
- 5) Denial of credit
- 6) Bounced or bad checks
- 7) Failure to make child or spousal support payments
- 8) Bankruptcy

c. Misuse of Information Technology

- 1) Attempting to circumvent or defeat security or auditing systems.
- 2) Downloading, storing, or transmitting classified on or to unauthorized software, hardware, or information system.
- 3) Introduction, removal, or duplication of hardware, software, or media to or from any system without authorization.

d. The following security issues must be reported to the DON CAF:

- 1) Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the U.S. by unconstitutional means.
- 2) Foreign influence concerns/close personal association with foreign nationals or nations.
- 3) Foreign citizenship (dual citizenship) or foreign monetary interests.
- 4) Sexual behavior that is criminal or reflects a lack of judgment or discretion.
- 5) Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security clearance processing.
- 6) Unexplained affluence or excessive indebtedness.
- 7) Alcohol abuse.
- 8) Illegal or improper drug use/involvement.
- 9) Apparent mental, emotional or personality disorder(s).
- 10) Criminal conduct.
- 11) Noncompliance with security requirements.
- 12) Engagement in outside activities that could cause a conflict of interest.
- 13) Misuse of Information Technology Systems.

e. Self-reporting on your Personal Activities

- 1) Change in Personal Status
    - a) Marital status - married, divorced
    - b) Cohabitation - living in spouse-like relationship; intimate relationship, engaged
    - c) Change of name
  - 2) Foreign Travel
    - a) Security Office will provide State Dept advisories on hazardous conditions and any known security concerns.
    - b) Receive a defensive security briefing.
- f. Reporting Foreign Contacts
- 1) Must report contact with individuals of **any foreign nationality**, either within or outside the scope of your official duties, in which:
  - 2) Illegal or unauthorized access is sought to classified or otherwise sensitive information.
  - 3) You may be concerned that you are a target of an attempted exploitation.
- g. Reporting Financial Problems
- 1) Filing for bankruptcy
  - 2) Garnishment of wages
  - 3) Have a lien placed upon your property for failing to pay a creditor
  - 4) Eviction from a residence for failure to pay rent
  - 5)
- h. Reporting Arrests
- 1) Any, regardless of whether or not you were convicted or charges were dropped.
  - 2) Other Involvement with the Legal System: Target of legal action such as being sued. Possibility you might be required to discuss your job under oath.
- i. Psychological Counseling
- 1) Psychological treatment is reported unless it is for marital, family or grief counseling.
  - 2) Strongly encouraged and endorsed.
  - 3) Seeking help for routine life crises does not reflect adversely on an individual's judgment.
  - 4) Viewed as a positive sign that an individual recognizes that a problem exists and is willing to take steps toward resolving it.
  - 5) Does not jeopardize your security clearance.

j. So, I report a personal problem, then what? At some time in your life, you may face problems with inter-personal relationships, depression, alcohol, family issues, or similar difficulties. Vast majority of those seeking professional help do not suffer damage to their career. On the contrary, it enables one to get help with an unmanageable problem in order to get on with life. Early intervention is often a key to early resolution.

14. Operational Security (OPSEC) - Everyone, regardless of grade, rank, or position should be aware of OPSEC and its implications. Everyone shares in the responsibility of safeguarding our nation's security. You are a protector and can prevent the adversary from piecing together a picture of our nation's strengths and weaknesses.

a. What is OPSEC? How can it influence or apply to your work? Generally, OPSEC is all actions taken to deny the enemy information on friendly military operations and activities.

b. The essential elements of OPSEC are physical security, information security, signal security, and deception. The purpose of OPSEC is to deny the enemy sensitive information concerning planned, ongoing, and completed activities. You must safeguard both classified and sensitive unclassified information. The enemy employs three ways of gathering information: Human collectors; signals monitoring; and photography (to include use of satellites). To prevent the enemy from gathering sensitive information, we need to first identify our essential bits of information, whether or not they are classified or unclassified. Next, we need to determine the vulnerability of our activities or information to hostile scrutiny. Once that is done, we can implement countermeasures to safeguard these activities or information. This is done by the use of physical security, information security, signal security, deception, or simply understanding and implementing OPSEC.

c. OPSEC measures not only protect Combat Operations during time of crisis or war, but also prevent disclosure of logistical, personnel, training, research and development, and other administrative and support activities in Peacetime. Some of the areas that warrant applications of OPSEC principles are:

- 1) Research, development, testing and evaluation of military equipment, and doctrine.
- 2) Establishment of contracts with industry for the manufacture of U.S. Navy equipment.
- 3) Provisions of logistical support to friendly Armed Forces.
- 4) Preparation of articles for publication.
- 5) Administrative support for other commands.

b. No matter where you work, you are susceptible to enemy surveillance. We must safeguard our activities against hostile human intelligence, hostile signal intelligence, and hostile photographic techniques, to include satellites. During War or Peace, hostile intelligence services place a high priority on continuously gathering accurate and timely data on the U.S. and Allied Forces. To aid in that goal, they monitor our scientific and technical research and development to support their country's research or to counter ours. To keep that "edge" over our opponents, we employ the traditional security programs such as physical security, information security, signal security, and deception.

c. Security Precautions - If you look around any military reservation, you notice fences, guards, restricted areas, locks, security containers, and alarms, just to mention a few. These are the more overt means of physical security. Even though these are designed to deter or delay entry by unauthorized personnel, they can be breached. Therefore, we need to further protect our activities from these intruders or from those "few" among us who may be working for the other side. Every job on this base touches in some way or another sensitive information or activities. Any information that can "tip off" an individual about a certain project or key personnel is considered sensitive. To prevent this information from getting out, the following measures should be taken:

1) Information transmitted by telephone is not secure. The telephone system is one of the easiest channels to use for the collection of information.

"Discussion of classified information over non-secure circuits is prohibited. Official government communications systems and facilities, including official DoD telephones and telephone systems, are subject to COMMUNICATIONS SECURITY (COMSEC) monitoring at all times, and the use of such systems, facilities or telephones constitutes consent to COMSEC monitoring."

"DO NOT DISCUSS CLASSIFIED INFORMATION ON NONSECURE TELEPHONES. OFFICIAL DoD TELEPHONES ARE SUBJECT TO MONITORING FOR COMSEC PURPOSES AT ALL TIMES. DoD telephones are provided for the transmission of official government information. Use of official DoD telephones constitutes consent to COMSEC telephone monitoring in accordance with DoD Directive 4640.6."

a) Never discuss classified information on phone lines, even parts thereof. Do not talk around a classified subject; bits and pieces can readily complete missing parts to a puzzle.

b) All military lines should be answered properly, i.e., place of work, your name, this is a non-secure line, and may I help you please. This is an ALCOM requirement of 1983.

2) When you leave for the day, clear your desk. Don't leave important papers in or on your desk. Lock them in a file cabinet or security container. All classified material must be handled according to regulations.

3) During the day, you should not leave important or sensitive material open to view by anyone. Items such as shipping logs, strength or attrition reports, training directives, after-action reports, duty assignments, or even job descriptions are considered sensitive enough to protect against probing eyes. These are just a few of the items that an individual could collect to develop a description of a particular project.

4) As you leave for the day, ensure that your desk, file cabinet, security container, and door are locked. Be aware that when you talk about "sensitive" items in a public or unauthorized area you are a security leak. You are divulging information that could alert an agent about the sensitivity or status of a project or individual. Do not develop that bad habit of trying to impress others about the importance of your job. Any information, whether classified or unclassified, should only be released to someone if the individual has, first the need-to-know and also, the proper security clearance. If need be, verify the individual's need-to-know, clearance, and identity with his/her supervisor or appropriate security manager.

5) When you use phones or radios, beware of what you say. Pre-plan your calls or messages to avoid disclosing information. Use a STU-III secure, voice telephone for all your classified calls. For Unclassified calls, make your message short and informative and do not make any inferences to classified or sensitive subjects. A slip of the tongue could alert an agent to continually monitor your phone. The phones are monitored. Try to avoid classifying or categorizing projects as new or improved; this tells the sensitivity of that project. Simple things like duty assignments could also alert someone as to troop dispositions or status.

6) Before an article is submitted for publication, ensure the paper has not inadvertently disclosed sensitive or classified information. Have it proofread by security personnel.

7) Practice some form of deception as part of your OPSEC measures. Keep your projects or papers away from view. If your project is conducted outside, then safeguard it against ground and aerial (including satellite) surveillance. Try not to stereotype your behavior or actions, since a change in your status may indicate something of importance is or will be occurring. Try to vary your

routine for your projects or duties. Test or train at different times of the day. You may want to safeguard your activities with cover stories.

d. Responsibilities - From the mail clerk to the Commanding Officer, OPSEC measures should be followed and endorsed. Only you can prevent the leakage of information. Prevent items such as SOPs or policy documents from falling into the grasp of an alert agent. Safeguard your contract or effectiveness reports on new equipment or training. OPSEC is a continual process; make it a good habit. Also, be alert for suspicious activities or people disclosing sensitive material in an unauthorized area and report them to your supervisor or security manager. Report incidents such as:

1) Attempts by unauthorized individuals to obtain military information by any means.

2) Undue curiosity on the part of individuals about projects being conducted, security areas, security procedures, and key personnel.

3) Should you be approached for information, be non-committal. Try to break the conversation discreetly without arousing suspicion or concern. Remember any details about the individual and incident, and report them to the Security Manager or your supervisor.

e. In conclusion, you have the responsibility of safeguarding sensitive and classified information within your environment. Never discuss sensitive aspects of your job in public and remember - what you do at work stays at work.

"THINK SECURITY, THINK AMERICA"

I certify that I have read and thoroughly understand the contents of this document.

Date

\_\_\_\_\_  
Signature

Printed Name

Witnessed by:

\_\_\_\_\_  
Signature