



# The Safety Corner

From the Marine Corps Center for Lessons Learned

April 2010

## This Issue of the Safety Corner Highlights Operational Security

Inside this issue:		OSI Studied F-22 Pilot's Online Postings	7-8
Operational Security is...	1	Classification Guidance/Classification Markings	8-9
The OPSEC Process/Examples of Critical Information	2	Personal Identifying Information	10
How Information is Collected	3	For Official Use Only (FOUO)	11
Operational Security Guidance for Family Members	4	Marine Corps Short Narratives	12
Countermeasures/Operation Eagle Eye	5	Navy Short Narratives	13
OPSEC Quiz	6	Fatality Summary	14



### Operational Security is...

keeping potential adversaries from discovering our critical information. As the name suggests, it protects our operations planned, in progress and those completed. Success depends on secrecy and surprise, so the military can accomplish the mission quicker and with less risk.

**OPSEC is mostly common sense. If we all take the time to learn what information needs protecting and how we can protect it, we can continue to execute our missions effectively.**

During the Cold War, it was the communist threat. Today economic superiority and political gain are the driving forces, with new threats emerging everyday. Our current and former allies as well as our adversaries routinely collect information pertaining to a wide array of topics including technology. Some of this information is incomplete in and of itself. But when pieced together, the entire picture is formed and a vulnerability is exposed.

For more information see [MCO 3070.2](#)

### The OPSEC 5-step Process

- Identify** YOUR Critical Information
- Analyze** YOUR Threat
- Analyze** YOUR Vulnerabilities
- Assess** YOUR Risk
- Employ** appropriate Protective Measures



Log onto the Marine Corps Center for Lessons Learned Webpage.

NIPRNET <http://www.mccll.usmc.mil>

SIPRNET <http://www.mccll.usmc.smil.mil>

[Subscribe to MCCLL Products](#)

Please add MCCLL Safety Corner to your list of trusted addresses.

Director, MCCLL: C. H. Sonntag  
 Operations Officer: Major Joe Novario  
 Editor: William Richardson

[Do you have a safety story you'd like to share? We'd like to hear about it and inspire others.](#)



**1. Identify Your Critical Information**

What do you want to protect? Why do you want to protect it? Is it governed by a regulatory requirement? Can it be defined as sensitive but unclassified?

**Examples of potential critical information:**

- ◆ Travel itineraries
- ◆ Operational planning information
- ◆ Employee addresses
- ◆ Employee phone lists
- ◆ Budget information
- ◆ Entry/Exit security procedures

**2. Analyze the Threat**

Who wants the sensitive information? Is there more than one adversary? What is their objective? What will they do to get to your sensitive information? What methods will they use to get it?

**There are 2 elements of threat:**

- ◆ Intent
- ◆ Capability

**3. Analyze the Vulnerabilities**

How is your information vulnerable? How is it protected or not protected? Or is it properly protected?

**Examples of vulnerabilities:**

- ◆ Critical information posted on the Internet
- ◆ Non-secure communications

**4. Assess the Risk**

Is the risk great enough to do something about the threat? How would the loss of sensitive data affect your operations? What would be the cost of losing sensitive information?

**Risk is determined by analyzing three factors:**

- ◆ Threat
- ◆ Vulnerability
- ◆ Impact

**5. Develop and Apply Countermeasures**

What countermeasures will block access to your information? Adopt measures specific to your operation.

**Examples of countermeasures:**

- ◆ Limit web page access
- ◆ Shred sensitive hard copy
- ◆ Sanitize bulletin boards
- ◆ Monitor public conversations
- ◆ Do not use e-mail to discuss sensitive operations
- ◆ Training and awareness

**Examples of Critical Information**

**Department of Commerce**

It is important to remember that there are many more examples of critical information than those listed below.

- ◆ Deployments
- ◆ Technology
- ◆ Capabilities
- ◆ Exercises
- ◆ Participation in DoD exercises
- ◆ Missions
- ◆ Planned intercept missions
- ◆ Law enforcement support missions
- ◆ Major event support like the Super Bowl or Olympics
- ◆ Communications
- ◆ Frequencies and access tones
- ◆ Locations of resources
- ◆ Airplanes, vehicles, repeater sites, etc.



**OPSEC requires the active participation of every service member, regardless of his or her rank or job.**

## How Information Is Collected

Critical information is information on the core secrets of an activity, capability, or intention that, if known to the adversary, could weaken or defeat the operation.

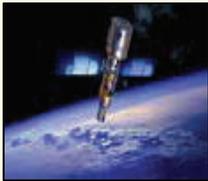
- ◆ Critical information is the information about your operations that adversaries need to achieve their goals.
- ◆ Critical information usually involves only a few key items.
- ◆ If those items are unavailable to us, they could impact the way we conduct business.
- ◆ Our critical information is information required to be successful in our jobs.

Information may be collected by monitoring telephone and public conversations, analyzing telephone directories, financial or purchasing documents, position or "job" announcements, travel documents, blueprints or drawings, distribution lists, shipping and receiving documents and even personal information or items found in the trash.

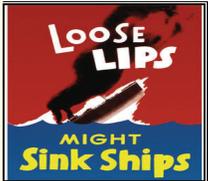
## Traditional Collections



Signals Intelligence (SIGINT) is the interception of electro-magnetic signals from telephones, faxes, computers, radios, and/or anything else transmitted in the open.



Imagery Intelligence (IMINT): Photographic imagery includes overhead photography by satellite or any other means, including individuals with cameras.



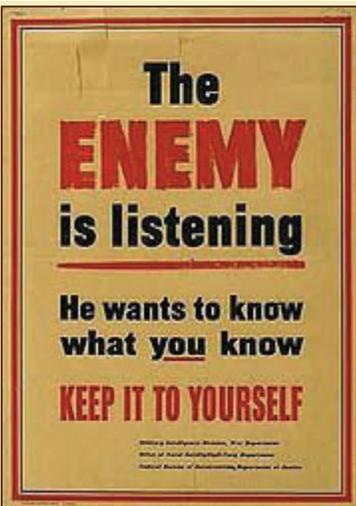
Human Intelligence (HUMINT): Traditional spy. Least likely means!



Open Source Intelligence (OSINT): In the world of secret services, OSINT means useful information gleaned from public sources, such as scientific articles, newspapers, phone books and price lists. Open source intelligence includes internet probes which are very effective. Adversaries are not the only ones interested in our e-mail. Sailors aboard USS *Cole* were shocked to find out that the personal e-mail messages they sent home to family and friends were forwarded to the media to be used as quoted material in news stories without their permission.

## Adversary

## Homeland Security



Who are we talking about? During World War II, it was the Axis powers (Germany, Italy, Japan, Hungary, Romania, and Bulgaria). In the Cold War days, you knew it was the communist threat. Today, the Cold War is over but new threats have emerged. Let's not focus strictly on terrorists right now. Remember that there are other adversaries, for example, foreign intelligence services that continue to collect information on us that could be used to hurt us in the future. We sometimes only focus on what just happened, but it is a certainty that our adversaries will continually look for and find any weak links.

Economic superiority and political gain are other driving forces. Our former allies during the Cold War and Desert Storm are now collecting technology from us to gain an advantage in the global marketplace.

### What are the capabilities of the adversary?

We can never underestimate the capabilities or strength of conviction of terrorists or any other adversary. Nothing is more dangerous than people who are willing to die for a cause.

**THE THREAT IS REAL**

As a family member of the military community, you are a vital player in our success and we could not do our job without your support. You may not know it, but you also play a crucial role in ensuring your loved ones' safety just by what you know of the military's day-to-day operations. You can protect your loved ones by protecting the information that you know. This is known in the military as, "Operations Security", or OPSEC.

**Unofficial Websites** The posting of pictures and information that is pertinent to your loved one's military unit to personal or family websites has the potential to jeopardize their safety and that of the entire unit. Coordinate with your unit's Family Readiness Officer and have pictures screened before posting to the "Official" Key Volunteer website. This will ensure that you contribute to OPSEC and keep the force safe.

**What Can You Do?**

There are many countries and organizations that would like to harm Americans and degrade US influence in the world. It is possible and not unprecedented for spouses and family members of US military personnel to be targeted for intelligence collection. This is true in the United States, and especially true overseas!



**1. Be Alert.** Foreign Governments and organizations can collect significant amounts of useful information by using spies. A foreign agent may use a variety of approaches to befriend someone and get sensitive information. This sensitive information can be critical to the success of a terrorist or spy, and, consequently, deadly to Americans.

**2. Be Careful.** It is very important to conceal and protect certain information such as flight schedules, ship movements, temporary duty locations and installation activities, just to name a few. Something as simple as a phone discussion concerning where you are going on temporary duty or deploying to can be very useful to US adversaries.



**3. Protecting Critical Information.** Even though this information may not be secret, it is what the Department of Defense calls "critical information." Critical information deals with specific facts about military intentions, capabilities, operations or activities. If an adversary knew this detailed information, US mission accomplishment and personnel safety could be jeopardized. It must be protected to ensure an adversary doesn't gain a significant advantage. By being a member of the military family, you will often know some bits of critical information. Do not discuss them outside of your immediate family and especially not over the telephone.

**The Don'ts of OPSEC**

**Don't:**

- |                                       |  |
|---------------------------------------|--|
| Discuss future destinations.          | Discuss future operations or missions. |
| Discuss dates and times of exercises. | Discuss readiness issues or numbers.   |
| Discuss specific training equipment.  |  |

**A Reminder About Common Sense On Social Networks**

**Paul Bove**



As the use and popularity of social networks continue to increase, an occasional reminder to use the Internet wisely couldn't hurt. A little common sense can help protect your reputation, as well as prevent potentially costly repairs to a virus-infected computer. We'd like to remind you and everyone online, of a few basics that can be helpful. If you have specific questions or issues, contact your local help desk for assistance.

- ◆ Don't click on a link you don't recognize, especially if it was sent to you via email.
- ◆ Don't post pictures or comments that might be embarrassing, or that might be in violation of UCMJ.
- ◆ Don't post information that could compromise OPSEC.

When it comes to internet activities watch what you say about your work. Shred paperwork with Critical Information that relates to your professional and personal business when it is no longer needed. Be careful not to compromise our Critical Information when talking on an unsecured phone, or in public about sensitive topics. We all have the responsibility to practice good OPSEC. By exercising caution, we protect our Critical Information, our mission, and most importantly lives.



Source: [Official Blog of the United States Air Force](http://Official Blog of the United States Air Force)

## Countermeasures



- ◆ Know your surroundings.
  - ◆ Ensure all people listening have a "need to know" of any information you could be talking about.
  - ◆ Don't talk shop while off duty. You could be giving out information to people that don't have a "need to know".
  - ◆ Use secure communication, Secure Encrypted Telephones, Secret Internet Protocol Router Network (SIPRNET) and others as appropriate.
  - ◆ Don't discuss critical information over unsecured phones or e-mail or in unsecured environments.
  - ◆ Don't try to talk around classified or critical information.
  - ◆ It's better to go talk to someone in person than to risk a disclosure of information.
  - ◆ Report the unusual.
  - ◆ Ensure all people in your work area belong. If someone is present that shouldn't be there, verify their credentials and make sure they are either escorted out of your work area or taken to the area they are trying to find.
- ◆ If someone you don't know is asking you questions concerning your job, the materials you work with or other information that makes you feel uncertain, do not answer! Seek guidance and report it!

## Shredding Documents

BB&T



When you put a piece of paper in the trash it can be difficult to know what happens to it. Since few people burn trash anymore, it is likely that your trash passes through several stages on its way to a landfill or incinerator. Every step that occurs once the trash leaves your control has risk that someone will find personal information they can use to cause you harm.

One way to safeguard personal information is to shred it before it goes into the trash. All documents that contain information in the categories of For Official Use Only, Privacy Act, or personal identifying information are required to be shredded.

For paper records, disposal methods, such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are acceptable.

### Electronic data files with personal information

Floppy diskettes and CDs should be shredded, destroyed or made unusable in some manner. Computer hard drives deserve special attention. Hard drives may have information on finances, taxes, user names, passwords and other information that should not fall into the

wrong hands. Deleting files and formatting a hard drive does not permanently remove the files from the system. Before disposing, recycling or donating a PC, the hard drive should be removed and physically destroyed.



## Eagle Eyes



"Eagle Eyes" is a suspicious activity reporting program. The program encourages people, on and off Bases and Stations, to participate and play an important role in deterring, detecting and defeating criminal or terrorist crimes.

Every citizen, military or civilian, can have a positive effect in detecting and defeating criminal or terrorist crimes. The Eagle Eyes program is an anti-terrorism initiative that enlists the eyes and ears of military members and citizens in local community.

If you observe any suspicious activity, anytime during the day or night, call PMO or the local authorities.

The foundation of the Eagle Eyes program is the education of military and local population about typical activities terrorists engage in prior to an attack. Armed with this information, you can recognize elements of potential terrorist activities when you see them.

Your involvement in the Eagle Eyes program is critical. Law enforcement relies on our citizen's participation as a means of detection and deterrence. You play a vital role in detecting, deterring and preventing acts of terrorism. It's your eyes and ears, your sense of why something is unusual or out of place, that can prevent acts of terrorism. After all, you are the expert on what activities do, or do not, belong in your neighborhood and community.

(continued)

## Eagle Eyes (continued)

Everyone on base and the surrounding community is considered part of the anti-terrorism team; as such you can report information 24 hours a day. Everyone is encouraged to stay alert whether at home, work or even while driving. Always keep an Eagle Eye out for suspicious behaviors such as:

- ◆ **Surveillance** - The act of someone recording or monitoring activities using camera equipment, taking notes, drawing maps or using binoculars or any other vision enhancement devices.
- ◆ **Elicitation** - Anyone or any organization attempting to gain information or in person about military operations or its personnel.
- ◆ **Test of Security** - Any attempts to measure reaction times to security breaches or to penetrate physical security barriers.
- ◆ **Acquiring Supplies** - Purchasing, or even stealing weapons, explosives, uniforms, vehicle decals and even Department of Defense identification media.
- ◆ **Suspicious Persons out of Place** - People who just don't seem to belong there. This could be the individual asking questions you know they do not have the need to know. An individual sitting outside the base perimeter fence in their car watching personnel entering and exiting the base.
- ◆ **Dry Runs** - Putting people in position and moving them about without actually committing a terrorist act.
- ◆ **Deploying Assets** - This would be the final behavior before the terrorist act. People and supplies are put in place to commit a terrorist act. This would also be your last chance to alert authorities before terrorism occurs.

By looking out for these suspicious activities, all base personnel will have a hand in preventing terrorist or criminal incidences from occurring on military installations and surrounding communities. If you observe any suspicious activity, anytime during the day or night, make note of it and call the PMO office located on your Base or Station or local authorities.

## OPSEC Quiz

OPSEC

1. The first "step" in the OPSEC process is:

- a. Assessment of the risks
- b. Application of the countermeasures
- c. Identification of the critical information
- d. Stop doing stupid things

2. OPSEC, as a methodology, originated in \_\_\_\_\_.

- a. The Korean War
- b. The Vietnam Conflict
- c. World War II
- d. The War of the Roses

3. "OPSEC" means:

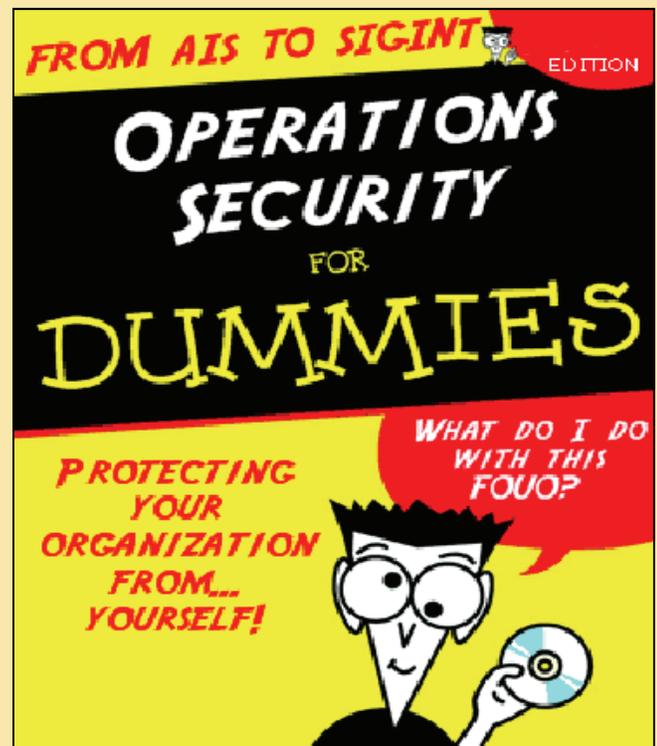
- a. Operations Security
- b. Optional Security
- c. "Oops" Security
- d. Overall-posture security

4. The \_\_\_\_\_ team was ordered into existence by \_\_\_\_\_.

- a. Purple Dragon, Admiral Ulysses Sharp
- b. Crouching Tiger, Captain Kangaroo
- c. Spartan II, Sergeant Major Avery Johnson
- d. Purple Dragon, President Reagan

5. Which of the following is an ILLEGAL method used by adversaries to gain info?

- a. Dumpster Diving
- b. Public Eavesdropping
- c. Asking Nicely
- d. None of the above



Answers on page 8

If you Google "Dozerf22", the screen name LtCol Michael Shower used on a popular online aviation forum, you'll find more than 600 links to Internet sites around the world that published his answers to detailed questions about sensitive but unclassified F-22 Raptor information.

Shower discussed topics ranging from F-22 lot numbers at different bases to Raptor vulnerabilities and software glitches, according to briefing slides that have spread rapidly across the Air Force.

The briefing grew out of an investigation into whether Shower illegally posted classified information. Even after he was exonerated of revealing classified details, a local unit of the Air Force Office of Special Investigations not involved in the investigation turned details of the inquiry into an example of an operational security violation.

Shower became an F-22 test pilot in 2002 at Edwards Air Force Base, Calif., and was anointed the first commander of the 90th Fighter Squadron at Elmendorf Air Force Base, Alaska, last May.

Building a reputation, Shower started posting on Web sites after he was designated an F-22 airshow pilot. He created quite a fan base, and garnered several comments like "That rocks..." or "awesome thread" following posts.

An F-22 discussion thread on FenceCheck.com, a site geared to aviation enthusiasts, regularly featured posts by Shower. That thread had 700 posts and received more than 68,000 hits before it was shut down. Forum users even posted Raptor photos with specific parts circled, asking Dozerf22 to identify them, according to the slides.

But the attention Shower received and the detailed information he posted did alarm some visitors, who wondered about the source of the questions. "Waaaay too many spies on this forum," one visitor wrote. After an unnamed person at Air Combat

Command reported Shower to OSI last December, the Secretary of the Air Force Acquisitions Security Detail launched an investigation into the squadron commander's online activities to find out if his posts were classified. Investigators concluded Shower did not release classified information, and he did not receive any disciplinary action.

Still, the OSI unit at Davis Monthan Air Force Base, Ariz., turned the probe into an unclassified briefing titled "Cyber OPSEC: An F22 Case Study," and presented it to the Davis Monthan Threat Working Group last month. The briefing provides details about the questions Shower received and the sensitive information contained in some answers.

The brief never uses Shower's name, but it includes a picture of him with only his face blocked out, and describes how easy it is to confirm his identity using his Fence Check login name, Dozerf22, which is almost identical to his call sign, Dozer.

Discuss: Will you be more cautious in online activities now? OSI spokeswoman Linda Card said the briefing was never intended to go past its initial presentation at Davis-Monthan, but admits it has been sent throughout the Air Force by threat working groups at other bases.

In an e-mail to Air Force Times, Shower said he was unfairly targeted by the briefing, and he made sure to answer only questions that had already been reported. "I only discussed items that were open source and available to the public," he said. "It is also why I did not answer many of the questions that were asked because they would have touched on issues that were not appropriate."

Two Pacific Air Forces officers, who asked to remain anonymous because of the story's sensitivity, said they were surprised a training tool would use a current commander as an example of inappropriate behavior. "How is he supposed to ever counsel an airman on OPSEC again" one officer asked.

Before the investigation, Shower was a model pilot with a career most dream of. An Air Force Academy graduate, Shower flew F-15Cs, including combat patrols over Iraq during Operation Northern Watch. He also engaged two Mig-29 Fulcrums of the Serbian Air Force on the first night of Operation Allied Force over Serbia in March 1999 while helping escort a wave of F-117 Nighthawks.

The briefing slides Air Force Times obtained listed some of the questions Shower received in the exact form they appeared on various message boards. They also pointed out how many posters used poor English, insinuating that technical Raptor questions came from foreign users.

"I have a question and if it is sensitive I'm sure someone will let me know..." reads one question in the briefing, "but looking at the actuator blister fairings, especially on the vertical inboard fins, that are diamond shaped, how the heck do they move without impacting the skin?" asked one user, according to the slides. "I have two small questions for Raptor and JSF, and I would be very gratitude if you would like to give me some answers," began another.

Shower said he understood that he couldn't check the background of each user who asked a question on the message board and contends that is why he was so careful in answering them. It's unclear exactly which questions Shower answered since details of the investigation haven't been made public, and the discussion thread on Fence Check has been deleted.

But the briefing slides say Shower's answers dealt with "thrust vectoring," "what specific doors and flaps do," "weapons systems operational details," "fuel figures and weight impact on performance," "status of radar upgrades," "compatible missile systems," "confirmed and denied performance rumors" and "aircraft lot numbers at different bases."

(continued)

## OSI Studied F-22 Pilot's Online Postings (continued)

Shower's Fence Check discussion is not an isolated incident, said retired Air Force Col. Tom Ehrhard, a senior fellow at the Center for Strategic and Budgetary Assessments. Since the Cold War ended, OPSEC has eroded, especially with the advent of the Internet. Now it is easier for airmen to slip up and post information they shouldn't on blogs, message boards and social networking sites.

For instance, message boards are ripe with B-2 information and speculation about what caused the recent crash on Guam, he said. Web site editors for online forums such as Fence Check and F-16.net said they continue to monitor their sites for potentially classified information and understand their sites could

be targeted by counter-intelligence agents looking for airmen to mistakenly post service secrets.

"We only share information that is already in the public domain, and carefully vet posts that might cross that line. We won't allow photos of military planes with opened panels, for example, or the posting of flight schedules and/or deployment dates," said Roger Kemp, Fence Check's editor.

Jon Somerville, an editor for F-16.net, said his site does all it can to make sure operational security violations don't occur, but due to lack of training, it can be an almost impossible task to ensure the site is completely clean.

"Sometimes we do see material posted which is a clear violation of the OPSEC rules," Somerville said via e-mail to Air Force Times. "This content is modified and a message sent to the forum poster. Fortunately this happens very rarely and usually as a result of a mishap which has just occurred."

Shower confirmed he stopped posting on message boards by request from his leadership and warned other airmen to be extremely careful about what they write online. "Anything you say can come back to haunt you and everyone must be aware of that," Shower said.

(Source: [AirforceTimes](#))

### Answers To Quiz From Page 6

- |      |  |
|------|--|
| 1. c | <b>5 of 5</b> You're an OPSEC master, even your parents don't know your real name! |
| 2. b | <b>4 of 5</b> Almost perfect...  |
| 3. a | <b>3 of 5</b> Not Bad, you understand OPSEC.                                       |
| 4. a | <b>2 of 5</b> You're getting there- just remember, OPSEC's all in the wrist        |
| 5. d | <b>1 of 5</b> Want a Rolex? \$20.  |

## Classification Guidance

Executive Order 12356 is the only basis for classifying information except as provided by the Atomic Energy Act of 1954, as amended. It is the policy of the Department of the Navy to make available to the public as much information concerning its activities as possible, consistent with the need to protect the national security.

Unnecessary or higher than necessary classification will be avoided. If there is reasonable doubt about the need to classify information, it will be determined by an Original Classification Authority (OCA). When there is reasonable doubt about the appropriate level of classification, the information will be safeguarded as if it were classified at a higher level until an original classification authority makes a determination.

Classified material will be physically marked, annotated, or identified by other means. The purpose of marking classified material is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading and declassification actions. Therefore, all classified material must be marked in a manner that leaves no doubt about the level of classification assigned to the material, which parts contain or reveal classified information, how long the material must remain classified and any additional measures necessary to protect the material.

### Basic Markings

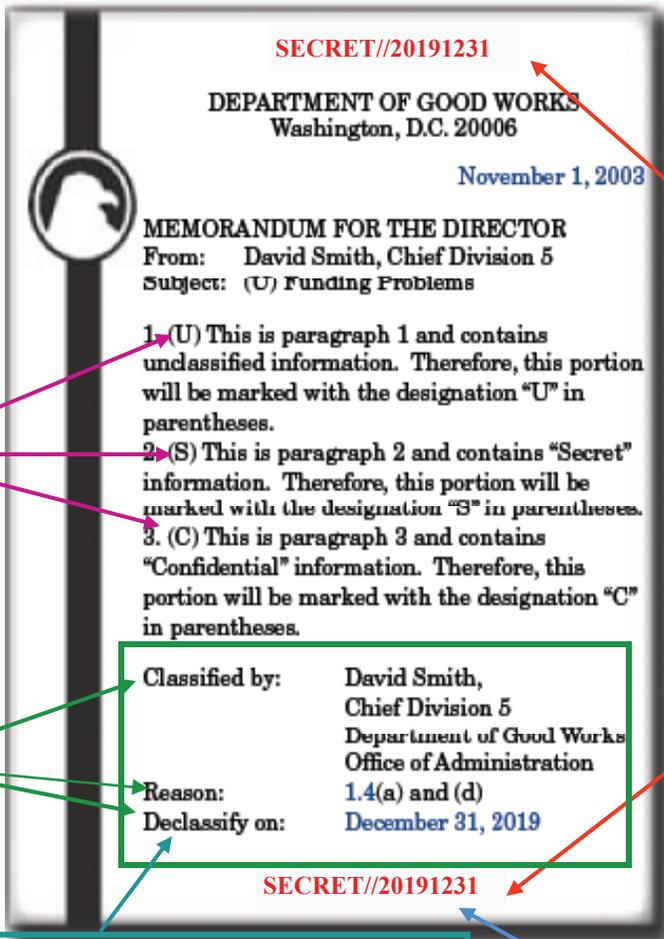
Classification markings will be stamped, printed, or written in capital letters, larger than those used in the test document or conspicuously on other material, and when practical, in the color red. Markings are required for all classified information, regardless of the medium by which it is revealed, with the following exceptions:

- ◆ An article which has appeared, in whole or in part, in newspapers, magazines, or elsewhere in the public domain, will not be marked, controlled or restricted in any manner while it is being reviewed and evaluated for comparison with classified information. The results of the review and evaluation, if classified, must remain separate from the article in question.
- ◆ Classified material will not be marked if the markings themselves would reveal a confidential source or relationship not otherwise evident in the material.
- ◆ A declassification date or event, or the notation Originating Agency's Determination Required (OADR), will not be applied to material which contains, in whole or in part, Restricted Data or Formerly Restricted Data.
- ◆ Classified correspondence to foreign governments, or their embassies, missions or similar official offices in the United States, will be marked only with the overall classification. Copies of the correspondence held by U.S. commands must carry all of the required markings.

(Source: [CSMR](#))

# Classification Marking

This classification marking system, used in conjunction with EO 12958, as amended, and ISOO Implementing Directive No 1 marking guidance, prescribes a standard set of markings to be applied to information. The example below depicts each component of the required markings.



Portion markings must be included

Overall page markings must include the overall classification, any caveats that apply to the document, and the declassification date

Examples:  
SECRET//20191231  
SECRET//NOFORN//20191231

Originally classified document

A derivatively classified document would have the following:  
Derived from: (replace Classified by:)  
Declassify on:

Required date format:  
YYYYMMDD

## Classification Categories

US Classification	Non-US Classification
TOP SECRET (TS) SECRET (S) CONFIDENTIAL (C) UNCLASSIFIED (U)	NATO
	Joint Classification

SCI Control System	Special Access Program
HUMINT (HCS) COMINT (SI) TALENT KEYHOLE (TK)	

## Foreign Government Information Markings

## Non-Intelligence Community Markings

SPECIAL CATEGORY (SPECAT)  
 SENSITIVE INFORMATION (SINFO)  
 LIMITED DISTRIBUTION (LIMDIS)  
 EXCLUSIVE DISTRIBUTION (EXDIS)  
 NO DISTRIBUTION (NODIS)  
 SENSITIVE BUT UNCLASSIFIED (SBU)  
 SENSITIVE BUT UNCLASSIFIED NOFORN (SBU-NF)

## Dissemination Controls

AUTHORIZED FOR RELEASE TO (REL TO)  
 CONTROLLED IMAGERY (IMCON)  
 FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)  
 FORMERLY RESTRICTED DATA (FRD)  
 KEYRUT  
 ORIGINATOR CONTROLLED (ORCON)  
 RISK SENSITIVE (RSEN)  
 USA/\_\_\_\_\_ EYES ONLY  
 NON-SCI SOURCES AND METHODS INFORMATION (SAMI)  
 RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL (RELIDO)  
 UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI)  
 CAUTION-PROPRIETARY INFORMATION INVOLVED (PROPIN)  
 DEA SENSITIVE (DSEN)  
 FOR OFFICIAL USE ONLY (FOUO)  
 FRONTO  
 NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN)  
 RESTRICTED DATA (RD)  
 SEABOOT

This document is unclassified. Classification markings are for training purposes only.

## Personally Identifiable Information



Personally Identifiable Information, or PII refers to information that can be used to distinguish or trace an individual's identity.

- ◆ Person's name
- ◆ Social security number
- ◆ Biometric records

**Personal data could be but is not limited to:**

- ◆ Financial, credit, and medical data
- ◆ Social security number
- ◆ Birthdates
- ◆ Family data
- ◆ Security clearance level
- ◆ Home addresses and telephone numbers
- ◆ Mother's maiden name; other names used
- ◆ Drug test results and the fact of participation in rehabilitation programs
- ◆ Family data
- ◆ Religion, race, national origin
- ◆ Performance ratings

### The loss of PII has major implications:

- ◆ Can erode confidence in the government's ability to protect information
- ◆ Can impact our business practices
- ◆ Can lead to major legal action

### Different methods that PII is stored and disseminated:

- ◆ On Hard Drives
- ◆ On Portable media
- ◆ On Paper documents
- ◆ On E-mail

More detailed guidance can be found at [HQMC PII](#)

## Ten Rules To Protect Personal Information

1. **DO NOT** be afraid to challenge "anyone" who asks to see Privacy Act information that you are responsible for.
2. **DO NOT** maintain records longer than permitted under records disposal.
3. **DO NOT** destroy records before disposal requirements are met.
4. **DO NOT** place unauthorized documents in Privacy Act record systems.
5. **DO NOT** commingle information about different individuals in the same file.
6. **DO NOT** transmit personal data without ensuring it is properly marked. Use "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE."
7. **DO NOT** use interoffice envelopes to mail Privacy data.
8. **DO NOT** place privacy data on shared drives, multi-access calendars, the Intranet or Internet that can be accessed by individuals who do not have an official need to know
9. **DO NOT** create a new system of records without first consulting your Privacy Office or CNO.
10. **DO NOT** hesitate to offer recommendations on how to better effectively manage privacy data.

### BOTTOM LINE

If you collect it...you must protect it

If in doubt...leave it out

Just because you've always handled personal information one way...doesn't mean that is the best- way.

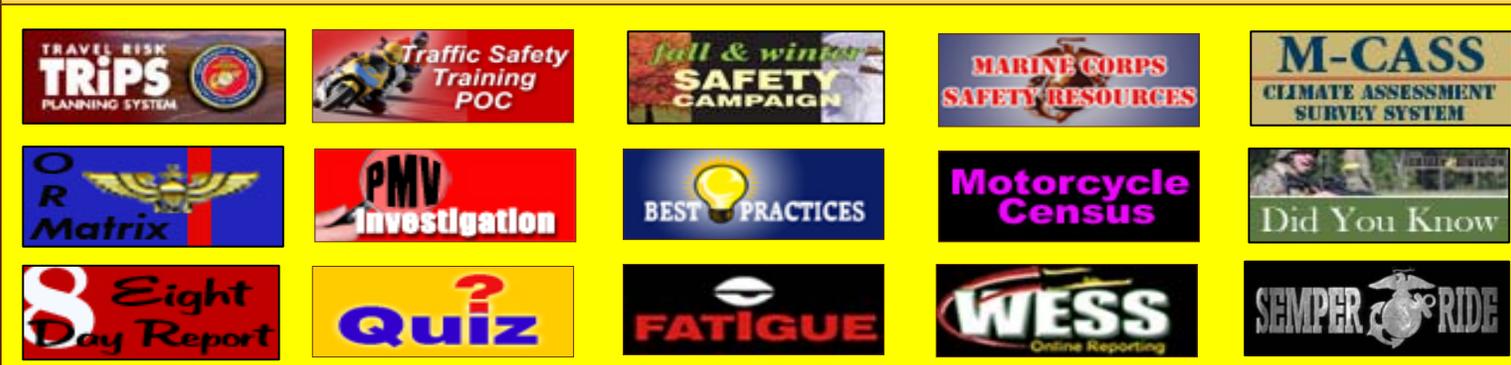
For Official Use Only (FOUO) is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA):

- ◆ Information which is currently and properly classified.
- ◆ Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)
- ◆ Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- ◆ Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision-making process and contain subjective evaluations, opinions and recommendations.
- ◆ Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
- ◆ Information that has not been given a security classification, may still be withheld from the public because disclosure would cause a foreseeable harm, is to be marked with "For Official Use Only" caveat as stipulated in DoD 5400.7-R, the Freedom of Information Act. **Examples of documents to be marked FOUO include unclassified unit after action reports (AAR) and other lessons learned type documents.**
- ◆ Unclassified documents that containing FOUO information shall be marked "For Official Use Only" at the bottom on the outside of the front cover (if any), on each page containing FOUO information, and on the outside of the back cover (if any). Each paragraph containing FOUO information shall be marked as such.
- ◆ Distribution of For Official Use Only (FOUO) documents are limited to DoD Components and between officials of DoD Components and DoD contractors to conduct official business for the Department of Defense. Per [MARADMIN 336/08](#), emails that contain FOUO information must be digitally signed and encrypted. DoD websites that contain FOUO information are required to be CAC card protected.

All personnel have the responsibility to ensure that no information that might place our service members in jeopardy or that would be of use to our adversaries is posted to websites that are readily accessible by the public. Although not a finite list, such information includes, among other things, technical information, operational plans, troop rotation schedules, position and movement of U.S. Naval Craft, description of overseas military bases, vulnerability of weapons systems or discussion of areas frequented by U.S. personnel overseas.

[DoD 5400.7-R](#), DoD Freedom of Information Act Program, describes exemption and guidelines for the types of information that may qualify as FOUO. As with classified information, it is the originator's responsibility to identify and mark information that may be FOUO.

## Popular Places



**USMC AVIATION CLASS A MISHAPS**

29 Oct 09 (California) AH-1W crashed into water after midair collision. (2 Fatalities)

26 Oct 09 (Afghanistan) AH-1 and UH-1 crashed in open desert. (4 Fatalities)

**USMC GROUND CLASS A**

20 Mar 10 (Camp Lejeune, NC) Lcpl died as a result of injuries sustained while participating in a command-sponsored boxing session.  
05 Mar 10 (MCAS New River, NC) Civilian employee checked out boat from marina to conduct a routine maintenance check ride and never returned.

22 Dec 09 (Afghanistan) LCpl died while performing maintenance on a M88 when hoist chain broke causing vehicle to fall.

03 Dec 09 (Camp Pendleton, CA) Cpl died when parachute failed to open while conducting low level static line jump.

**USMC OPERATIONAL MOTOR VEHICLE**

18 Mar 10 (Jacumba, CA) LCpl died when the GOV in which he was a passenger ran off the road and overturned.

14 Mar 10 (Afghanistan) Cpl died in a MRAP mishap when the vehicle rolled over while he was in the turret gunner position.

04 Nov 09 (Camp Pendleton, CA) LCpl died in automobile mishap when his POV was hit by HMMWV.

**USMC PRIVATE MOTOR VEHICLE FATALITIES**

28 Mar 10 (Summerton, SC) LCpl died in an automobile mishap when tread separated from tire causing vehicle to swerve into the median, roll and strike a tree.

18 Mar 10 (San Diego, CA) Two LCpl's died in an automobile mishap when the vehicle crashed through a guardrail and into a canyon.

15 Mar 10 (Mobile, AL) Cpl died in motorcycle mishap when he struck a curb and was thrown from the bike.

13 Mar 10 (Atlanta, GA) LCpl died in an automobile mishap after being struck head-on by drunk driver traveling the wrong direction on the freeway.

27 Feb 10 (Kapolei, HI) E-5 died in a motorcycle mishap when he collided with the vehicle in front of him.

05 Jan 10 (Camp Lejeune, NC) PFC died in a single vehicle mishap.

27 Dec 09 (Westport, CT) SVM was passenger in auto that lost control/struck tree.

18 Dec 09 (San Diego, CA) Cpl died after being struck by an automobile in a hit and run mishap.

08 Dec 09 (Kailua, HI) Sgt died in a motorcycle mishap.

26 Nov 09 (Morongo Valley, CA) LCpl died when the vehicle in which he was a passenger overturned several times. Two other SVMs were hospitalized.

14 Nov 09 (New Brunswick, NJ) SSgt died 23 Nov 2009 from injuries sustained as a passenger in an automobile mishap.

06 Nov 09 (San Diego, CA) Sgt died in a motorcycle mishap when he collided with another vehicle.

27 Oct 09 (New Bern, NC) PFC died 03 Nov from injuries sustained in automobile mishap when vehicle rolled and struck a tree.

17 Oct 09 (Murrieta, CA) SSgt died in a motorcycle mishap when he collided with a vehicle that pulled out into his lane of travel.

13 Oct 09 (Santa Clara, CA) Sgt died in a multiple vehicle mishap.

09 Oct 09 (Escondido, CA) LCpl was in a minor two vehicle mishap and was being treated by emergency medical personnel at the scene when he was struck and killed by a third vehicle.

01 Oct 09 (New Bern, NC) PFC died in an automobile mishap after he struck the back of a school bus that was stopped at a railroad crossing.

**USMC OFF-DUTY/RECREATIONAL FATALITIES**

03 Apr 2010: (Port Barre, LA) LCpl died in a recreational boating mishap.

28 Mar 10 (Fallbrook, CA) LCpl found unresponsive after a night of drinking.

24 Dec 09 (Monroe, NY) Marine vomited in his sleep, did not wake up and died of asphyxiation.

09 Dec 09 (Albuquerque, NM) PFC was found deceased in private residence

06 Dec 09 (Havelock, NC) Cpl died from a gunshot wound to the chest.

**USN AVIATION CLASS A MISHAPS**

28 Oct 09 (Corpus Christi, TX) T-34C did not return from VFR training flight. (2 Fatalities)

**USN AFLOAT CLASS A MISHAPS**

19 Feb 10 CPO electrocuted working in auxiliaries room.

16 Feb 10 (Key West, FL) PO2 died while conducting a training dive evolution.

28 Nov 09 PO1 reconnecting piping interface in AUX 2 touched 440VAC panel.

**USN SHORE CLASS A MISHAPS**

03 Dec 09 (Portsmouth, VA) Civilian employee died after falling from roof of building.

**USN PHYSICAL TRAINING CLASS A MISHAPS**

19 Feb 10 (Port Hueneme, CA) PO2 died during PT run.

16 Feb 10 (Kuwait) PO1 died following a PT run.

09 Feb 10 (Ventura County, CA) MCPO found dead in barracks after morning PT.

05 Dec 09 PO3 died after fall from treadmill.

14 Oct 09 (Norfolk, VA) PO1 died while participating in command departmental PT.

**USN PRIVATE MOTOR VEHICLE FATALITIES**

10 Apr 2010: (Bremerton, WA) SN died in a single-vehicle mishap when the automobile struck a Jersey barrier and pole.

05 Apr 2010: (Jacksonville, FL) SN died in a motorcycle mishap.

13 Mar 10 (San Diego, CA) ENS died in an automobile mishap after being thrown from the vehicle. Alcohol, speed and seatbelts are the initial factors.

20 Feb 10 (Snoqualmie, WA) PO2 died after head-on collision with another vehicle.

11 Feb 10 (Washington, MO) PO1 died in a single vehicle mishap when automobile overturned and SVM was ejected.

03 Jan 10 (Chicago, IL) Seaman died in automobile mishap.

26 Dec 09 (Fresno County, CA) SVM S-bound on interstate in heavy rain, lost control of auto.

28 Nov 09 (James City County, VA) SA died in an automobile mishap. Two other SVMs sustained non life-threatening injuries.

14 Nov 09 (Pensacola, FL) MCPO died in a motorcycle mishap when he was struck head-on by a drunk driver.

16 Oct 09 (San Diego, CA) CDR died 25 days after being hit by a truck while riding his bicycle.

13 Oct 09 (Chesapeake, VA) PO2 died in a motorcycle mishap. PO2 on second motorcycle is in critical condition.

11 Oct 09 (Oahu, HI) PO2 died in a motorcycle mishap when he lost control and collided with oncoming traffic.

05 Oct 09 (Holden, MA) PO3 died in a single motorcycle mishap when he struck a tree.

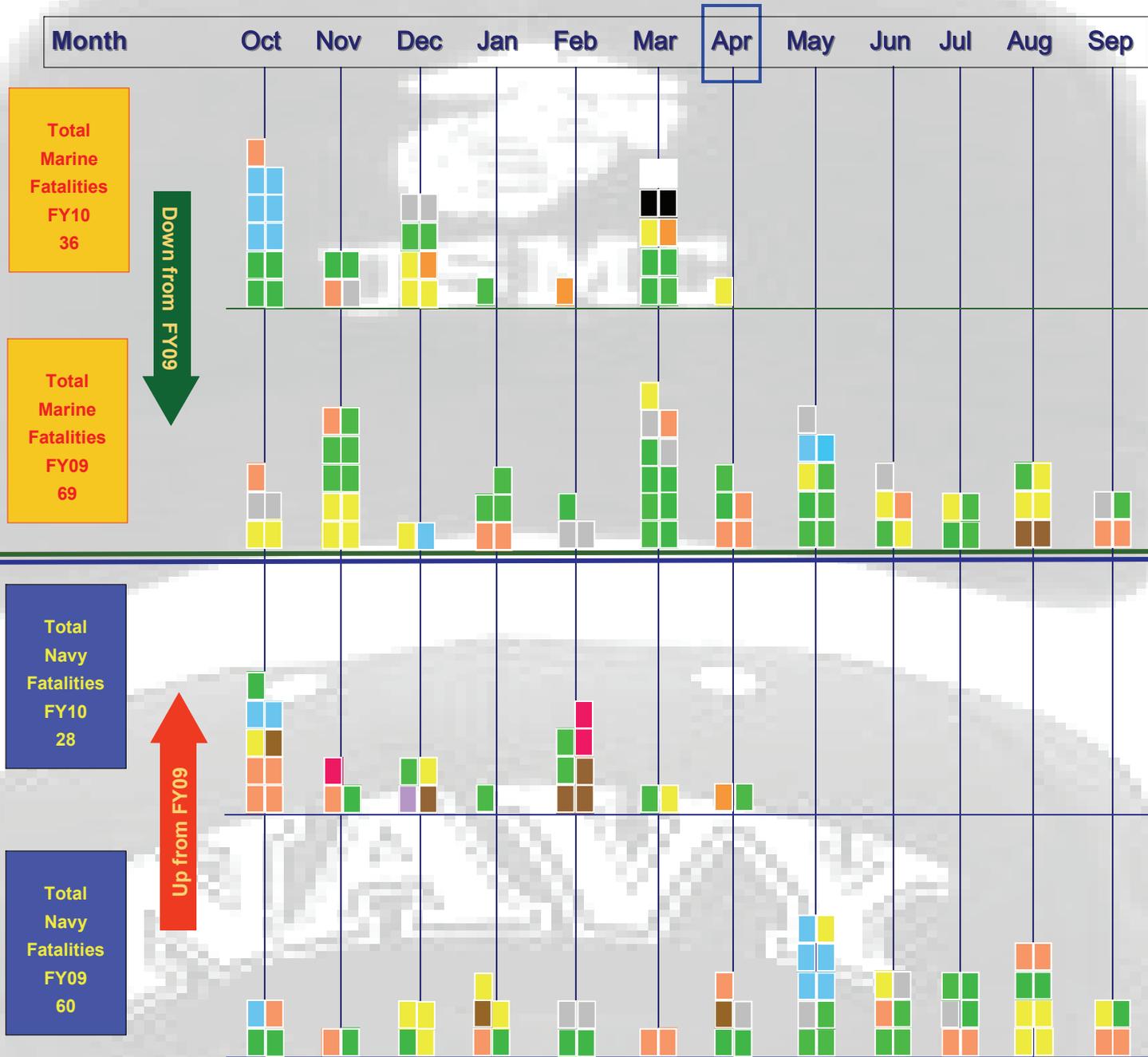
01 Oct 09 (Chocowintiny, NC) PO2 died in a motorcycle mishap when he lost control and then struck an oncoming vehicle.

**USN OFF-DUTY/RECREATIONAL FATALITIES**

09 Dec 09 (Norfolk, VA) PO3 died in an off-duty ATV mishap.

12 Oct 09 (Wahiawa, HI) PO2 died in a recreational parachuting mishap when his primary and reserve parachutes failed to open.

# Fatality Summary as of April FY10



Ground	PMV	GOV	Aviation	Motorcycle	Off Duty/Recreational	Shore	PT	Afloat	Training/Operational
--------	-----	-----	----------	------------	-----------------------	-------	----	--------	----------------------

Note: This report has been compiled from publicly available information and is not official USMC policy. Although information has been gathered from reliable sources the currency and completeness of the information reported herein is subject to change and cannot be guaranteed.