DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO

5510
Ser N09N2/9U223112

MAY 07 2009

From: Chief of Naval Operations

Subj: INTERIM POLICY CHANGES, REMINDERS AND CLARIFYING GUIDANCE TO SECNAV M-5510.36

Ref: (a) SECNAV M-5510.36

Encl: (1) Interim Policy Changes, Reminders and Clarifying Guidance to SECNAV M-5510.36
(2) Document Review Worksheet
(3) F. Bennett email of 23 Mar 09, "Rating Element - Management of Classified Information"

1. Enclosure (1) contains interim policy changes, reminders and clarifying to guidance provided in reference (a), and are effective immediately pending an update. Some changes and guidance stated in enclosure (1) is specific to Navy only. We are coordinating with Headquarters, U.S. Marine Corps (USMC), Plans, Policies and Operations (PP&O), Security Division (PS), to obtain the USMC equivalent guidance to incorporate in the next revision to reference (a). Enclosure (2) provided for your use in recording sampling results for the policy change noted in enclosure (1), paragraph 2b. Enclosure (3) is a reminder for compliance with paragraph 2-1.5h of reference (a), and is restated in enclosure (1), paragraph 2a.

2. The information contained in this policy memo does not replace other existing policy letters related to the Department of the Navy Information Security Program or Navy Telecommunications Directives issued by Commander, Naval Network Warfare Command, in coordination with this office, since issuance of reference (a).

3. Addressees are requested to disseminate this information to subordinate activities. It will also be posted to our website at www.navysecurity.navy.mil.

4. The CNO (N09N2) point of contact is Bridget A. Ouellette at (202) 433-8842, DSN 288-8842, or bridget.a.ouellette@navy.mil.

B. M. JACKSON
Assistant for Information
and Personnel Security

Distribution:
SECNAV
CNR
OGC

Subj: INTERIM POLICY CHANGES, REMINDERS AND CLARIFYING GUIDANCE TO SECNAV M-5510.36

NAVY JAG
CMC (PPO)
CNO (DNS-34)
COMUSFLTFORCOM
COMPACFLT
COMUSNAVEUR-COMSIXFLT
COMUSNAVCENT
COMUSSOCOM
COMNAVAIRSYSCOM
COMNAVSEASYSCOM
COMNAVFACENGCOM
COMSPAWARSYSCOM
COMNAVSUPSYSCOM
COMNAVRESFOR
BUPERS
COMNAVDIST
CNIC
DIRSSP
ONI
COMNAVLEGSVCCOM
USNA
NAVPGSCOL
NAVWARCOL
BUMED
PRESINSURV
COMNAVSPECWARCOM
COMOPTEVFOR
NAVHISTCEN
FLDSUPPACT
COMNAVSAFECEN
NETC
NAVCRIMINVSERV (CODE 11)
NAVY IPO

INTERIM POLICY CHANGES, REMINDERS AND CLARIFYING
GUIDANCE TO SECNAV M-5510.36

1. Chapter 1 - Introduction to the Information Security Program:

a. Change paragraph 1-4.12a to read: Headquarters, U.S. Marine Corps, Plans, Policies and Operations (PP&O), Security Division (PS), is responsible for implementation of the Information Security Program within the U.S. Marine Corps, based on guidance outlined in this manual. All requests for interpretation of regulatory guidance, waivers and exceptions of the DON ISP are appropriately coordinated with CNO (N09N2) via CMC (PS).

2. Chapter 2 - Command Security Management:

a. Reminder: Compliance with paragraph 2-1.5h (See enclosure (3)).

b. Add to last sentence of paragraph 2-11.1: Providing the results of a command review (i.e., assist visit, program review of specific focus area(s), or self inspection) to CNO (N09N2) will help facilitate oversight responsibilities. Therefore, echelon I and II commands shall submit the results of their review to CNO (N09N2), no later then 30 working days after the end of each fiscal year, and ensure it also includes the following, at a minimum.

1. Total number of inspections conducted (to include each subordinate command, if applicable).

(a) Include the name of each subordinate command.

2. Significant trends (positive and negative).

3. Corrective action(s) and anticipated completion, if significant security weaknesses identified.

4. Challenges (i.e., policy constraints, resource issues, etc.).

(a) This information may already be inclusive in items 2 and 3 above. If not, it shall be included.

5. Total number of security violations (i.e., Preliminary Inquiries (PI) and Judge Advocate General Manual (JAGMAN) Investigations).

(a) Further define the portion of the total resulting from Electronic Spillages (ES) (i.e., Total PIs 12. 10 out of 12 were result of ES).

6. Conduct random sampling of originally (if applicable) and derivatively classified documents at various times throughout the fiscal year to ensure compliance with marking requirements in Chapter 6. Documents are defined in paragraph 6-1.4. Commands shall use enclosure (2) to document the marking sampling, to ensure consistency throughout the Department of the Navy. (Note: The Information Security Program Data Report (SF-311) collected annually and reported to the Information Security Oversight Office is a separate requirement.)

(a) The requirement to conduct random sampling only applies to commands that have significant classification activity. Significant is defined as 100 or more. Commands with less then 100 are still encouraged to conduct a sampling to assess compliance with marking requirements.

(b) Summary of results shall include total number of documents sampled, percentage of each type of discrepancy outlined in enclosure (2), and actions taken to improve marking if there is an error rate of at least 20% (Note: this may be covered in items 2 and 3 above). Breakout the summary of results by originally and derivatively classified documents.

7. Confirm the requirements of SECNAV M-5510.36, paragraph 3-3.1a through d have been met and paragraph 4-6, as applicable. If not, advise of anticipated completion date.

8. Confirm requirements of SECNAV M-5510.36, paragraph 5-4 have been met. This applies only to Original Classification Authorities (OCAs) with security classification guides. Contact the RANKIN Program Manager at (202) 433-8861 or DSN 288-8861 for assistance, if needed.

3. Chapter 3 - Security Education:

a. Guidance to assist with compliance with paragraph 3-3.1a and b: Minimum training requirements are outlined in "32 CFR Parts 2001 and 2004, Directive No. 1; Final Rule," Section 2001.71.c.1 through 3, which is available at http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.html. Training for OCAs can be found at www.navysecurity.navy.mil (under Classification Management) and for both OCAs and derivative classifiers at https://dssacdsws.dss.mil/index.htm (under Information Security Courses). Also, by means of access to the Secure Internet Protocol Router Network (SIPRNET) individual's have the capability to originally (only if an OCA) and derivatively classify information. OCAs and derivative classifiers are required to be trained prior to exercising their authority, per Chapter 3-3. Training will help facilitate proper classification decisions and reduce the proliferation of electronic spillages.

4. Chapter 5 - Security Classification Guides:

a. Add to paragraph 5-3.1, before the last sentence: OCAs shall provide the DoD Security Classification Guide Data Elements (DD Form 2024) to CNO (N09N2) with each submission of new, revised or cancelled SCGs.

1. Note: The above guidance will also be included in the update to the OPNAVINST 5513.1 series.

b. Change the first sentence to paragraph 5-3.3 to read: The OPNAVINST 5513 series contains lists of individual SCGs for systems, plans, programs, or projects related to the overall subject area of the instruction.

5. Chapter 6 - Marking:

a. Exhibit 6C (Equivalent Foreign Security Classifications):

1. Add: Singapore equivalent is same as the United States for Top Secret, Secret and Confidential, with Restricted equal to our For Official Use Only.

2. Change: Spain equivalents are as follows: Top Secret is Secreto, Secret is Reservado, Confidential and Other remain as stated in the exhibit.

6. Chapter 9 - Transmission and Transportation:

a. Definition for "domestic" cited in paragraph 9-3.7, first sentence: The definition of domestic in the context of domestic contracts, per the DoD Blanket Purchase Agreement (BPA) for FEDEX and UPS carriers, includes the Continental United States (CONUS), Alaska, Hawaii, and the Commonwealth of Puerto Rico.

7. Chapter 10 - Storage and Destruction:

a. Add after the last sentence to paragraph 10-3.1a(2): Open storage areas constructed per exhibit 10A shall be designated in writing by the Command Security Manager (CSM).

b. Add new sub-paragraph to 10-3: 6. Controlled Access Areas (CAA) and Restricted Access Areas (RAA) shall be designated in writing by the Command Security Manager (CSM). Designation of a CAA or RAA shall comply with the requirements in the Information Assurance (IA) Publication 5239-22, "IA Protected Distribution System (PDS) Publication." It is a designation that the physical security standards

for a CAA or RAA have been met. It is not certification of the PDS as that is the responsibility of the Information Assurance Manager. The CAA or RAA are for areas through which PDS carrying classified information traverse, such as SIPRNET.

1. Navy only: If there are deviations from the minimum physical security requirements of IA Pub 5239-22 for a CAA or RAA, the accreditation package must also include a letter from the Commanding Officer acknowledging the deviations and requesting that NETWARCOM as ODAA accept the risk.

c. Additional guidance for paragraph 10-3: Checklists are available to assist you with validating the requirements for a Secure Room (SR), CAA, or RAA, and can be found at https://infosec.navy.mil (once there, click on Documentation, NETWARCOM, Residential Storage). Keep in mind that the checklist stated for a SR was developed for open storage up to Secret in residence. However, the standards in that checklist apply to open storage for Top Secret.

d. Add to end of paragraph 10-10.2: Commanding General of U.S. Marine Forces Pacific Command, Commanding General of Marine Corps Combat Development Command and Commanding General of Marine Corps Systems Command.

e. Clarification to "Fleet Commanders" in paragraph 10-10.2: Fleet Commanders are U.S. Fleet Forces Command, Commander, Pacific Fleet, Commander, U.S. Naval European Command, and Commander, U.S. Navy Central Command.

f. Additional guidance for paragraph 10-10: Navy military and civilian personnel shall refer to NTD 03-09, "Summary of Requirements for Use of SIPRNET in Residential Quarters," for additional guidance that was issued as coordinated policy with CNO (N09N2) and Commander, Naval Network Warfare Command.

g. Change first sentence to paragraph 10-19 to read: "Records of destruction are not required for Secret and Confidential information except for special types of classified information or removable storage devices (i.e., removable hard drives) (see paragraphs 7-8 and 10-17).

h. Additional guidance for paragraph 10-19: Navy military and civilian personnel shall refer to NTD 12-08 "Disposition of Navy Hard Drives," for additional guidance that was issued as coordinated policy with CNO (N09N2) and Commander, Naval Network Warfare Command.

8. Chapter 12 - Loss or Compromise of Classified Information:

a. Add new subparagraph to 12-4 to read as follows: 3. Electronic spillages (ES) are unacceptable and pose a risk to national security.

There continues to be a significant number of ES across DON networks, degrading operational readiness and underscoring a lack of Information Security discipline. For the purpose of ES, a Preliminary Inquiry (PI) is mandatory, regardless if it meets the criteria of paragraph 12-7. A JAGMAN investigation is still required if the PI results in serious disciplinary action or prosecution is contemplated against any person(s) believed responsible for the compromise of classified information.

b. Navy military and civilian personnel shall refer to NTD 11-08, "Electronic Spillage Requirements," for additional guidance that was issued as coordinated policy with CNO (N09N2) and Commander, Naval Network Warfare Command.

c. Change paragraph 12-8.2, second sentence to read: Per reference (a), CNO (N09N2) will notify the United States Security Authority for NATO affairs (USSAN) via the office of the Deputy Undersecretary of Defense (TSP&NDP).

d. Change reference (a), on page 12-12, to read: United States Security Authority for North Atlantic Treaty Affairs (USSAN) Instruction 1-07, Apr 2007

P.O.C. (include name, commercial/dsn phone number, email): _____

COMMAND_____ ADDRESS_____

	TYPE OF DOCUMENT				LEVEL OF CLASS			DURATION OF CLASSIFICATION								TYPE OF CLASS			SOURCE OF DERIVATIVE			DISCREPANCIES																				
	MESSAGE	MEMO/LETTER	ELECTRONIC MEDIA (includes emails)	OTHER	TOP SECRET	SECRET	CONFIDENTIAL	DATE/EVENT DECLASS < 10 YRS	DECLASS 10 YEAR	DECLASS > 10 YRS < 25 YRS	DECLASS 25 YRS.	25X1-25X9*	X1-X8 or OADR*	SOURCE MARKED X1-X8 or OADR*	NOT INDICATED	ORIGINAL	DERIVATIVE	CANNOT DETERMINE	CLASSIFICATION GUIDE	MULTIPLE SOURCES	SINGLE SOURCE/OTHER	OVER CLASSIFIED	UNDER CLASSIFIED	OVERALL CLASSIFICATION MARKING	CAVEATS (INTELL, WARNING NOTICES, and REL TO)	PORTION MARKING	"CLASSIFIED BY "LINE (original classification only)	"REASON" LINE (original classification only)	SOURCE INDICATED FOR "DERIVED FROM " LINE (derivative classification	MULTIPLE SOURCES NOT LISTED FOR "DERIVED FROM" LINE (derivative classification only)	UNKNOWN BASIS FOR MULTIPLE SOURCES LISTED IN "DERIVED FROM" LINE (derivative classification only)	"DOWNGRADE TO" LINE	DURATION OF CLASSIFICATION FOR "DECLASSIFY ON" LINE	OTHER
1																																								
2																																								
3																																								
4																																								
5																																								
6																																								
7																																								
8																																								
9																																								
10																																								
11																																								
12																																								
13																																								
14																																								
15																																								
16																																								
17																																								
18																																								
19																																								
20																																								

Take additional notes on back of form

*Improper application of these markings should be indicated by a dark border around the box:

Ouellette, Bridget Anne CIV NCIS, Code 24

From: Bennett, Frank M CIV NCIS, Code 24
Sent: Monday, March 23, 2009 11:13 AM
To: King, Walter L CIV USFF, N02S; Miller, Tom LCDR COMPACFLT, N0041; Ikehara, Sidney S CIV COMPACFLT, N0041B; 'Jeffrey.grunigen@eu.navy.mil'; 'joseph.orosco@me.navy.mil'; 'michael.topping@me.navy.mil'; Garrity, William P CDR COMUSNAVSO, N2; 'mccantsr@cotf.navy.mil'; Wofford, Johnnie CIV N01S; 'george.hulak@navsoc.socom.mil'; 'john.whalen@jfcom.mil'; 'rgorka@usna.edu'; Riester, Peter CIV NAVAIR; Atchison, David H CIV AIR 7.4.1, Security; Kay, Harry CIV NDW WNYD, N1; Brough, James R NETC, N00415; Frandsen, Donald LT NETC, Admin; Davis, Janice K CIV NAVFACHQ; Haddox, Barry D CIV (NAVFACHQ); Brown, Cynthia A CIV FLDSUPPACT; 'brenna.'; Martin, Joseph CIV CNIC HQ, N3AT; 'mwentling@nmic.navy.mil'; 'rlohr@nmic.navy.mil'; Beasley, Heidi A CIV JAG, OJAG CODE 17; 'Diana.Luckey@med.navy.mil'; Moore, Alphonso CIV; Powers, James C CIV BUPERS-00Y, PERS-334; 'mandersen@nps.navy.mil'; Parker, Doris S NAVSAFECEN, 053; Beveridge, Gene E. CIV NAVSAFECEN, 05; Geary, Patrick J CIV SEA 00P; Rosado, Ben CIV SPAWAR HQ, 8.3.3; 'barbet.bryant-gordon@ssp.navy.mil'; 'lisa.koenig@ssp.navy.mil'; Lafata, Mary J CIV (SUP 03X); 'leonard.coleman@nwc.navy.mil'; Jimenez, Frank R GENERAL COUNSEL; Smith, Jacqueline L CIV AAUSN, SPD; Albrecht, Erich L CIV NAVYIPO, IPO-09X; Alcoy, Shelly M CIV NETWARCOM, N0; Gray, Carrie LCDR NIOC Norfolk N2; 'leslie.bethune@usmc.mil'; 'linderman.burkhart@usmc.mil'; 'william.t.potts@usmc.mil'; 'charles.b.silk@usmc.mil'; Haskett, Mark L CIV NCIS, Code 11; Hawkins, Anesia NAVAUDSVC; Lacross, Rita CIV PRESINSURV ADMIN; Howard, Curtis CIV ONR, 43; Woodruff, Jesse J CIV Navair 4.0X; 'lovel.waiters@navy.mil'; Jones, Douglas A CIV CID Corry Station; Titus, Sheryl L CIV COMNAVREG MIDLANT NORFOLK VA; Emerson, Sherry D CIV CNRMW Great Lakes, N00D; Kay, Harry CIV NDW WNYD, N1; Nichols, David CIV IT; Arcaira, Vidal B CIV CNRNW, N00S; Thomas, Jeanette L CIV CNRSE HQ, N00CS; Baylon, Veronica CIV CNRSW, N00; 'Jeffrey.grunigen@eu.navy.mil'; 'roland.clark@guam.navy.mil'; Messinger, Norman CIV PACOM, J5; 'william.horne@me.navy.mil'
Cc: Jackson, Benita M CIV NCIS, Code 11; Ouellette, Bridget Anne CIV NCIS, Code 24
Subject: Rating Element - Management of Classified Information
Signed By: frank.m.bennett@navy.mil

Attachments: Bennett, Frank M CIV NCIS, Code 24.vcf

Bennett, Frank M CIV NCIS, Cod...

Ref: (a) SECNAV M-5510.36
(b) Executive Order 12958, as amended
(c) 32 CFR Parts 2001 and 2004 (ISOO Implementing Directive 1)
(d) DoD 5200.1-R

Per reference (a), para 2-1.5h you must "ensure the performance rating system of all DON military and civilian personnel, who duties significantly involve the creation, handling, or management of classified information, include a critical security element on which to be evaluated." This includes Original Classification Authorities. References (b) through (d) are also clear and mutually supportive of this requirement. It is imperative you ensure command compliance with this requirement; especially for those that have converted to NSPS or those pending conversion.

We understand NSPS may pose a challenge for complying with this requirement. We highly recommend you work with your NSPS specialist, within your command, on how to best incorporate this as a stand-alone objective or inclusion within another objective that covers a myriad of other significant duties (such as EEO, Supervisory Responsibilities, etc.). We do not advocate the latter as the solution, merely a recommended workaround, given the fact that the number of objectives for NSPS must be kept to a minimum and it is sometimes difficult to establish a separate rating element (or objective in the case of NSPS) for every duty and/or responsibility. Furthermore, we do

not dictate in reference (a), Exhibit 2A that a command security instruction shall include the requirement to rate an individual on their security responsibilities (as stated above), but it is highly recommended that it be included. At the very least it would help to serve as a reminder to command management to include the above stated requirement when rating personnel; regardless, of the type of performance rating system.

Very respectfully,

Frank M. Bennett
Chief of Naval Operations (N09N2)
DON Classification Management Program Manager
202-433-8847
Don't forget to visit our website at www.navysecurity.navy.mil

"Standing by to Support the Fleet"

On this date 23 March 1882 - SECNAV Hunt issues General Order No. 292 creating Office of Naval Intelligence.