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

OPNAVINST 5513.1F
N09N2
7 DEC 2005

OPNAV INSTRUCTION 5513.1F

From: Chief of Naval Operations

Subj: DEPARTMENT OF THE NAVY SECURITY CLASSIFICATION GUIDES

Ref: (a) SECNAVINST 5510.36

Encl: (1) Subject Categories for Security Classification Guides
(2) Guide Format and Responsibilities for Preparation
(3) Guide Update Submission Format
(4) Security Classification Criteria, Principles and Considerations
(5) Administrative Data
(6) Sample Security Classification Guide

1. Purpose. To assign responsibilities and establish procedures for preparing and issuing security classification guides for Department of the Navy (hereafter referred to as "Department") classified systems, plans, programs, and projects. This instruction has been substantially revised and should be read in its entirety.

2. Cancellation. OPNAVINST 5513.1E.

3. Background

a. Reference (a) requires that designated Original Classification Authorities (OCAs) prepare a security classification guide for each Department system, plan, program, or project under their cognizance which creates classified information. In support of this requirement, the Chief of Naval Operations (CNO) (N09N2) manages a system called the Retrieval and Analysis of Navy Classified Information (RANKIN) Program, which issues security classification decisions made by Department OCAs.

b. Security classification guides serve both legal and management functions by recording Department original classification determinations made under Executive Order (EO) 12958, as Amended, of 28 March 2003, and its predecessor and successor executive orders on national security information. Guides are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements. Guides may also include information concerning special public release requirements and

foreign disclosure considerations.

4. Responsibilities

a. Officials designated Original Classification Authority (OCA) in accordance with reference (a) are responsible for:

(1) Making original classification determinations and preparing new security classification guides.

(2) Conducting reviews at least once every five years and, when necessary, revising security classification guides under their cognizance.

(3) Issuing short-term interpretive guides consistent with those issued by the OPNAV Instruction 5513 series.

(4) Providing the CNO (N09N2) with copies of all new security classification guides, revisions, cancellations, interpretations, and notifications of review, for issuance in the OPNAVINST 5513 series.

b. CNO (N09N2) is responsible for:

(1) Entering all security classification guides into the Department database.

(2) Reviewing new or revised guides to ensure compliance with existing executive orders, regulations, directives and instructions.

(3) Issuing all Department security classification guides delineated by major subject categories, using the current editions of OPNAV Instruction 5513 series as described in enclosure (1). In cases of operational necessity, OCAs may authorize for immediate use such new or revised guides as necessary; such guides must, however, be promptly cancelled when issued by CNO (N09N2) in the OPNAVINST 5513 series.

(4) Assisting OCAs in preparing security classification guides when necessary.

c. All Department personnel who classify information will use the guidance issued in the OPNAVINST 5513 series.

5. Procedures

a. Security classification guides will be prepared following the format described in enclosure (2).

b. Revisions to security classification guides will be submitted to CNO (N09N2) in the format shown in enclosure (3).

c. Security classification guides will follow the general principles described in enclosure (4).

d. Administrative data relating to Department security classification guides is contained in enclosure (5).

e. A sample security classification guide is provided in enclosure (6).

6. Applicability. This instruction applies to all Department activities that originate, handle or receive classified information.

7. Action

a. Officials designated in reference (a) as OCAs shall comply with this instruction and the procedures outlined in enclosures (2) through (5).

b. All Department personnel responsible for producing classified information shall use the security classification guides issued under this instruction to derivatively classify national security information.

/s/
DAVID L. BRANT
Special Assistant for Naval
Investigative Matters and Security

Distribution:
Electronic only, via Navy Directives Website
http://neds.daps.dla.mil

SUBJECT CATEGORIES FOR SECURITY CLASSIFICATION GUIDES

OPNAV Instruction 5513.1F:	Department of the Navy Security Classification Guides (Assigns specific responsibilities for security classification guide preparation, updating procedures, and general administration.)
OPNAV Instruction C5513.2B:	Air Warfare Programs
OPNAV Instruction S5513.3B:	Surface Warfare Programs
OPNAV Instruction S5513.4D:	General Intelligence, Cover and Deception, Security and Investigative Programs
OPNAV Instruction S5513.5B:	Undersea Warfare Programs
OPNAV Instruction S5513.6C:	Communications and Satellite Programs
OPNAV Instruction S5513.7C:	Mine Warfare Programs
OPNAV Instruction S5513.8B:	Electronic Warfare Programs
OPNAV Instruction S5513.9B:	Nuclear Warfare Programs
OPNAV Instruction S5513.10B:	Advanced Technology and Miscellaneous Programs
OPNAV Instruction 5513.11B:	Ground Combat Systems
OPNAV Instruction 5513.12C:	Intelligence Research Projects
OPNAV Instruction S5513.13C:	Non-Acoustic Anti-Submarine Warfare (NAASW) Programs
OPNAV Instruction 5513.15D:	Special Warfare Programs
OPNAV Instruction 5513.16A:	Declassification of 25-Year Old DON Information

GUIDE FORMAT AND RESPONSIBILITIES FOR PREPARATION

A. Format. The following format, although originally designed for weapon systems, may be adapted to any classified program. If a paragraph does not fit a particular program, the notation "Not Applicable" should be entered. As security classification guides are considered technical documents, they must indicate the applicable distribution statement (see reference (a)) on the first page. Guides determined to contain export-controlled technical data will also be marked as required (see reference (a)).

01. Identifying data

ID: A numerical designation assigned by CNO (N09N2) to serve as the permanent identifier for the guide. For example, ID: 04D-15 will indicate OPNAVINST S5513.4D, enclosure (15). OCAs may assign consecutive "point" numbers to indicate a change to the guide prior to formal issuance through the RANKIN system; e.g., ID: 04D-15.2 will indicate OPNAVINST S5513.4D, enclosure (15), change 2.

CL: The security classification (including Unclassified) of the content of the guide itself will be shown in abbreviated form; e.g., "U", "C", "S". If classified, each individual part of the guide will be marked to indicate its classification level in accordance with the portion marking requirements of reference (a).

SU: The subject of the guide will be entered.

OC: The code of the command subject matter experts responsible for day-to-day interpretations of the guide will be entered; when more than one code is responsible, all will be included.

CA: The designation of the OCA who is responsible for and has approved the classification determinations will be entered; when more than one authority is responsible, all will be included.

OD: Date the guidance on the subject was originally issued will be entered.

CD: Date the guidance was last validated by a review or changed by the OCA (entered by CNO (N09N2)).

RD: Date the guidance will next be reviewed (entered by CNO (N09N2)).

02. Threat/Background. State where the following information can be obtained: A complete threat assessment or

background data to include what information is to be protected and denied to potential enemies. This information, usually provided by the Office of Naval Intelligence (ONI), may be included in the guide, however, classification and dissemination restrictions must be considered. Additionally, under EO 12958, as amended, the classification authority is required to identify the reason(s) for the decision to classify. This is accomplished by a brief reference to the list of applicable category(ies) in section 1.4 of EO 12958, as amended, e.g., the citation "Classified under category 1.4(a) of EO 12958, as amended" would indicate that the reason the information is classified is because it not only meets the damage criteria of the EO but it also falls under the category of "military plans, weapons systems, or operations." If more than one category applies, state as succinctly as possible the applicable categories, e.g., "Classified under category 1.4(a) with the exception of information elements 07A(1)-(5) which are classified under category 1.4(c)." A list of these classification categories is found in enclosure (4).

03. Mission. Describe what the goal of the program is or what has already been accomplished. This is normally best stated in the form of a mission statement. An unclassified statement is preferred.

04. Financial. Provide classification requirements and downgrading/declassification data for budgetary information. Although Department of Defense (DOD) policy prohibits the disclosure of budget and procurement data prior to presentation by the Executive Branch to the Congress, this type of information is generally not classified. Therefore, guidance should indicate that current year budgetary data is unclassified and outyear data is "For Official Use Only" (FOUO) until submitted to Congress. Budgetary information may require classification if it reveals significant information concerning the trends and emphasis of the U.S. research and development program. As a practical matter, it is recommended that the classification of budgetary information be avoided since classifying this type of information typically creates an onerous administrative burden.

05. Milestones. State the classification requirements and downgrading and/or declassification date or event for milestones expected during technical development. In general, milestones, except for initial operational capability (IOC) dates or testing dates, do not warrant protection since they are so variable. Even IOC and testing dates, however, should not be classified unless they could significantly aid a potential enemy by revealing the time available to emplace or develop countermeasures.

06. Performance data and technical characteristics. Provide the classification level and downgrading and/or declassification date or event for separate performance and technical characteristics such as speed, range, velocity, maneuverability,

etc. Descriptions should be specific. For example, a topic might read: "Range: C-15 (However, the statement that the missile range is "about 100 NM," is unclassified).

07. Operational and Tactical. Provide the classification level and downgrading and/or declassification date or event for each aspect of the operational or tactical utilization of the program.

08. Hardware. The classification level and downgrading and/or declassification date or event will be entered for the end item and its components, including visual access and external view. Paragraph 2d of enclosure (4) is applicable to this. Any special classified hardware destruction or demilitarization procedures may be provided. Computer resources hardware guidance will be placed in the "Computer Resources" portion of the guide.

09. Computer Resources. Provide the classification level and downgrading and/or declassification date or event for separate categories or subsystems. Care must be taken to separate militarily sensitive information and data base domains from non-military applications and/or architecture. Such categories would include:

a. Information/Decision Support. Including capture, presentation, storage, movement, processing, control, security.

b. System. Including applications, languages, tools, methodologies, management, artificial intelligence.

c. Artificial Intelligence. Including knowledge-based (expert) systems, robotics, image processing, natural language processing, speech processing, neural networks.

d. Hardware. Including architecture, peripherals, components, firmware.

e. Software. Including languages, data base management, design tools.

f. Networks/Communication. Including local area networks (LANs) and wide area networks (WANs).

10. Other. Guidance which cannot be categorized in any of the other topics is to be stated here.

RANKIN Program Manager Note. The RANKIN Program Manager may occasionally include a comment at the end of a guide to provide RANKIN program management data and/or any other miscellaneous information concerning that guide. These notes are intended to be a management tool and will not supplant any guidance provided by that guide's OCA.

B. Responsibility for Preparation. The Department OCA assigned overall responsibility for a program will prepare the initial security classification guide and will provide the information required by paragraph A of this enclosure to CNO (N09N2).

C. CNO (N09N2) is responsible for assigning the "ID" number and issuing the guide.

D. Sample Guide. Enclosure (6) is a sample security classification guide.

GUIDE UPDATE SUBMISSION FORMAT

From: Originating Command
To: Chief of Naval Operations (N09N2)

Subj: CHANGE SUBMISSION FOR (ENTER SUBJECT AND ID NUMBER OF GUIDE)

Ref: (a) OPNAVINST 5513.1F

1. As required by reference (a), the subject guide has been reviewed and:

a. No changes are necessary, or,

b. This guide should be cancelled because (Insert reason, such as end of program. Also, indicate if all topics may be declassified or if continued classification is required because declassification would compromise similar classified programs. In the latter case, such programs should be identified), or,

c. The following changes are requested: (Insert precise changes such as "Topic 6A(4) should be changed to read (U) vice (C-10)", or "First line of 03. Mission, should read (attitude) vice (altitude)," or "Add following topic to paragraph 9C: (Quantities of items planned for procurement: C-13)"), or,

d. A complete revision or annotated copy is attached. (Annotations may be made by pen, cut and paste, or any legible means), or,

e. The attached guidance has been disseminated to appropriate personnel.

2. The (insert command name) point of contact for this matter is (insert action officer name and telephone number).

(Signature and title of the
OCA or other official authorized
by the OCA to submit changes)

NOTE: While the OCA for the guide does not have to sign the change submission personally, the originating command must maintain adequate records to indicate that the OCA has approved the action(s).

SECURITY CLASSIFICATION CRITERIA, PRINCIPLES AND CONSIDERATIONS

A. OCAs are urged to apply the following security classification criteria, principles and considerations to ensure correct classification:

1. Classification Criteria:

A determination to originally classify will be made only by an OCA when the unauthorized disclosure of the information could reasonably be expected to cause a degree of damage to the national security, and only when information falls into one or more of the following categories (from EO 12958, as Amended):

a. Military plans, weapons systems, or operations ("Category 1.4(a)");

b. Foreign government information ("Category 1.4(b)");

c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology ("Category 1.4(c)");

d. Foreign relations or foreign activities of the United States, including confidential sources ("Category 1.4(d)");

e. Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism ("Category 1.4(e)");

f. United States Government programs for safeguarding nuclear materials or facilities ("Category 1.4(f)");

g. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism ("Category 1.4(g)"); or

h. Weapons of mass destruction ("Category 1.4(h)").

2. Classification Principles:

a. The advantages and disadvantages of classification must be considered. Classification decisions should be based on objective review, sound judgment and risk management principles.

b. Specific information, which requires classification, must be identified in an unambiguous manner.

c. Basic research should not be classified unless the information concerns an unusually significant scientific "breakthrough," and there is sound reason to believe it may have a wide variety of military applications.

d. Items of equipment or other physical objects may be classified only when classified information may be derived from them by visual observation of internal or external appearance, structure, operation, test, application, or use.

e. A compilation of unclassified items may be classified if the items together provide an added factor which warrants classification.

3. Classification Considerations:

a. If considerable dissemination of the information is anticipated, it may make classification impractical.

b. Classification should be considered if it is necessary to protect a "lead-time advantage" (i.e., the interval between the acquisition of knowledge by the U.S. Government and the acquisition of knowledge by an adversary). This lead-time advantage must produce such a tactical or strategic advantage as to outweigh the benefits to the U.S. Government and U.S. industry from the unclassified use of the information.

c. The costs resulting from classification in terms of time, money, or personnel must be considered. Sound classification decisions will result in operational economies by permitting concentration on the protection of information actually vital to our national security.

d. Appearance in the public domain, or any previous compromise or possible compromise of information currently being contemplated for classification, should be considered.

e. Ensure that new classification decisions are consistent with existing classification decisions. For example, if you are preparing a guide on a new missile, all available classification guides for similar missiles should be examined. The DOD Index of Security Classification Guides (DOD 5200.1-I) (available in limited quantities from CNO (N09N2)) is useful in identifying existing guides.

4. Increasing Guide Usability. Experience has shown that OCAs can significantly increase guide usability by:

a. Making their security classification guides unclassified.

b. Making their security classification guides succinct and to the point.

c. Using standard or commonly understood words and phrases. The meanings of terms commonly used in Department guides (e.g., altitude, circular error probably, component, countermeasures, materiel, range, reliability, resolution,

software or vulnerability) should be consistent with those definitions published in technical or military glossaries, e.g., Joint Pub 1-02 (formerly Joint Chiefs of Staff (JCS) Pub 1), "Department of Defense Dictionary of Military and Associated Terms," (NOTAL). Guides should never use slang and should avoid using warfare community-unique words and phrases unless they are defined for the guide user.

ADMINISTRATIVE DATA

1. Public release. Confirmation, denial or extension of public statements relative to information concerning a classified Department program, whether classified or unclassified, is prohibited. The fact that information is unclassified does not automatically allow its public release. Information will be released to the public only through authorized channels, e.g., the originating command identified in paragraph 01 of the specific security classification guide and under the Department's Public Affairs Regulations, SECNAVINST 5720.44A.

2. Classification Recommendations. All users of Department classification guides are encouraged to assist in maintaining the accuracy and completeness of Department guides. If circumstances indicate a need for change(s) in the assigned classification(s), or if additional topics are required, completely documented and justified recommendations should be submitted to the OCA (copy to CNO (N09N2)) for the specific guide. Pending final decision, the information in question will be marked with a tentative classification equivalent to that contained in the current guidance or that recommended by the user, whichever is higher.

3. Regrading authority. The classification guidance prescribed by the OPNAVINST 5513 series constitutes authority for classifying, downgrading, upgrading or declassifying Department information. The individual guide should be referenced when effecting the change of classification on a document. For example, if the P-3 aircraft guide in OPNAVINST C5513.2B (enclosure (41)) effects a change in the classification of a document, a notation would be placed on the front cover such as: "Downgraded to Confidential by authority of OPNAVINST C5513.2B-41 by James A. Smith on 15 November 2003." If feasible, when the classification of a document is changed, all holders should be notified by the originator of the document.

4. Identification of Classification Requirement. In addition to assigning the overall document, page and portion classification, each document will be marked to indicate the authority for the classification action taken and the appropriate downgrading and/or declassification instructions. Each topic of a classification guide contains an abbreviation of the classification level and downgrading and/or declassification date or event for the described category of information. The following examples demonstrate the proper use of these abbreviations:

a. C-(declassify upon IOC). Classified Confidential to be declassified upon initial operational capability date:

Derived from: (insert identity of specific guide such as OPNAVINST C5513.2-25*)
Declassify on: Upon IOC of (enter nomenclature of program, e.g., the F-14)
*Indicates enclosure (25) to OPNAVINST C5513.2

b. S-(Declassify 8 years from date of origination). Classified Secret and declassified eight years following the month and day of origination of the information being classified:

Derived from: (insert identity of specific guide)
Declassify on: (enter day, month and year of the eighth year following origination)

c. S-07. Classified Secret and declassified in 2007 on the day and month of the original program guide date found on the OD line of paragraph 01 of each individual guide. In the following example, the specific guide indicates "OD: 97-01-17":

Derived from: (insert identity of specific guide)
Declassify on: 17 Jan 07

d. S-25 (DG/C/15). Classified Secret to be downgraded to Confidential in 2015 and declassified in 2025, both on the day and month of the Original program guide date found on the OD line of each individual guide. In the following example, the specific guide indicates: "OD: 04-04-06"

Derived from: (insert identity of specific guide)
Downgrade to: Confidential on 6 Apr 2015
Declassify on: 6 Apr 2025

e. S-RD. Classified Secret, containing Restricted Data:

Classified by: (insert identity of specific guide)

RESTRICTED DATA This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

f. S-25X1-human.

Derived from: (insert identity of specific guide)
Declassify on: 25X1-human

SAMPLE SECURITY CLASSIFICATION GUIDE

01. IDENTIFYING DATA:
ID: 02C-273
CL: U
SU: SUPER MISSILE (AGM-13)
OC: NAVAIR (AIR-720)
CA: COMNAVAIRSYSCOM
OD: 94-11-04
CD: 05-12-15
RD: 10-12-15

02. THREAT/BACKGROUND: Operational requirement CA-14703 of 25 June 1994 applies (NOTAL). Information originally classified by this guide under EO 12958, as Amended, is classified under category 1.4(a).

03. MISSION: To provide attack aircraft with a weapon capable of destroying air, surface and subsurface targets.

04. FINANCIAL:

A. Prior to budget submission: FOUO
B. Subsequent to budget submission: U
C. Unit cost: U

05. MILESTONES:

A. IOC: C-(Declassify after IOC).
B. MK 7 Missile Upgrade: C-(Declassify after upgrade is completed on 80% of inventory).

06. DESIGN PERFORMANCE AND FUNCTIONAL CHARACTERISTICS:

A. Target detecting device (TDD), MK-22:
(1) Range: C-07
(2) Reliability: C-07
(3) Lethality: C-07
(4) Specific frequencies: S-07
(5) Numerical frequency bandwidth: S-07
(6) Pulse width: S-07
(7) Pulse repetition rate: S-07
(8) Vulnerability to countermeasures: S-07
(9) Counter countermeasures: S-07

Distribution Statement D: Distribution authorized to DoD and U.S. DoD contractors only; Administrative/Operational use (November 2004). Other U.S. requests for this document will be referred to COMNAVAIRSYSCOM (AIR-720).

07. OPERATIONAL AND TACTICAL:

A. Tactics for:
(1) Air to subsurface employment: S-19
(2) Air to surface employment: C-19
(3) Air to air employment: S-19
B. Operational or exercise schedules which indicate that a Super Missile (AGM-13) will be fired: C-(Declassify 30 days after firing).

08. HARDWARE:

A. Missile (without TDD MK-22):
(1) End item: U (The complete missile is unclassified unless the TDD MK-22 is installed.)
B. Missile (with TDD MK-22):
(1) End Item: C-07
C. External view of missile: U
D. External view of TDD MK-22: U
E. Demilitarization procedures: In addition to the classified TDD MK-22, unclassified circuit boards A34561 through A34568, and the missile radome must be destroyed in order to demilitarize the system.

09. COMPUTER RESOURCES:

A. Information/Decision Support:
(1) Techniques for real-time adaptive control of distributed parallel processing systems and related onboard architecture and off-board telecommunications requirements: S-19
(2) Security related to use of imbedded computer programs (viruses) for operational security or deception: S-19
(3) Controls relating to prevention of unauthorized tampering or activation; specifically algorithms and architecture: S-19
B. System:
(1) Techniques for distributing data base/information base management functions in multisource, multiuser environment: S-19
C. Artificial Intelligence (AI):
(1) Fact of use in Super Missile (AGM-13): U
(2) Generic AI shell/inference engine information: U
(3) Specific rule or frame based details of AI decision making process: S-19
(4) Specific inference techniques, heuristic search techniques, and knowledge acquisition techniques used for missile flight, target acquisition and tracking, and target homing: S-19
(5) Pattern recognition and scene segmentation application used for flight profile, target recognition, and homing: S-19
D. Hardware:
(1) Real time spectrum analyzers and frequency synthesizers associated with wartime and exercise versions: S-19

(2) Electromagnetic environment operational capability, compatibility, and performance in all aspects that could lead to countermeasure definition: S-19

E. Software:

(1) Reduced Instruction Set Computing (RISC) use: C-07

(2) Countermeasure resistance techniques: C-19

(3) Fault isolation capability to bypass onboard component failure or battle damage: S-19

F. Network/Communication:

(1) Frequency spectrum plan for inter-missile and missile-platform information update: S-19

(2) Technical details of in-flight mission reprogramming capability: S-19

10. OTHER:

A. The fact that certain details of information are shown to be unclassified does not allow public release. Proposed public release of Super Missile (AGM-13) unclassified information will be processed through appropriate channels for publication approval.

B. All questions regarding "need-to-know" which cannot be resolved will be forwarded to NAVAIR (AIR-720).

RANKIN Program Manager Notes: A review of paragraphs 06A is being conducted to determine if those information elements should be changed from C-07 to C-19. The NAVAIR POC on the progress of that review is Dr. E. D. Smith (AIR-720), DSN 255-8877.