DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
2531 JEFFERSON DAVIS HWY
ARLINGTON VA 22242-5160

IN REPLY REFER TO

NAVSEAINST 5100.12A
Ser 03D7/008
11 DEC 95

NAVSEA INSTRUCTION 5100.12A

From: Commander, Naval Sea Systems Command

Subj: REQUIREMENTS FOR NAVAL SEA SYSTEMS COMMAND SYSTEM SAFETY PROGRAM FOR SHIPS, SHIPBORNE SYSTEMS AND EQUIPMENT

Ref: (a) NAVSEAINST 5400.1E
(b) DODI 5000.2 of 23 Feb 91
(c) SSS-STD-882
(d) NAVSEAINST 8020.6C
(e) MIL-STD-1385B
(f) SPAWARINST 5100.12A
(g) NAVSEAINST 9310.1B
(h) ASTM F1166

Encl: (1) Guide for Tailoring System Safety Program Requirements

1. Purpose

a. To establish and promulgate requirements and responsibilities for developing and implementing the Naval Sea Systems Command (NAVSEA) system safety program for the acquisition of ships, shipborne systems, and equipment. The functions described herein are elaborations on the responsibilities in reference (a), the NAVSEA Headquarters Organization Manual.

b. To ensure that safety, consistent with mission requirements and cost effectiveness, is designed and engineered into all military systems, subsystems, and equipment assigned to NAVSEA, and its affiliated Program Executive Offices (PEOs) and the Direct Reporting Program Manager (DRPM) for AEGIS. Functional support is provided to each PEO/DRPM by NAVSEA, pursuant to an operating agreement approved by the ASN(RD&A). This approach is based on reference (b), parts 6I and 7B, and reference (c). Reference (b) requires that system safety programs, tailored in accordance with reference (c), be applied in the acquisition of all systems. Enclosure (1) provides guidance for tailoring system safety programs based on reference (c).

2. Cancellation. This instruction supersedes NAVSEAINST 5100.12. Marginal change notations are not provided because of the extent of the revisions.

3. Scope

a. This instruction applies to the design, development, procurement and production of ships, shipborne systems, and equipments (to include hardware, firmware, and software) under the cognizance of COMNAVSEA (including shipyards, planning yards, SUPSHIPS, the Naval Ordnance Center, the Naval Surface Warfare Centers, and the Naval Undersea Warfare Center), and the affiliated PEOs and DRPMs for use by U.S. Navy personnel. Any modifications and alterations (e.g., Engineering Change Proposals (ECPs), Ship Alterations (SHIPALTs)) to ships, shipborne systems and shipboard equipments fall within the purview of this instruction. This instruction also applies to Government Furnished Equipment (GFE).

b. This instruction applies to Chemical/Biological/ Radiological (CBR) weapon systems, as well as industrial, handling, and operational exposure to radiation hazards associated with those systems, and to any conventional explosive or propellant used in nuclear or CBR weapon systems that have not already been reviewed and approved through nuclear or CBR weapon approval channels.

c. Detailed requirements supporting this instruction are contained in reference (d) for explosives, reference (e) for lasers, reference (f) for lithium batteries, and reference (g) for electro-explosive devices.

4. Background. Safety problems that are undetected until late in the design or construction of a ship or system can wreak havoc with budgets and schedules. Historically, the Navy corrected hazards after mishaps occurred. However, because of the increasing complexity and cost of systems, and increased concern over catastrophic accidents, the Defense Department adopted system safety as a primary discipline stressing preventive methods.

5. Discussion

a. This modification reflects current NAVSEA Headquarters Organization Manual responsibilities, reference (a), updates the NAVSEA System Safety Program requirements to meet DODI 5000.2, reference (b), and provides guidance for tailoring safety programs to meet SSS-STD-882, reference (c). Additional guidance for tailoring system safety

programs to meet the requirements of reference (c) is available from the NAVSEA Human Systems Integration Division, SEA 03D7.

b. MIL-STD-882 (System Safety Program Requirements) was used by many industries in establishing system safety programs for the products they develop because the commercial equivalent, SSS-STD-882, did not exist until July 1994. SSS-STD-882 is avalable for purchase from the System Safety Society, five Export Drive, Suite A, Sterling VA, 22170-4421.

c. DOD policy requires the use of commercial specifications and standards rather than military specifications and standards unless there are no commercial equivalents. Reference (c) is the commercial equivalent of MIL-STD-882 and is in accordance with DOD policy. Tailored application of either reference (c) or MIL-STD-882 should not result in any differences in the scope or cost of system safety program requirements.

d. Note that the Master Program Plan (MAPP) also meets the system safety program planning requirements of DODI 5000.2, and can be used as an alternative to traditional program planning documents. The MAPP User's Guide for system safety directs the user to consult MIL-STD-882 (now SSS-STD-882) and its appendices on tailoring the standard to fit the needs of a system safety program.

6. Definitions. The following definitions are applicable to this instruction:

a. Safety. Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Note that additional guidance on environmental safety issues is provided in OPNAVINST 5090.1A and OPNAVINST 5100.19C.

b. Ship Safety. Degree of safety attainable, based upon accepted standards and general shipbuilding specifications.

c. System. A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, or support mission requirements.

d. System Safety. The application of system engineering and management principles, criteria and techniques to optimize all aspects of safety for a given system within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

e. System Safety Program Plan (SSPP). A description of the tasks and activities required to implement the System Safety Program (SSP). This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems. For most programs, there could be two or more SSPPs. The managing activity prepares a SSPP describing how the program office intends to manage the overall safety program. The developing activity (often a contractor) will prepare their SSPP describing in detail the system safety program that will be performed. Subsystem developers may prepare their SSPPs for their portion of the overall program.

f. Hazard. A condition that could result in a mishap.

g. Mishap. An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

h. Hazard Severity. An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.

i. Hazard Probability. The probability that a hazard will result in a mishap, based on an assessment of such factors as location, or exposure, in terms of cycles or hours of operation, and affected population.

j. Managing Activity. This term usually refers to the government procuring activity (e.g., NAVSEA, the PEO's and DRPM's, ship design managers, program managers, project managers, acquisition managers, and all project activities under the control of NAVSEA). It may include prime and associate contractors or subcontractors who impose system safety tasks on their suppliers.

k. Qualified Safety Engineer/Manager. A qualified safety engineer/manager should have formal training in system safety and a level of experience in applying system

safety engineering and/or management commensurate with the associated tasks and complexity of the system.

1. Hazardous Material. Anything that because of its chemical, physical, or biological nature causes safety, public health, or environmental concerns.

7. Action. The following requirements and responsibilities must be considered when tailoring a system safety program for all ship and shipboard system acquisition programs, including alterations, modifications, and conversions:

a. Managing activity:

(1) Implement the safety policies and procedures for acquisitions under their cognizance.

(2) Provide detailed direction to life cycle engineers and managers in support of the policies and procedures expressed herein for specific acquisition and procurement programs.

(3) Designate a qualified key person(s) as the system safety engineer/safety manager, or the safety group personnel, as necessary, for each acquisition program. (i.e., a safety manager will normally serve on NAVSEA in-house ship design teams.) A safety group supports the safety manager. The safety group may consist of NAVSEA personnel, or NAVSEA or PEO/DRPM directed contractor personnel.

(4) Require that safety be incorporated early in the design, not added after the ship/system has been delivered. This approach has historically proven to be a significant cost reduction and problem avoidance technique.

(5) Specify, fund, and implement an SSP, initiated in the very early stages of the design process, and identified in acquisition plans.

(6) Carefully tailor the system safety program to meet specific program needs. (See enclosure (1) and reference (c) for guidance on tailoring system safety programs).

(7) Manage hazards by understanding their nature and impact, and assure that they are rectified. The managing activity must be aware of the hazard severity and probability of occurrence to make an informed decision whether to correct it by design action or to accept the

risk. Generally, the higher the risk, the higher the management level for making a risk management decision.

(8) Establish and conduct system safety milestone reviews and checkpoints (to be designated in program plans) for reviewing system safety program progress during design, development and construction.

b. Safety manager:

(1) Plan, organize, implement, and maintain an effective system safety program, tailored to the needs of the specific program, for the managing activity that is integrated into all life cycle phases.

(2) Prepare a SSPP, for approval by the managing activity, that reflects in detail how the total program is to be conducted. It must contain enough detail to assist responsible personnel in implementing each stage of the safety program.

(3) Review system requirements for high risk areas and prepare a Preliminary Hazard List (PHL).

(4) Conduct a Preliminary Hazard Analysis (PHA) of drawings and specifications, using historical data to identify hazards, develop lessons learned, and specify safety criteria for the evolving design.

(5) Establish definitive system safety program requirements for use in procurement or development of a system, including:

(a) Prepare the system safety design requirements for use in ship/system specifications.

(b) Specify the specific risk levels considered acceptable for the ship or system.

(c) Specify the system safety requirements that cannot be defined in the system specifications, which should be incorporated in the contractor or shipbuilder Statement of Work (SOW).

(d) Specify safety data (e.g., analyses, tests, or progress reports) that should be required in the contractor or shipbuilder SOW and Contract Data Requirements Lists (CDRLs) during the engineering and manufacturing development phase.

(e) Specify safety criteria to be applied during full scale development (detail design and construction) phase.

(f) Review the shipbuilder/contractor SSPP for acceptance for the managing activity.

(g) Provide historical safety data Government Furnished Information (GFI), if requested and available, to the shipbuilder or contractor.

(h) Monitor contractors' system safety activities as requested and review deliverable data to ensure compliance with system safety requirements.

(i) Require that the ship or system specifications be updated to reflect adverse results of analyses, tests, and evaluations as appropriate.

(j) Evaluate new and evolving system designs for safety design criteria to update applicable specifications and standards and submit recommendations to the responsible organization.

(k) Develop technical and design safety specifications for use in acquisitions, alterations, modifications and conversions.

(l) Participate in periodic safety design reviews of the evolving ship or system design and conduct periodic on-site physical surveys during production.

(m) Provide guidance to the managing activity in developing and implementing a system safety program.

(n) Establish methods for system safety program management and engineering to facilitate tracking hazards and document action taken.

(o) Provide safety related GFI on GFE and Government Furnished Material (GFM) to the contractor as requested and if available.

(p) Require that cognizant system safety personnel be qualified in the system safety process.

(q) Ensure that a health hazard assessment is made.

c. Director NAVSEA Human Systems Integration (HSI) Division, SEA 03D7, as the focal point for ship system safety programs:

(1) Develop command policies for ship and ship system safety and assess implementation. Monitor correction of safety deficiencies.

(2) Ensure that personnel safety requirements are integrated into the design of naval ships and systems in accordance with references (c) and (h).

(3) Develop and update system safety tools and techniques (e.g., GENSAFE, SDS 077-1, and the ship safety lessons learned database).

(4) Provide system safety support for the design, procurement, and test and evaluation for total ship integration of all shipboard systems, and maintain the ship safety lessons learned database.

(5) Develop and implement system safety programs and conduct hazard analyses for new and existing ships/ systems as required.

(6) Develop specifications for system safety implementation and monitor the shipbuilder system safety program as required.

(7) Coordinate with the Safety Recommendation (SAFEREC) Program Manager and serve as primary liaison with the Naval Safety Center.

(8) Provide a safety panel member on the Specification Control Board.

d. The Safety, Security, and Environmental Directorate of the Naval Ordnance Center (ORD-N71):

(1) Execute the responsibilities specified in reference (d) for explosives safety, reference (e) for laser safety, reference (f) for lithium battery safety, reference (g) for electrical and electromagnetic radiation safety. Coordinate with the lead NAVSEA codes in prosecuting weapons systems safety efforts for ship acquisition and the explosive aspects of nuclear and chemical weapons.

(2) Provide guidance to acquisition managers, developers, and project managers in the development of

weapons system safety programs tailored to meet the unique needs of nuclear and chemical weapons.

(3) Review program planning documentation, especially weapons system safety program plans and Integrated Logistics Support (ILS) plans for appropriateness of weapons system safety requirements and criteria, and maintain the SAFEORD, weapons safety lessons learned database.

(4) Provide guidance to acquisition managers concerning the evaluation, elimination, or control and management of risks identified during execution of weapons system safety programs.

(5) Serve as member of audit/design review teams in reviewing major acquisition programs to determine compliance with weapons system safety requirements.

(6) Provide the Chair of the Weapon System Explosives Safety Review Board (WSESRB).

e. NAVSEA systems and equipment designers/managers at NAVSEA Headquarters; naval shipyards; planning yards; SUPSHIPS; Naval Surface Warfare Center, and Naval Undersea Warfare Center activities, divisions, and detachments; Naval Ordnance Center divisions and weapons stations:

(1) Ensure that a system safety program is tailored for programs in accordance with reference (c), and implemented and maintained for all phases of the program.

(2) Designate a point of contact for all safety matters for the program.

(3) Ensure that all ECPs, technical manuals, and other documents receive proper review for safety before issue or change. Coordinate changes with affected field activity organizations.

(4) Analyze historical safety deficiency reports, failure analyses, and mishap investigations and recommend corrective action. Sources include Accident Injury Database (NAVSAFECEN), SAFEORD (NAVORDCEN, N-71), and NAVSEA Ship Safety Databases (SEA 03D7).

f. SUPSHIPS shall ensure that the contractual safety requirements of respective ship specifications, section 077, are complied with for new ship design and construction.

g. SUPSHIPS, Navy Shipyards, and Planning Yards shall ensure that the safety requirements of General Specifications for Overhaul (GSO), section 077, are complied with during repair and overhaul of Navy ships.

8. Exceptions:

a. Executive Order 12344 and Public Law 98-525 (42 USC 7158 note) establish the responsibilities and authorities of the Deputy Commander, Nuclear Propulsion Directorate (NAVSEA 08) who is also the Director, Naval Nuclear Propulsion Program, NOON, in the office of the Chief of Naval Operations over all facilities and activities which comprise the Program, a joint Department of Energy (DOE)/Navy organization. These responsibilities and authorities include prescribing and enforcing standards and regulations for the safety of reactors and associated naval nuclear propulsion plants. Nothing in this instruction supersedes or changes these responsibilities and authorities. Accordingly, this instruction is not applicable to Naval Nuclear Propulsion Program facilities and activities.

b. The PEOs and DRPMs are responsible for all technical and safety matters pertaining to PEO/DRPM cognizant technical and safety matters in accordance with reference (a). Accordingly, the PEO/DRPM will be consulted in all matters relating to or affecting PEO/DRPM systems, equipments, and support facilities. NAVSEA provides engineering and technical support, including system safety engineering support, to the PEOs/DRPMs in accordance with an operating agreement approved by the ASN(RD&A).

G. R. STERNER

Distribution: (1 copy each unless otherwise indicated)
NAVSEA Special List Y2
SEA 03D7 (25)
SEA 09A1 (5)
NSWC
NUWC
NAVORDCEN
Naval Publications and Printing Office, NDW

(Distribution continued, next page)

Distribution continued

Stocked: 25 copies
Defense Distribution Depot
Susquehanna Pennsylvania
Bldg 05
5450 Carlisle Pike
Mechanicsburg, PA 17055-0789

Copy to: (1 copy each unless otherwise indicated)
PEO-MIW
PEO-SUB
PEO-TAD
PEO-USW
DRPM-AEGIS
SNDL A1J ASN(RD&A)
A3 CNO
A5 BUMED
A6 CMC
FF5 NAVSAFECEN
FH15 NAVENPVNMEDU
FH25 NAVREGMEDCEN
FH26 NAVENVIRHLTHCEN
FKA1A COMNAVAIRSYSCOM
FKA1B COMSPAWAR
FKA1C COMNAVFACENGCOM
FKA1F COMNAVSUPSYSCOM
FKM27 NPPSMO
FKP7 NAVSHIPYD
FT88 EDOSCOL

GUIDE FOR TAILORING SYSTEM SAFETY PROGRAM REQUIREMENTS

1. System safety engineering, as an element of systems engineering, involves the application of scientific and engineering principles for the timely identification of hazards and initiation of the actions necessary to eliminate, control, or reduce the associated risk of hazards to an acceptable level. The degree of safety achieved in a system is directly dependent upon the emphasis given by the managing activity. This emphasis must be applied by the government and contractors during all phases of the life cycle. Design safety is a prelude to operational safety. The goal is to produce a product that will have negligible operational safety requirements or restrictions.

2. The managing activity should be aware that the issue of safety creates conflicting incentives for designers and developers of systems which include but are not limited to hardware, software, processes, procedures, training, facilities, and construction. Naturally, they have an incentive to avoid serious, flagrant hazards that may jeopardize the future of the program or cause them to incur liability for subsequent accidents. However, if safety problems are allowed to be created and remain undetected until late in the program, the fixes can wreak havoc on budgets and schedules.

3. A System Safety Program (SSP) must be tailored to meet the needs of the particular system. The SSP requirements may be as simple as a safety assessment report for a non-developmental item (NDI) that shows the system has a safe operating history, does not require adaptation to the marine environment, or any other modification for safe use on Navy ships. Conversely, a more complex system may require a more complete evaluation of the system from concept studies through disposal. The system may also require special types of analyses, e.g., fault tree analysis, hazardous material use and/or disposal analysis, or shock qualification analysis.

4. In tailoring the SSP, the managing activity must define the detail and depth of effort, and incorporate them into contractual documents. Additionally, the managing activity must define the acceptable level of risk for the design. The following task information is provided to assist the managing activity in developing the SSP. Additional guidance in tailoring SSS-STD-882 safety tasks for a particular program is available from the Human Systems Integration Division, NAVSEA 03D7.

a. Task Selection. Table 1, duplicated from Appendix A of SSS-STD-882, lists the management and engineering safety tasks to be considered by program phase. It is intended as a "shopping guide" for the managing activity and the safety manager to use in tailoring a system safety program.

TABLE 1. APPLICATION MATRIX FOR SYSTEM PROGRAM DEVELOPMENT

TASK	TITLE	TASK TYPE	PROGRAM PHASE 0	I	II	III	IV
101	SYSTEM SAFETY PROGRAM (SSP)	MGT	G	G	G	G	G
102	SYSTEM SAFETY PROGRAM PLAN (SSPP)	MGT	G	G	G	G	G
103	INTEGRATION/MANAGEMENT OF ASSOCIATE CONTRACTORS, SUBCONTRACTORS, AND AE FIRMS	MGT	S	S	S	S	S
104	SYSTEM SAFETY PROGRAM REVIEW/AUDITS	MGT	S	S	S	S	S
105	SSG/SSWG SUPPORT	MGT	G	G	G	G	G
106	HAZARD TRACKING AND RISK RESOLUTION	MGT	S	G	G	G	G
107	SYSTEM SAFETY PROGRESS SUMMARY	MGT	S	G	G	G	G
201	PRELIMINARY HAZARD LIST (PHL)	ENG	G	S	S	S	N/A
202	PRELIMINARY HAZARD ANALYSIS (PHA)	ENG	G	G	G	GC	GC
203	SAFETY REQUIREMENTS/CRITERIA ANALYSIS	ENG	G	S	S	S	GC
204	SUBSYSTEM HAZARD ANALYSIS (SSHA)	ENG	N/A	G	G	GC	GC
205	SYSTEM HAZARD ANALYSIS (SHA)	ENG	N/A	G	G	GC	GC
206	OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA)	ENG	S	G	G	GC	GC
207	HEALTH HAZARD ASSESSMENT (HHA)	ENG	G	G	G	GC	GC
301	SAFETY ASSESSMENT	ENG	S	S	S	S	S
302	TEST AND EVALUATION SAFETY	ENG	G	G	G	G	G
303	SAFETY REVIEW OF ENGINEERING CHANGE PROPOSALS, SPECIFICATION CHANGE NOTICES, SOFTWARE PROBLEM REPORTS, AND REQUESTS FOR DEVIATION/WAIVER	ENG	N/A	G	G	G	G
401	SAFETY VERIFICATION	ENG	S	G	G	S	S
402	SAFETY COMPLIANCE ASSESSMENT	ENG	S	G	G	S	S

NOTES:

TASK TYPE
- ENG - System Safety Engineering
- MGT - System Safety Management

PROGRAM PHASE
- 0 - Concept exploration
- I - Demonstration/validation
- II - Engineering/manufacturing Development
- III - Production/deployment
- IV - Operations/support

APPLICABILITY CODES
- S - Selectively Applicable
- G - Generally Applicable
- GC - Generally Applicable to Design Change Only
- N/A- Not Applicable

b. Risk Assessment. Each identified/validated hazard is assigned a Risk Assessment Code (RAC) by the activity safety office. The RAC represents the degree of risk associated with the deficiency and combines the elements of hazard severity and mishap probability. The following sample RAC is derived as follows:

(1) Hazard Severity Categories. A qualitative measure of the worst credible mishap resulting from human error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction. A hazard severity category is assigned by Roman numeral according to the following criteria:

• Category I - Catastrophic. May cause death, system loss (e.g., a system casualty affecting the ship's mission), or severe environmental damage.

• Category II - Critical. May cause severe injury, severe occupational illness, major system damage or major environmental damage.

• Category III - Marginal. May cause minor injury, minor occupational illness, minor system damage, or minor environmental damage.

• Category IV - Negligible. Will result in insignificant injury, insignificant occupational illness, insignificant system damage, or insignificant environmental damage.

(2) Mishap Probability. The mishap probability is the probability that a hazard will result in a mishap, based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and affected population. Mishap probability is assigned an Arabic letter according to the following criteria:

• Subcategory A - Likely to occur immediately or within a short period of time.

• Subcategory B - Probably will occur in time.

• Subcategory C - May occur in time.

• Subcategory D - Unlikely to occur.

(3) Risk Assessment Code (RAC). The RAC is an expression of risk that combines the elements of hazard severity and mishap probability. Using the sample matrix shown below, the RAC is expressed as a single Arabic number that can be used to help determine hazard abatement priorities.

HAZARD SEVERITY	MISHAP PROBABILITY			
	A	B	C	D
Category I	1	1	2	3
Category II	1	2	3	4
Category III	2	3	4	5
Category IV	3	4	5	5

RAC
1-Critical
2-Serious
3-Moderate
4-Minor
5-Negligible