DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO
OPNAVINST 5100.24B
CNO (N09F)
FEB 0 6 2007

OPNAV INSTRUCTION 5100.24B

From: Chief of Naval Operations

Subj: NAVY SYSTEM SAFETY PROGRAM POLICY

Ref:
(a) DOD Directive 5000.1
(b) DOD Instruction 5000.2, Operation of Defense Acquisition System, of 12 May 03
(c) SECNAVINST 5000.2C
(d) SECNAVINST 5100.10J
(e) MIL-STD-882D, Standard Practice for System Safety, of 10 Feb 00
(f) SECDEF Memorandum, Reducing Preventable Mishaps, of 22 Jun 06
(g) USD AT&L Memo, Defense Acquisition System Safety, of 23 Sep 04
(h) MIL-HDBK 46855A, Human Engineering Program Process and Procedures, of 17 May 99
(i) SECNAVINST 5420.188F
(j) NAVFACINST 5100.11J, NAVFACENGCOM Safety and Health Program, of 18 Jan 00
(k) Department of the Navy (DON) Acquisition and Capabilities Guidebook, of Feb 05
(l) Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3170.01E, Joint Capabilities Integration and Development System, of 11 May 05
(m) Chairman, Joint Chiefs of Staff Manual (CJCSM) 3170.01B, Operation of the Joint Capabilities Integration and Development System, of 11 May 05
(n) DOD Instruction 7000.14, DOD Financial Management Policy and Procedures, of 3 Mar 06
(o) SECNAVINST 4105.1A
(p) NAVSO P-3692, Independent Logistics Assessment Handbook, Department of the Navy Guide for Conducting Independent Logistics Assessments, of Sep 06
(q) OPNAVINST 5100.8G
(r) OPNAVINST 5450.180D
(s) OPNAVINST 5102.1D/MCO P5102.1B
(t) OPNAVINST 8020.14/MCO P8020.11
(u) OPNAVINST 3960.16A

(v) NAVSEAINST 5100.12A, Requirements for Naval Sea Systems Command Systems Safety Program for Ships, Shipborne Systems, and Equipment, of 20 Jan 05
(w) DOD Guide to Integrated Product and Process Development (Version 1.0) of 5 February 96
(x) SECNAVINST 4855.3B, Product Data Reporting and Evaluation Program (PDREP), of 22 Dec 05
(y) SECNAVINST 4140.2, Management of Aviation Critical Safety Items, of 25 Jan 06
(z) OPNAVINST 5100.23G
(aa) OPNAVINST 5100.19D
(bb) BUMEDINST 6270.8A, Procedures for Obtaining Health Hazard Assessments (HHAs), of 3 Jan 02
(cc) OPNAVINST 5100.27A/MCO 5104.1B
(dd) SECNAVINST 5100.14D
(ee) OPNAVINST 5420.70F
(ff) OPNAVINST 4730.5P
(gg) OPNAVINST 9080.4B
(hh) NAVSEAINST 8020.6D, Navy Weapon System Safety Program, of 15 Jan 97
(ii) NAVSEAINST 9310.01B, Naval Lithium Battery Safety Program, of 13 Jun 91
(jj) OPNAVINST 3500.39B/MCO4500.27B

Encl: (1) System Safety Definitions
(2) Acronyms
(3) Supplemental Guidance to Tailoring a System Safety Program and Process
(4) Guidelines for Identifying Key System Safety Needs in Capability Documents and Subsequent Program Documents

1. Purpose. To delineate Chief of Naval Operations (CNO) policy on system safety. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 5100.24A.

3. Objective. The objective of this instruction is to provide policy for the implementation of system safety in the Department of the Navy in support of references (a) through (d) and throughout all phases of the Joint Capabilities Integration and Development System (JCIDS) and the Department of Defense acquisition process consistent with reference (e). The objectives of the system safety policy are to eliminate or reduce associated mishap risks and thereby improve operational readiness, reduce life cycle cost, and increase environmental and safety and occupational health for all acquisition programs,

over the entire program life cycle supporting the goals of reference (f).

4. Background

a. The Department of Defense (DoD) and the Department of the Navy (DON) have directed that safety is an inherent responsibility of command. Operational readiness requires the application of principles of risk management through early identification and resolution of hazards and associated mishap risks in the acquisition framework to protect personnel and prevent the loss or degradation of systems. Protection of personnel is critical. Rapid development of technologies and application of system safety to the acquisition process are essential to ensure effective evaluation of hazards, consideration of the user community in design, and risk acceptance at a management level consistent with potential mishap risk. References (a) through (d), (f), and (g) emphasize DoD's and DON's commitment to personnel safety and health, environmental protection, and mission effectiveness through proper application of system engineering and Human Systems Integration (HSI) using references (b), (e), and (h). This instruction is the result of a collaborative effort that included Navy and Marine Corps acquisition community and systems engineering representation. It was determined during this process that System Safety is adequately addressed for the acquisition activities of the Marine Corps, which include activities with Army and Navy sponsorship. System Safety Policy is addressed in the Marine Corps Systems Command ESOH Handbook, http://www.marcorsyscom.usmc.mil/sites/safety/default.asp published by MARCORSYSCOM, who serves as Marine Corps focal point for System Safety. Consequently a combined OPNAV Instruction and Marine Corps Order (MCO) addressing System Safety was not needed.

b. The Assistant Secretary of the Navy (Research, Development & Acquisition) (ASN (RD&A)) is responsible for ensuring DON Science and Technology (S&T) projects and acquisition programs comply with DON environmental, safety and occupational health (ESOH) policy and is the focal point for all DON S&T and acquisition ESOH issues in accordance with reference (c). ASN (RD&A) is the mishap risk acceptance authority for "high" risk in accordance with references (b), (c) and (e). The ASN (RD&A) Chief Engineer's Office (CHENG) provides oversight for the integration of ESOH into the system engineering process.

c. The Assistant Secretary of the Navy (Installations and Environment) ((ASN I&E)) is responsible for formulating DON ESOH policy per references (c) and (d). ASN (I&E), or designee, as a program decision principal advisor per with references (c) and (i), is authorized to participate in program decision meetings (PDMs). The Deputy Assistant Secretary of the Navy (Safety) (DASN(S)) is responsible for safety and occupational health policy for the ASN (I&E), relative to system safety including system safety management/engineering and independent safety assessments during system acquisition and MILCON program reviews. In addition, ASN, (I&E), per references (c) and (d), assists ASN (RD&A) by:

(1) Providing support for acquisition program decisions by attendance or designation of a representative at program decision meetings.

(2) Supporting the system safety review process by participation in system safety reviews or designation of attendant representatives upon request and in conjunction with other program reviews such as Integrated Logistics Assessments (ILAs).

(3) Providing representation to the System Safety Advisory Board (SSAB).

5. Applicability. System safety, as defined in this instruction, is applicable to systems command support for all Navy acquisition programs defined to include: new and existing systems, sub-systems, equipment, software programs to include any associated research and development, construction, modification, modernization, overhaul, repair, and disposal. Facility system safety requirements are further delineated in reference (j). Operational commanders, requirements officers, and resource sponsors shall support the system safety program. This instruction applies to both developmental and non-developmental items and provides supplemental guidance to support implementation of the requirements of references (c), (d), (g), and the guidance of reference (k). This instruction supports the integration of system safety into the acquisition and JCIDS processes per references (l) and (m).

6. Navy System Safety Policy. Reference (c) requires program sponsors, acquisition commands and their field activities (including contractor support), and research and development commands to administer the system safety engineering and risk management process by applying reference (e) to all

developmental and sustaining engineering activities. The goal of the system safety program is to increase operational readiness by reducing the likelihood of mishaps and unnecessary expenditures of funds to correct hazards identified during initial development and throughout the life cycle of system development. Facilities engineering and military construction (MILCON) projects shall use system safety principles under direction of the Naval Facilities Engineering Command (NAVFAC) per reference (d) and as specified in reference (j). Definitions, descriptions and acronyms used in system safety are listed and defined in enclosures (1) and (2). Control of life cycle cost is a vital consideration in acquisition. Application of the system safety process supports cost and risk management in adherence to reference (n). Reference (a) through (c) requirements for application of the system safety process, are delineated by reference (e), as supplemented by guidance in enclosure (3), to ensure that:

a. All acquisition programs, as directed by references (a), (b), (c), (d) and (g), provide for the identification, evaluation and elimination, reduction and control, review and ultimate acceptance of residual safety, health and environmental hazards at a management level consistent with their level of risk. This begins prior to system production/construction and continues during operations and support (deployment) in order to minimize life cycle cost and programmatic risk. The acceptance authority for risk is defined by the mishap risk classification consistent with references (b), (c) and (e).

b. System safety mishap risk requirements, criteria and constraints shall be addressed by the originators of each operational capability requirement and summarized in the JCIDS documents. The capability to operate and sustain systems and equipment without undue mishap risk to the user community is essential to development, fielding and sustainment of effective military capabilities, and must be reflected in Initial Capabilities Document (ICD), Capabilities Development Document (CDD), and Capability Production Document (CPD) per references (c), (l) and (m). Guidance for addressing safety capabilities of new systems and equipment and ensuring appropriate requirements for risk management are provided in enclosure (4). Naval Safety Center and U.S. Coast Guard data indicate that the majority of mishaps on-board ships are the direct result of human error; therefore reduction of the potential for mishaps must address design to reduce the incidence of human error and to make systems error-tolerant as described in reference (h).

c. Requests for proposals and invitations for bid on system acquisitions and contracts should support reference (a) through (c) requirements by specifying reference (e) and appropriate system safety tasks and analyses. Enclosure (3) and the Naval Safety Center Acquisition Safety webpage at: http://safetycenter.navy.mil/acquisition/default.htm may be used as a guide to help determine system safety tasks, as appropriate.

d. Contractual system safety provisions are reviewed for currency prior to the start of the design and during the acquisition program review at each applicable milestone.

e. Engineering Change Proposals (ECPs), Requests for Deviations (RFDs), waivers, alterations, and modifications, documenting system safety impacts, including residual mishap risk, are reviewed using the system safety risk management process, prior to acceptance.

f. Milestone reviews consider status of the acquisition programs and include evaluation of the system safety program and assess compliance/conformance with the program's risk management strategy consistent with reference (c). Table 2 of Enclosure (3), provides guidance for inserting safety and occupational health into acquisition programs and milestones. The status of the system safety program shall be documented in the Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE), required by reference (b). ILAs, per references (o) and (p), should consider the status of safety, health and environmental programs and review system safety program documents, the Systems Engineering Plan (SEP), the HSI plan and PESHEs in accordance with reference (b). The Human Factors Engineering (HFE) effort within the HSI program will define the process for designing human machine interfaces to enhance safety and reduce the potential for human error as described in references (b) and (h).

g. System safety management incorporates all appropriate (ESOH) specialty areas. Enclosure (3) provides a listing of some applicable ESOH specialty areas and associated requirements references.

7. Responsibilities

a. The Chief of Naval Operations (CNO). The CNO shall develop acquisition system safety requirements, recommend mandatory acquisition system safety policy, assist in system

safety policy implementation, review system safety related documentation, and provide system safety advice and assistance to acquisition personnel.

(1) The Special Assistant for Safety Matters (CNO (N09F)) shall advise and assist the CNO in reviewing Navy system safety program policies, objectives, and effectiveness in accordance with references (q) and (r). CNO (N09F) shall support ASN (RD&A) in developing safety and occupational health requirements, recommending policy, assisting in safety and occupational health policy implementation, reviewing safety and occupational health related documentation, and providing safety and occupational health assistance to acquisition personnel. In accordance with the reference (c) requirement that CNO establish ESOH advisory boards, CNO N09F will establish and chair a SSAB to provide guidance for implementation of system safety programs. The SSAB will not supersede or replace existing ESOH advisory boards. The SSAB will be available to support Project Managers (PMs) and milestone decision authorities upon request.

(2) Commander, Naval Safety Center shall:

(a) Act as the data repository and center of expertise for mishap and hazard information, communicate safety hazards to relevant Program Executive Offices (PEOs), PMs, acquisition commands, or other appropriate technical authority, and provide technical support for the identification of safety issues and hazards to PMs and acquisition commands in accordance with references (d), (q), (r) and (s).

(b) Maintain safety expertise relevant to each major platform and category of operational activity. Such expertise should be provided by platform analysts who have fleet experience with particular weapons systems/platforms. These analysts should liaise with the program office(s) relevant to systems under their purview and should participate in program support activities such as membership in system safety working groups.

(3) CNO (N1/NT)is responsible for supporting the PEOs, Systems Commands (SYSCOMs), and Direct Reporting Program Managers (DRPMs) in linking technology that reduces manpower and personnel requirements and life cycle costs throughout a program's life cycle. CNO (N1/NT) and CMC (DC, MR&A) provide guidance to CNO (N09F), SYSCOMs and PEOs in HSI areas to support designs that maximize user community capabilities and system efficiency while reducing risk of injury. CNO (N173), in consultation with N09F, PEOs, and SYSCOMs, will identify

associated training areas and may distinguish the limitations of training in achieving desired system performance and system safety objectives.

(4) CNO (N4) (Deputy Chief of Naval Operations (Fleet Readiness and Logistics)) provides policy, resources, structures, and mechanisms to meet defined readiness requirements of Navy operating forces and their associated shore installations. In accordance with reference (c), CNO (N4) shall support ASN (RD&A) in developing environmental requirements, recommending policy, assisting in environmental policy implementation, reviewing environmental related documentation, and providing environmental assistance to acquisition personnel. Additionally, in accordance with reference (t), CNO (N4) shall provide overall direction and resources for DON explosives safety review, oversight, and verification functions.

(5) CNO (N8), and related program sponsors execute the JCIDS process for DON. Per references (l) and (m), ESOH considerations shall be addressed as part of the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF), and policy considerations or other system attributes sections. Enclosure (4) provides guidelines and examples for incorporating ESOH considerations in JCIDS.

(6) CNO (N091) ensures that Navy Test and Evaluation (T&E) includes evaluation of safety and health for those involved in testing as well as the user community, in accordance with references (b), (c), and (u).

b. Milestone Decision Authorities (MDAs), PEOs and PMs. Regardless of their program's acquisition category, per reference (c), are responsible for ensuring that system safety risk management is integrated into their overall systems engineering and risk management processes. References (b), (c), (g) and (v) require PMs to use reference (e) in all developmental and sustaining engineering activities. In addition, Naval Sea Systems Command (NAVSEA) reference (v) requires PMs to develop, resource and sustain an HSI Plan that supports all phases of system acquisition and modernization. PMs will ensure that reference (b) requirements to use a system safety process in order to integrate ESOH into the system engineering process are documented in the SEP. Hardware, software, and support should all be considered in the system safety process. PMs are required by reference (c) to identify system safety hazards, assess the mishap risks, and then report on their program's system safety measures and the status of

residual risk acceptance decisions at the appropriate levels. The Integrated Product Team (IPT) process is the preferred tool to ensure cross-disciplinary consideration of risk factors and management in the design process per reference (w).

c. Systems Commands, Naval Air Systems Command (NAVAIR), NAVSEA, Naval Supply Systems Command (NAVSUP), Space and Naval Warfare Systems Command (SPAWAR), Support Commands and Research & Development (R&D) Organizations. Ensure the promotion and monitoring of system safety assessments related to the acquisition of systems, sub-systems, materials, equipment, Critical Safety Items (CSI), and software under their purview during research and development, new construction, modernization, repair, and overhaul. All Navy warrant holders and technical authorities should include system safety in the execution of their technical authority, as appropriate. Systems Commands, Support Commands and R&D Organizations provide technical support for the SSAB as required. NAVFAC system safety responsibilities are further delineated in reference (j).

d. Operational Commands/Combatant Commands/Type Commands. Identify and communicate hazards arising during operation and maintenance of systems, support system safety processes, and provide operational advisory groups of fleet representatives for support of system acquisition and life cycle management. References (x) and (y) provide guidance and criteria on reporting of material deficiencies, including safety issues and those that may require product improvements. Reference (z) addresses aviation critical safety items. Mishap reporting should also consider issues that may be addressed in future designs. Reference (s) provides requirements for mishap reporting, further guidance is available at: http://www.safetycenter.navy.mil/wess/default.htm. Operational Commands/Combatant Commands/Type Commands provide technical support for the SSAB as required.

e. The Chief, Bureau of Medicine and Surgery (BUMED)

(1) Support the ASN (RD&A) in integrating occupational health considerations into S&T projects and the systems engineering process of acquisition programs per enclosure (7) of reference (c) requirements.

(2) Provide health hazard assessments when requested by PMs, per references (aa), (c), and (cc).

(3) Provide Occupational Health (OH) support and data, at the request of the PMs and system safety lead, in all aspects of OH which includes occupational medicine (medical treatment and surveillance), industrial hygiene, environmental health, and radiation health; including field support as stated throughout references (aa) and (cc).

(4) Participates on the Laser Safety Review Board (LSRB), which provides a system safety review of all DON lasers used in combat, combat training, or classified in the interest of national security and all lasers capable of exceeding class 3A levels, including those used in optical fiber communication systems, in accordance with references (dd) and (ee).

f. The Director of Naval Nuclear Propulsion Program CNO (N00N). Following outlined responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by Public Laws 98-525 and 106-65), and ensuring consistency throughout the joint Navy/Department of Energy organization of the Naval Nuclear Propulsion Program, shall develop, implement and oversee all policy and practices pertaining to system safety and this instruction for activities under the Director's cognizance.

g. Commander, Operational Test and Evaluation Force (COMOPTEVFOR). Performs independent tests and evaluations of acquisition products for DON, in accordance with references (c) and (u). They provide an independent evaluation of how well the material solution meets the defined operational requirements. Their inputs support oversight of the acquisition process.

h. The President, Board of Inspection and Survey (PRESINSURV). Develops and establishes CNO policy and procedures for trials, material inspections, and surveys of ships and service craft consistent with law, regulations, and the terms of contracts; examines naval vessels periodically by a board of naval officers to determine fitness for further service; conducts material inspections and surveys of ships and service craft and provides assessment of the material readiness of these vessels; provides independent verification of a newly constructed ship's readiness for acceptance/delivery and to determine if builder responsible equipment is operating satisfactorily during the guarantee period following acceptance; and conducts environmental protection and safety and occupational health oversight inspections of naval ships to include equipment, program compliance, and training. References

(ff), (gg) and (hh) outline the role and responsibilities of PRESINSURV.

i. Naval Ordnance Safety & Security Activity (NOSSA). Provides the Chairperson and Secretariat of the Weapon System Explosives Safety Review Board (WSESRB).

(1) WSESRB is responsible for reviewing and advising DON weapon system acquisition programs, including energetic systems, weapon devices and those systems that manage and control weapons to ensure that system safety and ordnance environmental aspects are met prior to introduction to the fleet in compliance with the requirements of reference (t). WSESRB operations are delineated by reference (ii). The WSESRB and SSAB collaborate in the exchange of safety information and may share membership.

(2) Software System Safety Technical Review Panel (SSSTRP) is a sub-panel of the WSESRB established to review the complex safety issues related to software control of weapon systems. The SSSTRP provides expert technical review of software intensive systems or where the only modifications to the system have been in software.

(3) Fuze and Initiation Systems Technical Review Panel (FISTRP) is a sub-panel of the WSESRB established to provide expert technical review of the safety programs for fuze designs including electronic safe and arm devices, ignition safety devices, and related safety and arming devices used in Navy weapon systems. The FISTRP interfaces with the Army Fuze Safety Review Board and Joint Service Fuze Standardization and Engineering Working Group.

(4) Lithium battery safety program is managed by NOSSA Electrical Safety Lithium Battery Branch. The Navy's lithium battery safety program applies to all lithium battery powered devices intended for use or transport on Navy facilities, ships and aircraft regardless of source. Requirements for the lithium battery safety program are contained in reference (jj).

(5) Insensitive Munitions (IM) are also a part of the weapon systems program and are a NOSSA responsibility. The IM Review Board (IMRB) consisting of IM Subject Matter Experts (SME's) review all IM qualification test results and provides recommendations to the WSESRB.

j. Laser Safety Review Board (LSRB). The LSRB provides a systems safety review of all DON lasers used in combat, combat

training, or classified in the interest of national security and all lasers capable of exceeding class 3A or class 3R levels, including those used in optical fiber communication systems. This includes systems that are used by other military services and lasers previously registered with the Federal Drug Administration (FDA) for which modifications in design or use are intended. The LSRB does not review lasers planned solely for experimental laboratory, industrial, or medical use. Additionally, the LSRB acts as a source of laser safety guidance for any systems regardless of their intended use and can be convened to address issues.

8. Implementation

a. CNO supports ASN (RD&A) in developing system safety acquisition requirements and assists in policy implementation by reviewing system safety related documentation, providing system safety related guidance and assistance to acquisition personnel and programs, verifying that identified mitigation measures achieve mishap reduction objectives, and ensuring that accepted mitigation measures are implemented.

(1) The Special Assistant for Safety Matters (CNO (N09F)):

(a) Supports the program sponsors in identifying system safety associated risk factors and necessary capabilities for existing and proposed systems.

(b) May provide support to acquisition programs through participation in IPTs, ILAs and similar working groups.

(c) Establishes and coordinates the SSAB under the authority of reference (c), paragraph 7.3.3, requiring CNO to establish ESOH Advisory Boards. The SSAB will advise the PEOs, PMs, and acquisition commands in evaluating and enhancing the effectiveness of system safety for their respective programs to minimize risk. The SSAB may, if requested by the MDA or the PM, conduct an assessment of the programs' system safety documentation and/or system safety programmatic requirements. The SSAB does not supersede the requirement to be reviewed by other review boards. The SSAB will consist of key personnel as established in the SSAB Charter. The SSAB will consult with ASN (RD&A) CHENG and provide guidance for integrating system safety into the systems engineering process.

(2) The Naval Safety Center:

(a) Provides data, when requested by systems commands, PEOs, and PMs, to assist in identification of safety and health hazards associated with legacy systems, in accordance with references (q) (r), (ii) and (kk).

(b) Informs appropriate SYSCOMs, PEOs and PMs of any hazards identified through mishap investigations, trend analyses, or other Naval Safety Center functions.

(c) Provides platform analysts to participate in the SSAB as required.

b. MDA in accordance with references (b) and (c):

(1) Ensures that all identified hazards have been adequately addressed and accepted at the appropriate authority level.

(2) Ensures milestone documentation includes a PESHE.

c. PEOs/SYSCOM Commanders, or Flag-level or Senior Executive Service (SES) designees/DRPMs, Chief of Naval Research (CNR) are the acceptance authorities for serious ESOH risks as defined in references (b) and (e).

d. Program Managers (PMs). PMs shall implement system safety on all acquisition programs as required by references (b), (c), (e) and (g). PMs are the risk acceptance authority for medium/low ESOH risks per references (b) and (e). Key considerations include:

(1) Documenting the system safety engineering approach.

(2) Designating in writing a system safety lead for each program. Suggested minimal qualifications for the system safety lead are provided in enclosure (3).

(3) Ensuring the contractor led system safety effort is integrated into the government system safety program. This teaming arrangement does not preclude the responsibility to ensure and verify contractor performance.

(4) Ensuring that there is a formal closed loop process for managing hazards. Per references (b) and (e) requirements, no hazards shall be closed until the mitigating measure's implementation has been verified and the residual mishap risk accepted by the appropriate authority. All residual mishap risks must be accepted prior to fielding.

(5) Ensuring organizational structures and resources are adequate to perform required system safety program actions. This should include establishing a system safety working group comprised of government and contractor representatives, who are responsible for implementing specific safety program requirements.

(6) Ensuring the identification of recommended CSIs for naval aviation programs in accordance with reference (z).

(7) Formally integrating the system safety program into the acquisition process by:

(a) Integrating system safety into the systems engineering, risk management processes, and human systems integration processes, as documented in the SEP.

(b) Documenting the system safety program status and plan in the PESHE.

(c) Including the system safety program requirements and criteria in acquisition documentation, requests for proposals, specifications, and statements of work.

(d) Ensuring that residual risk acceptance decisions are presented at technical and program reviews.

(e) System safety representation across the program IPT structure to ensure cross-functional support for the system safety program.

(f) Integrating system safety with the other elements of HSI.

(8) Establishing procedures to identify and manage hazards that are discovered post-fielding, and document associated mishap risk acceptance decisions and communicate the mishap risks and required actions to the fleet as appropriate. The process should include proactive review of fleet feedback such as those provided by execution of references (x) and (y).

(9) Providing safety releases for all test events involving personnel Operational Test Readiness (OPT) certification criterion involving safety in reference (c) satisfies this requirement for Operational Test & Evaluation (OT&E) performed by COMOPTEVFOR.

(10) Reviewing engineering changes, alterations, deviations, waivers, and modification proposals for impact on safety.

(11) Maintaining a permanent record of identified hazards and closeout actions consistent with reference (e). Copies of system safety program documentation should be forwarded to CNO (N09F) and the Naval Safety Center as appropriate.

(12) Ensure that HSI processes are implemented to design human machine interfaces in compliance with human factors engineering standards and criteria, to reduce the incidence of human errors, to make systems error tolerant, to reduce the incidence of ergonomic injuries, and to enhance human performance, as described in reference (h).

e. BUMED. The BUMED shall support acquisition commands, test and evaluation organizations and NAVFAC in risk assessment of new systems and facilities in accordance with references (c), (d), (aa), and (cc).

f. SYSCOMs shall:

(1) Establish a command point of contact for system safety.

(2) Establish and maintain a capability to conduct system safety assessments by:

(a) Defining command system safety objectives, guidance, and policy.

(b) Ensuring organizational structures and resources are adequate to perform required system safety program actions.

(c) Ensuring that system safety personnel are trained.

(d) Ensuring system safety guidance is appropriately conveyed in contracts.

(e) Integrating system safety into systems engineering, risk management and human systems integration processes.

(f) Ensuring R&D project efforts include safety criteria, critical items and hazards identified as part of the project documentation.

(3) When performing testing, ensure the requirements in the Safety Release are followed and system safety requirements are addressed.

(4) When reviewing engineering changes, alterations, deviations, waivers, and modification proposals, evaluate the impact on safety of the change to the system and interfaces.

(5) Provide representation to the SSAB.

(6) Ensure that system safety is fully integrated with the other elements of HSI.

g. NAVFAC, is required to apply system safety process and evaluation to support facility safety in design in accordance with references (d) and (j).

h. Operational Commands/Type Commands shall:

(1) When identifying capabilities gaps through the JCIDS process, consider the recommendations detailed in enclosure (4) that may affect safety.

(2) Support the system safety process by participating in working groups as appropriate.

(3) Participate in the mishap risk review process per references (e) and (kk).

(4) Include operational expert representation from any areas of safety concern on all Operational Advisory Groups (OAGs).

R. F. Willard

R. F. WILLARD
Admiral, U.S. Navy
Vice Chief of Naval Operations

Distribution:
Electronic only, via Department of the Navy Issuances Website
http://doni.daps.dla.mil

SYSTEM SAFETY DEFINITIONS

1. Terms Defined. The following terms and their definitions, listed in alphabetical order, will aid in interpreting this instruction and in the continued administration of Navy system safety program policies and procedures. This is a partial list of definitions and descriptions most commonly used in a system safety program (SSP). For additional assistance, definitions, descriptions, and acronyms, refer to the Defense Acquisition University Dictionary of Acquisition Terms and Acronyms at: http://akss.dau.mil/jsp/glossary.pdf. Reference (k) provides a more extensive list of system safety terms.

a. Acquisition Program. A directed, funded effort that provides a new, improved, or continuing materiel, weapon or information system or service capability in response to an approved need. Acquisition programs are divided into categories that are established to facilitate decentralized decision-making, execution, and compliance with statutory requirements.

b. Critical Safety Item (CSI). A part, an assembly, installation equipment, launch equipment, recovery equipment, or support equipment for an aircraft or aviation weapon system if the part, assembly, or equipment contains a characteristic any failure, malfunction, or absence of which could cause a catastrophic or critical failure resulting in the loss of or serious damage to the aircraft or weapon system, an unacceptable risk of personal injury or loss of life, or an uncommanded engine shutdown that jeopardizes safety.

c. Hazard. Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

d. Hazardous Material. Any material that, because of its quantity, concentration, or physical, chemical, or infectious characteristics, may pose a substantial hazard to human health or the environment.

e. Human Systems Integration (HSI). Includes the integrated and comprehensive analysis, design, assessment of requirements, concepts and resources for system manpower, personnel, training, safety and occupational health, habitability, personnel survivability, and human factors engineering.

f. Joint Capabilities Integration and Development System (JCIDS). JCIDS is defined in CJCSI 3170.01E. JCIDS supports the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Requirements Oversight Council (JROC) in identifying, assessing, and prioritizing joint military capability needs as required by law. The capabilities are identified by analyzing what is required across all functional areas to accomplish the mission.

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. Mishap Risk. An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.

i. Non-Developmental Item (NDI). An NDI is any previously developed item of supply used exclusively for government purposes by a federal agency, a state or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above that requires only minor modifications or modifications of the type customarily available in the commercial marketplace in order to meet the requirements of the processing department or agency.

j. Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE). The Programmatic ESOH Evaluation (PESHE), including ESOH risks, is a strategy for integrating ESOH considerations into the systems engineering process, identification of ESOH responsibilities, and a method for tracking progress.

k. Residual Mishap Risk. The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence.

l. Safety. Freedom from those conditions that cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

m. System. An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

n. System Safety. The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

o. System Safety Advisory Board (SSAB). The System Safety Advisory Board (SSAB) is an advisory group established by CNO N09F in accordance with reference (c) requirements to provide review of system safety policies affecting multiple systems commands and support the system safety efforts of specific acquisition programs upon request. The SSAB will advise the Program Executive Officers (PEOs), Program Managers (PMs), and acquisition commands in evaluating and enhancing the effectiveness of system safety for their respective programs to minimize risk. The SSAB may, if requested by the MDA or the PM, conduct an assessment of the programs' system safety documentation and/or system safety programmatic requirements. The SSAB will consist of key personnel as established in the SSAB Charter. The SSAB will consult with ASN (RD&A) CHENG and provide guidance for integrating system safety into the systems engineering process.

p. System Safety Lead. The system safety lead, sometimes called the Principal for Safety, is the single point of contact for system safety-related matters. The system safety lead is designated in writing by the program manager and has the authority to speak for them on system safety-related matters. A system safety lead is the technical authority regarding matters of system safety.

q. System Safety Program (SSP). The combined tasks and activities of system safety management and system safety engineering.

r. System Safety Working Group (SSWG). A formally chartered group of persons, representing organizations initiated during the system acquisition program, organized to assist the PM in achieving the system safety objectives. Regulations of the military components define requirements, responsibilities, and memberships.

s. User Community. An operational command or agency that receives or will receive benefits from the acquired system. Combatant Commanders (COCOMs) and their Service Component commands are the users. There may be more than one user for a system. Because the Service Component commands are required to

organize, equip, and train forces for the COCOMs, they are seen as users for systems. The user community spans the life cycle and includes, but is not limited to: operators, maintainers, administrators, support personnel, supervisors, managers/command, trainers, and installers.

ACRONYMS

The following acronyms, listed in alphabetical order, will aid in interpreting this instruction.

AoA	Analysis of Alternatives
ASN (I&E)	Assistant Secretary of the Navy (Installations and Environment)
ASN (RD&A)	Assistant Secretary of the Navy (Research, Development & Acquisition)
BUMED	Bureau of Medicine and Surgery
CDD	Capability Development Document
CHENG	Assistant Secretary of the Navy (RD&A) Chief Engineer's Office
CJCS	Chairman of the Joint Chiefs of Staff
CNO	Chief of Naval Operations
CNR	Chief of Naval Research
COCOM	Combatant Commanders
COMOPTEVFOR	Commander, Operational Test and Evaluation Force
COTS	Commercial-Off-The-Shelf
CPD	Capability Production Document
CSI	Critical Safety Item
CSP	Certified Safety Professional
DASN (S)	Deputy Assistant Secretary of the Navy (Safety)
DC, M&RA	Deputy Commandant Manpower and Reserve Affairs
DCR	Direct Change Recommendation
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
DRPM	Direct Reporting Program Manager
ECP	Engineering Change Proposal
ESOH	Environmental, Safety and Occupational Health
FDA	Federal Drug Administration
FDR	Flight Data Recorders
FOC	Full Operating Capability
FHA	Functional Hazard Assessment
FISTRP	Fuze and Initiation Systems Technical Review Panel
FRP	Full-Rate Production
FRP DR	Full-Rate Production Decision Review
GFE	Government Furnished Equipment
GPWS	Ground Proximity Warning Systems
HERF	Hazards of Electromagnetic Radiation to Fuel
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to Personnel
HHA	Health Hazard Assessment

HSI	Human Systems Integration
HSIP	Human Systems Integration Plan
ICD	Initial Capabilities Document
ILA	Integrated Logistics Assessment
IM	Insensitive Munitions
IMDS	Integrated Material Diagnostic Systems
IOC	Initial Operational Capability
IPT	Integrated Product Team
JCD	Joint Capabilities Document
JCIDS	Joint Capabilities Integration and Development Systems
JFC	Joint Functional Concepts
JROC	Joint Requirements Oversight Council
KPP	Key Performance Parameters
LSRB	Laser Safety Review Board
MDA	Milestone Decision Authority
MFOQA	Military Flight Operations Quality Assurance
MILCON	Military Construction
NAVAIR	Naval Air Systems Command
NAVFAC	Naval Facilities Engineering Command
NAVSUP	Naval Supply Systems Command
NDI	Non-Developmental Item
NEHC	Navy Environmental Health Center
NEPA	National Environmental Policy Act
NOSSA	Naval Ordnance Safety & Security Activity
OAG	Operational Advisory Group
ORD	Operational Requirements Document
OSHA	Occupational Safety and Health Administration
O&SHA	Operating and Support Hazard Analysis
OT&E	Operational Test & Evaluation
PDM	Program Decision Meetings
PE	Professional Engineer
PEO	Program Executive Officer
PESHE	Programmatic Environmental Safety and Health Evaluation
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard Analysis List
PM	Program Manager
PRESINSURV	President, Board of Inspection and Survey
R&D	Research and Development
RFD/W	Request for Deviation/Waiver
RFP	Request for Proposal
SA	Safety Assessment
SCA	Safety Compliance Assessment
SCF	Safety Critical Functions
SCN	Specification Change Notices
SEP	Systems Engineering Plan

SES	Senior Executive Service
SHA	System Hazard Analysis
SOW	Statement of Work
SPAWAR	Space and Naval Warfare Systems Command
SPR	Software Problem Report
SRCA	Safety Requirements/Criteria Analysis
SSHA	Subsystem Hazard Analysis
SSMP	System Safety Management Plan
SSP	System Safety Program
SSPP	System Safety Program Plan
SSAB	System Safety Advisory Board
SSWG	System Safety Working Group
SSSTRP	Software System Safety Technical Review Panel
S&T	Science and Technology
SYSCOM	System Command
T&E	Test and Evaluation
WSESRB	Weapon System Explosives Safety Review Board

SUPPLEMENTAL GUIDANCE TO TAILORING A SYSTEM SAFETY PROGRAM AND PROCESS

1. Purpose. This enclosure is intended to provide supplemental guidance to the requirements provided in references (3-a) through (3-e) for programs to tailor system safety task performance and implementation to the stage, risk, and complexity of their program. It is provided as information for the Program Manager (PM) and/or acquisition authority. This supplemental guidance provides the PM with the recommended qualifications for the system safety lead (Table 1) and a sample list of tasks (Table 2) indicating the task category (managerial or technical) at each program life cycle phase. Tasks listed in Table 2 are those most commonly used in a system safety program. Other tasks may be assigned depending on the complexity of the program/project.

2. Integrating System Safety into the Joint Capabilities Integration and Development System (JCIDs) and Acquisition Processes

a. Role of Capabilities Documents. Evaluations conducted prior to program initiation through the Analysis of Alternatives (AoA) and Initial Capabilities Document (ICD), and/or the Joint Capabilities Document (JCD), should consider the viability of various technical approaches in achieving military objectives without excessive risk to mission or personnel, including ESOH considerations. Capabilities Development Documents (CDDs) and Capabilities Production Documents (CPDs) should include language requiring HSI, ESOH lessons learned, and life cycle risk management as related to the capabilities being proposed for development. References (3-f) and (3-g) provide guidance for development of capabilities documents. The capabilities documents support the development of task assignments, including system safety program elements, in the Request for Proposal (RFP), the Statement of Work (SOW), and system specifications.

b. System's Engineering Plan (SEP). PMs, regardless of the Acquisition Category of their programs, integrate system safety risk management into their overall systems engineering and risk management process. PMs ensure the reference (3-c) requirement to integrate the ESOH risk management strategy into the systems engineering process is incorporated in the SEP.

c. Programmatic Environmental Safety and Occupational Health Evaluation (PESHE). The acquisition strategy shall

incorporate a summary of the PESHE, including ESOH risks, a strategy for integrating ESOH considerations into the systems engineering process, identification of ESOH responsibilities, and a method for tracking progress.

3. Guidance for Implementation. The system safety program identifies the specific activities (e.g., analyses, tests, inspections) to help meet the CDD/CPD or Operational Requirements Document (ORD) requirements and ensures identification of risks from legacy systems and new processes. The PM's system safety lead and the contracting agent should provide in-depth details of any additional tasks and a description for PM approval. The tasks and descriptions are provided so that the PM is aware of the choices for which tasks are to be performed and made part of the RFP and SOW as required by the CDD/CPD, AoA and ICD. Table 1 provides the PM with a recommended education and experience chart to assist the PM in choosing well-qualified system safety personnel. The PM, (with assistance from their chosen system safety working group (SSWG)) should ensure that the design agent, contractor, or performing activity provides in-depth details on task performance, organization, and personnel to ensure all aspects of safety are addressed as early as possible and throughout the development life cycle.

a. A system safety program should be tailored to meet the needs of the particular system, subsystem, equipment, or software. For example, a system safety program requirement may be as simple as a safety assessment report for a legacy system being used in a new, but similar, application that shows a systems safe operating history and documents adaptation to its new proposed environment or any other modification for safe use in its proposed environment. Conversely, a more complex system may require a more complete evaluation of the system from its earliest stages through disposal.

b. In tailoring the system safety program, the PM should define the detail and depth of effort and incorporate them into contractual documents. The PM should define the level of risk for design. The guidance in this enclosure will assist in tailoring the system safety program to meet mission needs in a cost effective way.

c. Human Systems Integration as described in the Defense Acquisition Guidebook, Reference (3-h),plays a major role in the design process. Front-end analysis methods, such as those described in Reference (3-i), should be pursued to maximize the

effectiveness of the new system. Initial emphasis should be placed on "lessons learned" from predecessor or comparable systems to help identify and eliminate characteristics in the new system that require excessive cognitive, physical, or sensory skills or high aptitudes; involve complex fault location or workload intensive tasks; necessitate excessive training; require proficiency training; or result in frequent or critical errors or safety/health hazards. Placing an emphasis on the "human-in-the-loop" ensures that systems are designed to operate consistent with human performance capabilities and limitations, meet system functional requirements, and fulfill mission goals with the least possible demands on manpower, personnel, and training. Moreover, HSI minimizes added costs that result when systems have to be modified after they are fielded in order to correct performance and safety issues.

4. Organization. The PM should establish a system safety organization or function and lines of communication within the program organization and with associated government and contracted organizations. Interfaces should be established between system safety and other elements and disciplines of the program with emphasis on integration in the systems engineering process. To support this, a SSWG should be established consisting of qualified personnel as designated by the PM. The group should include government and the acquisition prime contractor personnel. The group should consist of, but is not limited to, key personnel such as: system safety lead, HSI/human engineering professional, safety and occupational health professional, environmental engineer, and system engineer representing each area of expertise, as needed. Representatives from operational commands, type commands, the Chief, Bureau of Medicine and Surgery (BUMED)/Navy Environmental Health Center (NEHC) and the Naval Safety Center may provide support on an as-needed basis. The system safety lead should be the PM's point of contact to the System Safety Advisory Board (SSAB). The system safety lead should have a direct line of communication to the PM.

5. Task Selection. Table 2 lists the management and engineering safety tasks to be considered at program milestones. It is intended as a guide for the PM and the system safety program. The PM is to establish a system safety plan (SSP) by developing a planned approach for safety task accomplishment.

a. Provide Qualified Personnel. The PM should provide qualified personnel, as noted in Table 1, to accomplish the system safety program.

Table 1. Recommended Qualifications for System Safety Lead

NOTE: Functions can be military, civilian or contractor

Program Complexity	Education[1]	Safety Experience	Certification[1]
High Consequence systems include new ship-builds, combat systems, missiles, torpedoes, aircraft **systems**, etc.	Bachelor of Science (BS) Degree in Engineering, Computer Science, or related discipline. Desired: Masters in Engineering, Engineering Administration, or Safety Program Management	4 Years in System Safety plus 2 Years on similar systems	Desired: CSP[2] or PE[3] and Related System Safety[4] and Software Safety[5]
	Bachelor's Degree or Associates Degree in Engineering plus specialized training in System Safety	6 Years in System Safety plus 4 years on similar systems	Desired: CSP[2] or PE[3] and Related System Safety[4] and Software Safety[5]
	High **School Diploma** plus specialized training in System Safety	10 years in System Safety plus 8 years on similar systems	Related System Safety[4] and Software Safety[5]
Medium Consequence systems include fuzes, shoulder launched weapons, wheeled vehicle components, etc.	Bachelor's Degree in Engineering, Computer Science, or related discipline plus specialized training in System Safety	4 Years in System Safety	Desired: PE[3] and Related System Safety[4] and Software Safety[5]
	Bachelor's Degree or Associates Degree in Engineering plus specialized training in System Safety	4 Years in System Safety plus 2 years on similar systems	Desired: CSP[2] or PE[3] and Related System Safety[4] and Software Safety[5]
	High School Diploma plus specialized training in System Safety	5 years in System Safety plus 5 years on similar systems	Related System Safety[4] and Software Safety[5]

Program Complexity	Education[1]	Safety Experience	Certification[1]
Low Consequence systems include small arms ammunition, Computer Aided Designs, flares, hand-grenades, etc.	BS Degree in Engineering, Computer Science, or related discipline plus specialized training in System Safety	1 Year in System Safety	Desired: CSP[2] or PE[3] and Related System Safety[4]
	Bachelor's Degree or Associates Degree in Engineering plus specialized training in System Safety	2 Years in System Safety	Desired: CSP[2] or PE[3] and Related System Safety[4]
	High School Diploma plus specialized training in System Safety	3 years in System Safety plus 3 years on similar systems	Related System Safety[4]

[1] PM may specify or substitute other degrees or certifications in SOW depending on complexity of program.
[2] CSP - Certified Safety Professional
[3] PE - Professional Engineer
[4] Related system safety certification would be a test including tools, specifications, standards, etc. related to this group.
[5] Software safety certification would be to the level required for the complexity level.

b. Develop a System Safety Management Plan (SSMP) and System Safety Program Plan (SSPP). The PM and contractor, if applicable, should develop a SSMP and SSPP respectively. The program should describe in detail tasks chosen from Table 2 and activities of system safety management, including the flow down of system safety requirements and management to sub-contractors, and system safety engineering required to identify, evaluate, eliminate/control hazards, or reduce the associated mishap risk to a level acceptable to the PM throughout the system life cycle. Each SSMP describes, as a minimum, the four elements of an effective system safety program:

(1) A planned approach for task accomplishment

(2) Qualified people to accomplish tasks

(3) Authority to implement tasks through all levels of management

(4) Appropriate commitment of resources (both staffing and funding)

c. Conduct System Safety Review /Audits. The acquisition prime contractor performs and documents system safety reviews/audits as specified by the PM to perform reviews/audits of contractors, associate contractors, and support contractors and sub-contractors system safety program.

d. Develop a Hazard Tracking and Risk Resolution System. PMs should ensure that a database to document and track to resolution all hazards and their elimination or controls is developed. The database is maintained throughout the life of the system including disposal. It should include all hazards (personnel, weapons, health, operations, environmental, etc.).

e. Prepare System Safety Progress Summaries. The contractor should prepare periodic system safety progress reports summarizing general progress made relative to the system program during the specified reporting period (usually quarterly) and projecting work for the next reporting period.

f. Perform Functional Hazard Assessment (FHA). The FHA is used to identify and classify the system functions and the safety ramification(s) of functional failure or malfunction. These ramifications will be classified in terms of safety severity for the purpose of identifying the Safety-Critical Functions (SCF). The contractor should perform and document a FHA to obtain an initial risk assessment of a concept or system. Based on the best available data, including mishap data (if assessable) from similar systems and other lessons learned, functions associated with the proposed functional or physical design shall be analyzed to include inputs, outputs, critical interfaces, ramifications of functional failure, and the safety severity assessment for each ramification. Describing safety critical functions provides a means to place additional safety emphasis on selected functions in the acquisition design process.

g. Develop a Preliminary Hazard List (PHL). The PM or designee should examine the system shortly after concept definition effort begins and compile a PHL, identifying possible hazards that may be inherent in the concept and their associated mishap potential.

h. Conduct a Preliminary Hazard Analysis (PHA). The PM or designee should perform and document a PHA to obtain an initial

risk assessment of a concept or system. Based on best available data, including mishap data from similar systems and lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity, probability and operational constraint. Include safety provisions and alternatives needed to eliminate hazards or reduce their risk to an acceptable level.

i. Develop Safety Requirements/Criteria Analysis (SRCA). The PM or designee should perform a SRCA, which relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the hazards to an acceptable level. The SRCA uses the PHL and/or PHA as a basis.

j. Perform Subsystem Hazard Analysis (SSHA). The PM or designee should perform and document a SSHA to identify all components and equipment that could result in a hazard or whose design does not satisfy contractual safety requirements. This includes government furnished equipment (GFE), non-developmental items (NDI), Commercial Off-The-Shelf (COTs) and software.

k. Perform System Hazard Analysis (SHA). The PM or designee should perform and document a SHA to identify hazards and assess the risk of the total system design, including software and specifically to subsystem interfaces.

l. Perform Operating and Support Hazard Analysis (O&SHA). The PM or designee should perform and document an O&SHA to identify and evaluate hazards resulting from implementation of operations or tasks performed by persons. This analysis should use the Human Systems Integration (HSI) approach. References (3-i) through (3-q) provide guidance for application of the HSI into system evaluation and development.

m. Perform Health Hazard Assessment (HHA). The PM or designee should identify health hazards and recommend engineering controls, equipment and/or protective procedures, to reduce the associated risk to an acceptable level. Health hazards identified should include chemical, physical, biological and ergonomic stressors. Support may be requested from BUMED in accordance with reference (3-r).

n. Perform Safety Assessment. The PM or designee perform and document a safety assessment to (1) identify all safety features of the hardware, software, and system design, and to (2) identify procedural, hardware, and software related hazards

that may be present in the system being acquired. Generally, a safety assessment is prepared prior to a major milestone or test event and documents the current risk level associated with a given event and/or a particular point in time.

o. Verify System Safety in the Test and Evaluation Process. The PM should certify that safety actions have been completed to reduce, correct, or control hazards for the specific test and evaluation environment, in concert with the user and test communities. In accordance with reference (3-b) the PM shall provide safety releases to the developmental and operational testers prior to any test using personnel. Results during test and evaluation will be reported so actions can be taken to address safety hazards identified during testing.

p. Review Safety Review and Engineering Change Proposals (ECPs), Specification Change Notices (SCNs), Software Problem Reports (SPRs) and Request For Deviation/Waiver (RFD/W). The PM or designee should analyze each ECP, SCN, SPR and RFD/W to determine the hazards and assess the risk of the proposal.

q. Perform Safety Compliance Assessment. The PM or designee should perform and document a safety compliance assessment to identify and document compliance with appropriate design and operational safety requirements. Look for the assessment to incorporate the scope of the PHA, SSHA, SHA, and O&SHA to assure safe design, operation, maintenance, and to support the safety manager in tailoring a system safety program.

Table 2. Sample Application Matrix for System Safety Program Tailoring[1]

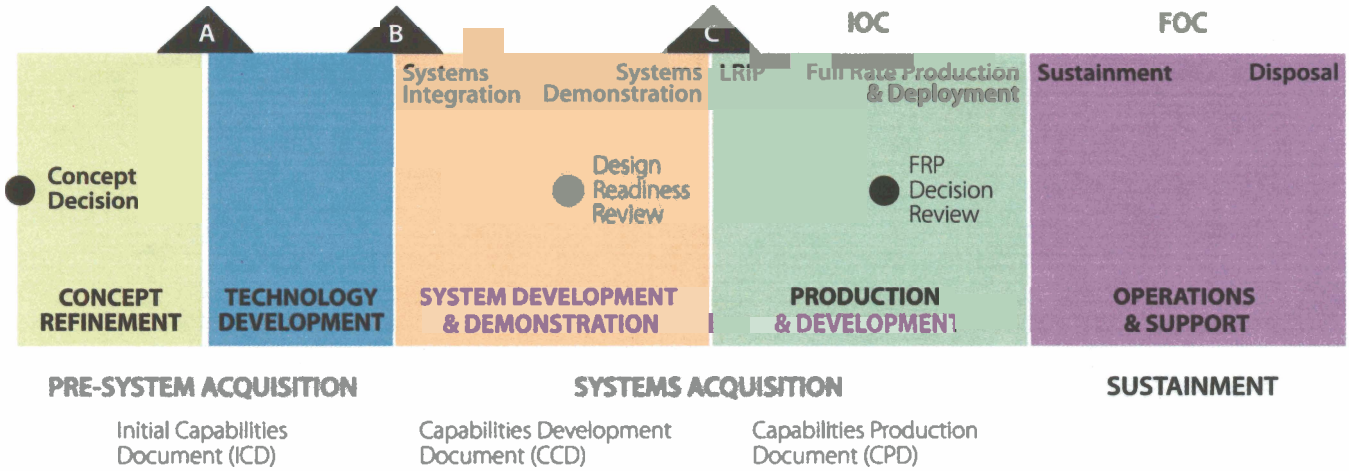
Task Description	Task Type	Program Phase Milestones (See Figure 1 below)				
	See below	A	B	C	IOC/ FRP	FOC (O&S)
System Safety Program (SSP)	MGT	A	A	A	A	A
System Safety Management Plan (SSMP)	MGT	A	A	A	A	A
System Safety Program Review /Audits	MGT	AN	AN	AN	AN	AN
System Safety Working Group Support (SSWG)	MGT	A	A	A	A	A
Hazard Tracking and Risk Resolution	MGT	AN	A	A	A	A
System Safety Progress Summary	MGT	AN	A	A	A	A
Functional Hazard Assessment (FHA)/Safety Critical Functions	ENG	AN	AN	AN	AN	AN (AD)
Preliminary Hazard List (PHL)*	ENG	A	AN	AN	AN	N/A

Task Description	Task Type	Program Phase Milestones (See Figure 1 below)				
	See below	A	B	C	IOC/ FRP	FOC (O&S)
Preliminary Hazard Analysis (PHA)*	ENG	A	A	A	AD	AD
Safety Requirements/Criteria Analysis*	ENG	A	AN	AN	AN	AD
Subsystem Hazard Analysis (SSHA)*	ENG	N/A	A	A	AD	AD
System Hazard Analysis (SHA)	ENG	N/A	A	A	AD	AD
Operating and Support Hazard Analysis (O&SHA)*	ENG	AN	A	A	AD	AD
Health Hazard Assessment (HHA)*	ENG	A	A	A	AD	AD
Safety Assessment* (SA)	ENG	AN	AN	AN	AN	AN
Test and Evaluation Safety*	ENG	A	A	A	A	A
Safety Review of Engineering Change Proposals (ECPs), Specification Change Notices, Software Problem Reports and Request for Deviations and Waivers	ENG	N/A	A	A	A	A
Safety Verification	ENG	AN	A	A	AN	AN
Safety Compliance Assessment (SCA)	ENG	AN	A	A	AN	AN
Programmatic Environment Safety and Occupational Health Evaluation (PESHE)**	MGT	AN **	A	A	A	AN

Task Type	Applicability Codes
ENG - System Safety Engineering	A - Applies to all programs
MGT - System Safety Management	AN - As Needed
	AD - Applicable to Design Change Only
	N/A - Not Applicable

[1] Tasks categorized as managerial are typically conducted by the PM's staff while those classified as technical are generally conducted by the support contractor(s).
*Tasks asterisked above should also be coordinated with or be part of HSI procedures.
**The PESHE is required by Table E3.T1 of reference 3-b (DODI 5000.2) for all programs at Milestones B, C, and at the Full-Rate Production Decision Review (FRP DR); and for ships, also at Program Initiation (Milestone A). The PESHE must be summarized in the Acquisition Strategy. The PESHE has no common format and is not a data item, but it summarizes the programs risk management approach for environment, safety and health issues throughout the program life cycle.

Figure 1. The Defense Acquisition Management Framework Milestones



Note: Figure 1. For further information and detail refer to reference (b).

6. Other potentially applicable environmental, safety and occupational health (ESOH) areas for special consideration:

a. Ordnance and explosives safety, per references (s) through (v).

b. Lithium battery safety, per reference (w).

c. Laser hazards, per reference (x).

d. Aviation critical safety items (CSIs), per references (y) through (cc).

e. Habitability and human systems integration (HSI) in accordance with references (3-b), (3-c), and (3-dd). HSI is required to integrate the capabilities and limitations of user community within the operating environment to form an effective, coordinated system. References (3-j) through (3-q), (3-dd) and (3-ee) provide process-specific criteria, design requirements, and standard practice for human engineering for varied military systems, equipment and facilities in support of the HSI requirements of reference (3-c).

f. Chemical processes and hazardous materials should be managed by application of references (3-e) and (3-ee) through (3-gg) criteria and process as applied to the selection and use of hazardous materials.

g. Noise and vibration evaluation and control in accordance with references (3-dd), (3-hh) and (3-ii).

h. Non-ionizing Radiation (including laser) and Radio Frequency Protection in accordance with references (3-x), (3-ee), (3-jj), and (3-kk).

i. Falls and Walking/Working Surfaces. Falls from height are the second leading cause of occupational fatalities and account for approximately 700 occupational fatalities annually in the United States. Slips, trips and falls from level work surfaces also contribute to mishaps. System safety evaluation of risks should consider and mitigate the hazards of work at elevated locations associated with defense systems to manage risk and life cycle costs of systems, vessels, aircraft maintenance and facilities maintenance. Early identification and management of fall hazards reduces the cost of control measures and the effectiveness of their employment. Occupational Safety and Health Administration (OSHA) regulations establish criteria ranging from 4 to 8 feet, depending upon industry, for implementation of control measures to prevent falls. System safety evaluation should identify and manage these risks using a hierarchy of controls stressing elimination, engineering controls/barriers and protective equipment systems where other measures are not practical or fully effective. OSHA standards and references (3-ee) and (3-kk) should be consulted for regulatory requirements and technical guidance.

j. Confined Spaces. Many defense systems, particularly ships and facilities, incorporate locations in which access/egress is restricted and personnel may be exposed to physical and chemical hazards. Design for life-cycle risk management should consider maintenance and safety of confined/enclosed spaces and mitigate and manage associated hazards. OSHA standards and references (3-ee) and (3-kk) should be consulted for regulatory requirements and technical guidance.

k. Machine Guarding and Control of Hazardous Energy. The system safety and human systems integration programs should identify potential hazardous energy sources that may be released during maintenance and provide means for their control through mechanical (lock-out) methods while minimizing or eliminating the need for procedural isolation techniques (tag-out). OSHA standards and references (3-ee) and (3-kk) should be consulted for regulatory requirements and technical guidance.

l. NEPA/EO 12114 Compliance and Environmental Management.

m. Potential system and survivability risks associated with software shall be managed through a process consistent with reference (3-ll) or equivalent criteria.

n. References (3-ee), (3-kk), (3-mm) and (3-nn) focus on the responsibilities of the operational and training communities for protection of personnel health and safety during operations, training and maintenance in accordance with Navy system safety policy objectives. Feedback provided by the operational community should be integrated into the system safety process. Fleet representatives should be invited to participate in the system safety process through membership in working groups and forwarding of relevant information.

7. System Safety Advisory Board (SSAB). The System Safety Advisory Board (SSAB), chaired by CNO (N09F), will be available to PMs and milestone decision authorities upon request.

References

(3-a) DOD Directive 5000.1, The Defense Acquisition System, of 12 May 03
(3-b) DOD Instruction 5000.2, Operation of Defense Acquisition System, of 12 May 03
(3-c) SECNAVINST 5000.2C, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, of 19 Nov 04
(3-d) SECNAVINST 5100.10J, Department of the Navy Policy for Safety, Mishap Prevention, Occupational Health and Fire Protection Programs, of 26 Oct 05
(3-e) MIL-STD-882D, Standard Practice for System Safety, of 10 Feb 00
(3-f) Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3170.01E, "Joint Capabilities Integration and Development System," of 11 May 05
(3-g) Chairman, Joint Chiefs of Staff Manual (CJCSM) 3170.01B, "Operation of the Joint Capabilities Integration and Development System," of 11 May 05
(3-h) Defense Acquisition Guidebook, Defense Acquisitions University 24 Jul 06
(3-i) MIL-HDBK 46855A Human Engineering Program Process and Procedures, of 17 May 99
(3-j) ANSI/EIA-632, EIA Processes for Engineering a System, of 1998

(3-k) ISO/IEC 15288, International Standard Systems Engineering System Lifecycle Processes, First Edition, of 1 Oct 02

(3-l) ISO 13407, International Standard Human-Centered Design Processes for Interactive Systems, First Edition, of 1 Jun 99

(3-m) ASTM F1337, Standard Practice for Human Engineering Program Requirements for Ships and Marine Systems, Equipment, and Facilities, of 2001

(3-n) NAVSEAINST 9700.2, Integrated Topside Safety and Certification Program for Surface Ships, of 11 Sep 98

(3-o) NAVSEA 3900.08A Human System Integration in Acquisition and Modernization 20 May 05

(3-p) MIL-STD-1472F, Department of Defense Design Criteria Standard Human Engineering of 23 Aug 99

(3-q) ASTM F1166-95a, Standard Practice for Human Engineering Design for Marine Systems, Equipment and Facilities, of 2000

((3-r) BUMEDINST 6270.8A, Procedures for Obtaining Health Hazard Assessments (HHAs), of 3 Jan 02

(3-s) OPNAVINST 8020.14/MCO P8020.11, Department of the Navy Explosives Safety Policy, of 1 Oct 99

(3-t) NAVSEAINST 8020.06D, Navy Weapon System Safety Program, of 21 Jan 03

(3-u) NAVSEAINST OP4, Ammunition and Explosives Afloat, of 15 Jan 03

(3-v) NAVSEAINST OP5, Ammunition and Explosives Ashore, of 2 May 02

(3-w) NAVSEAINST 9310.01B, Naval Lithium Battery Safety Program, of 21 Jan 03

(3-x) OPNAVINST 5100.27A/MCO 5104.1B, Navy Laser Hazards Control Program, of 24 Sep 02

(3-y) Public Law No 108-136 "National Defense Authorization Act for Fiscal Year 2004", Section 802, Quality Control In Procurement Of Aviation Critical Safety Items And Related Services

(3-z) DOD 4140.1-R, DOD Supply Chain Material Management Regulation, Section C8.5, DOD Aviation Critical Safety Item (CSI)/Flight Safety Critical Aircraft Part (FSCAP) Program, of 23 May 03

(3-aa) Defense Federal Acquisition Regulation Supplement 209-270, Aviation Critical Safety Items of 22 Feb 05

(3-bb) SECNAVINST 4140.2, Management of Aviation Critical Safety Items, of 25 Jan 06

(3-cc) Joint Aeronautical Logistics Commanders (JALC) "Aviation Critical Safety Item Management Handbook," of 4 Aug 05.

(3-dd) OPNAVINST 9640.1A, Shipboard Habitability Program, of 3 Sept 96

(3-ee) OPNAVINST 5100.23G, Navy Occupational Safety and Health (NAVOSH) Program Manual, of 30 Dec 2005

(3-ff) National Aerospace Standard (NAS) 411, Hazardous Materials Management Program, of 19 Jan 95

(3-gg) OPNAVINST 5090.1B Change Transmittal 4, Environmental and Natural Resources Program Manual, of 4 Jun 03

(3-hh) MIL-STD-1474D Change Notice 1, Noise Limits, of 29 Aug 97

(3-ii) DOD Instruction 6055.12, DOD Hearing Conservation Program, of 5 Mar 04

(3-jj) DOD Handbook 237D, Electromagnetic Environmental Effects and Spectrum Certification Guidance for the Acquisition Process, of 17 Feb 05

(3-kk) OPNAVINST 5100.19D Change 1, Navy Occupational Safety and Health (NAVOSH) Program Manual for Forces Afloat, of 30 Aug 01

(3-ll) Joint Software System Safety Handbook, of December 99

(3-mm) OPNAVINST 3500.39B/MCO 4500.27B, Operational Risk Management (ORM), of 30 Jul 04

(3-nn) OPNAVINST 5100.8G, Navy Safety and Occupational Safety and Health Program, of 2 Jul 86

GUIDELINES FOR IDENTIFYING KEY SYSTEM SAFETY NEEDS IN CAPABILITIES DOCUMENTS AND SUBSEQUENT PROGRAM DOCUMENTS

1. Purpose

a. System safety is considered to be a core priority to Navy acquisition because it identifies and provides means to track performance factors that could jeopardize mission performance and system survivability, or affect operator and maintenance worker safety and efficiency. System Safety is the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. Early consideration minimizes cost and schedule effects of unanticipated design problems and retrofits.

b. References (4-a) through (4-d) require the application of system safety in acquisition using reference (4-e) as a guide. References (4-f) and (4-g) guide the capabilities development process.

c. This enclosure provides guidance for identifying and describing safety capabilities and system characteristics necessary for mission performance and sustainment within Joint Capabilities Integration and Development Systems (JCIDS) documents in accordance with references (4-f) and (4-g). It provides recommendations for incorporating system safety language into the development of capabilities documents, supporting analyses and follow-on requirements.

2. Guidelines for Initial Capabilities Documents (ICDs) and Joint Capabilities Documents (JCDs)

a. The ICDs/JCDs describe capability gaps that exist in joint warfighting functions, as described in the applicable Joint Functional Concepts (JFC) and integrated architectures. The ICD defines the capability gap in terms of the functional area, the relevant range of military operations, and the timeframe under consideration. The ICD must capture the results of a well-framed functional analysis, as described in enclosure (a) of reference (4-g).

b. ICDs/JCDs and related analyses support program initiation before specific technical solutions, hardware and/or software have been developed. The safety, survivability, and ability to deploy and sustain prospective systems and equipment

are critical considerations during the technical development process.

c. In accordance with reference (4-b), environmental compliance, personnel safety, and survivability are critical elements of acquisition systems and the ICDs/JCDs should reflect those requirements.

d. ICDs/JCDs, and precursor documents, should describe the environmental conditions and operational settings in which capability is required. It is imperative for the operational community to describe all the anticipated conditions of use, platforms that the system will be deployed upon, and requirement for integration with other systems and equipment. Identify and describe operational capability gaps and support proposals for resolution using the JCIDS process per references (4-f) and (4-g). All capability documents must clearly identify the life cycle environment that any new system will encounter and the systems interfaces required. This should include effective descriptions of operational environment and need, safety impacts, description of the limitations of current Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) approaches in addressing these needs and recommendations for alternative solutions. For example, remote operation of unmanned vehicles will require different approaches and safeguards than manned vehicles, while reducing habitability constraints. At a minimum the documents must describe all the platforms the system should be used from, all the transportation and storage modes, other service interfaces, temperature, pressure, altitude, humidity, and categories of human interaction.

e. Recommended Draft Language for ICDs. Recommended draft language below addresses environmental, safety and occupational health (ESOH) areas per references (4-f) and (4-g) that may be tailored/used when developing ICDs. ESOH issues may be addressed in the context of capability gaps (Section 4) where present systems fail to adequately protect the mission or operators, in terms of their impact on threat and operational environment (Section 5). Necessary ESOH capabilities may be described in functional analysis (Section 6) and/or final recommendations (Section 7). Possible language for functional analysis (Section 6) and prospective recommendations are provided below:

(1) *"The system will ensure the safety and survivability of the system and provide a safe, healthy, and efficient/*

comfortable environment for operators. Risk factors will be identified, tracked, and managed through a system safety program consistent with reference (4-e)."

(2) *"For the system, safety considerations will be provided for in the program baseline to support sustainable operation and maintenance. Designs will be consistent with human factors engineering criteria per references (*) or equivalent standards."* *Cite references (4-h) through (4-l) and/or related criteria, as appropriate to the system under consideration.

(3) *"Development of the system and design of support processes and materials will identify mishap risks associated with hazardous materials and minimize their human health, safety and environmental impacts through selection of the alternatives consistent with operational requirements, cost, and efficiency."*

3. Ensure that Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) include consideration of safety and environment. Requirements for relevant analysis may be provided in the functional analysis (section 6) and/or the recommendations (section 7) of the ICD.

a. Possible language is provided below:

(1) *"Manpower, training, and personnel costs will be minimized through task and process identification, design for efficiency, and use of automated processes and equipment, where feasible, to reduce life cycle costs and mishap risks. Criteria for systems/equipment designs will utilize systems engineering and human systems integration (HSI) principles to ensure that designs are consistent with the capabilities and limitations of the anticipated users."* It is recommended that the "user community" be defined in the ICD/CDD/CPD//JCD/direct change requirement (DCR) Glossary. The "user community" includes, but, is not limited to: operators, maintainers, administrators, support personnel, supervisors, managers/command, trainers, and installers.

(2) *"The efficiency and safety of existing support equipment will be evaluated. System design will evaluate alternative processes and equipment to minimize costs and mishap risk while ensuring user and maintainer safety."*

b. Acquisition managers/systems managers are responsible for the design and planning for life cycle cost management of

systems, sub-systems and equipment throughout the life cycle. Operations, support, sustainment and ultimate disposal account for approximately 60% of life cycle costs. Ensuring safety and efficiency in these processes requires evaluating the existing (legacy) solutions and identifying risks and inefficiencies, as noted above.

c. Section 7.a of the ICD, should describe the materiel approaches that fill the HSI capability gaps in existing systems, and/or are expected to provide successful human performance, and adequate personnel survivability, health and safety, and quality of life in the emerging system or family of systems. If an evolutionary acquisition or spiral development is to be implemented to reduce the acquisition cycle and speed capability to the war-fighters, this has special implications for HSI. Essentially human factors engineering is more important for systems procured under a spiral acquisition strategy than for the conventional acquisition approach since, while system performance is improving over time, human performance must be optimized from the initial increment through each iteration, even while the hardware and software, and associated human-machine interfaces, are changing.

d. In ICD Section 7.b, HSI requirements in the AoA are identified. These include identification of HSI issues to be assessed for each alternative concept; metrics to enable assessment of the HSI issues; and expected results of the assessment. The overriding objectives of providing HSI inputs to the AoA planning are that an assessment will be made of: (1) the implications of each design alternative on human performance, workload, survivability, health and safety, and quality of life; and (2) the extent to which the design alternative addresses manpower optimization.

e. In ICD Section 7.c, HSI inputs include DOTMLPF implications and constraints of recommended materiel approaches, to include all HSI domains. Examples of HSI implications may include: end-strength limitations for manpower; affordability of developing knowledge, skills, abilities and training not currently available in the Navy; minimums and appropriate mix of manpower (military, civilian and contractor); joint manning options; the appropriate level and acceptable risks associated with automating critical functions; and environmental regulations and workspace safety compliance requirements."

4. Guidelines for Initial Capability Documents (ICDs), and Joint Capability Documents (JCDs) and DOTMLPF Change Recommendations (DCRs)

a. Safety-associated capabilities for CDDs and CPDs should be similar to those described above for ICDs/JCDs, but generally need to provide more specificity with regard to system attributes. Guided by the ICD and technology development activities, the CDD captures the information necessary to develop a proposed acquisition program(s). The CDD outlines an affordable increment of capability, typically reflected in a new or updated system or platform (such as ship, aircraft, or computer system). The CDD provides the operational performance attributes, including supportability, necessary for the acquisition community to design the proposed system, including key performance parameters (KPP) and other parameters that will guide the development, demonstration and testing of the current increment. The CDD must be validated and approved before the Milestone B decision. The CPD is the sponsor's primary means of providing authoritative, testable capabilities for the production and deployment phase of an acquisition program. The CDD and CPD must capture the results of a well-framed functional analysis, as described in enclosures (b) and (c) of reference (4-g). CDD and CPDs should seek to describe the environmental conditions and operational settings in which capability is required. This will support the selection and development of systems, sub-systems and equipment that accommodate various climactic conditions and settings, such as shipboard environments, while minimizing the need for later redesign.

b. For CDDs and CPDs, Appendix A of enclosures (f) and (g) of reference (g) identifies relevant sections of capabilities documents including; Section 6 (Attributes), Section 13 (DOTMPLF and Policy) and Section 14 (Other Attributes - including ESOH considerations).

c. The DCR is defined as a "Non-material solution" and is one of the JCIDS capabilities documents. This means that an existing product or piece of hardware is going to be used to meet the requirements of a new capability gap. Thus, it is reasonable to expect that a non-material solution will require the use of some existing piece of hardware (including COTS) in a way that will be different than the use it was originally designed for. As a result, the same safety issues should be addressed for a DCR that are addressed for the JCD, ICD, CDD, CPD documents. In particular, a very critical look at potential

HSI impact issues associated with the different use of the product by the war-fighters is required.

d. System attributes and critical processes that should be considered in these documents and derivative contractual and technical documents are described below.

(1) Hazardous Process and Materials. Approximately 80% of DoD hazardous materials and associated waste products are used or generated in association with maintenance/sustainment of defense systems. Therefore, proactive management of hazardous material and process is essential to mitigate safety and environmental mishap risks and related life cycle costs. In certain cases, hazardous materials or processes pose high risks to human life and environmental impacts and the use of these materials should be prohibited. Possible examples may include toxic material such as beryllium, cadmium or acutely toxic products. Suggested language for CDDs and CPDs is provided below:

(a) *"Development of the system and design of support processes and materials will identify mishap risks associated with hazardous materials and minimize human health, safety and environmental impacts through selection of alternatives consistent with operational requirements, cost, and efficiency."*

(b) *"Hazardous material usage will be managed through application of National Aerospace Standard (NAS) 411* [reference (4-m)] *or equivalent methods."*

(2) Risk Management. Suggested language for CDDs and CPDs is provided below. *"Potential ESOH risks will be identified and managed in accordance with MIL-STD-882D. Designs shall consider the following order of precedence of MIL-STD-882D for risk mitigation of identified hazards":*

- *"Eliminate hazards through design selection.*
- *"Incorporate safety devices."*
- *"Provide warning devices."*
- *"Develop procedures and training."*

(3) References (4-b) and (4-n) require PMs to apply human systems integration (HSI) to improve total system performance and reduce life cycle costs by lowering or eliminating mishap risk through a design process that integrates the seven domains of HSI: manpower, personnel, training, human factors engineering, environmental, safety and occupational

health (ESOH), habitability, and survivability (system safety interacts with all of the domains). All acquisition programs are required to address HSI with attention to optimal use of manpower, which helps ensure effective levels of system safety throughout operational and maintenance activities. Where practicable and cost effective, system designs should minimize or eliminate system characteristics that require excessive cognitive, physical, or sensory skills; entail extensive training or workload-intensive tasks; result in mission-critical errors; or produce safety or health hazards. Reference (4-c) describes requirements for addressing survivability. Reference (4-o) requires that force protection and survivability parameters shall be KPPs for "covered systems" including manned systems or any equipment intended to enhance personnel survivability that are expected to be deployed in an asymmetric threat environment and resource sponsors shall identify and include key capability attributes (KCAs) in all CDDs and CPDs. Suggested language for CDDs and CPDs is provided below:

(a) Manpower. *"The program will assess manpower requirements for the identified system. The system shall be adequately staffed to ensure the safe and efficient completion of mission."*

(b) Personnel. *"The program will work with the personnel community to describe the characteristics of user populations. To the extent possible, systems shall not require special cognitive, physical, or sensory skills beyond that found in the specified user population."*

(c) Training. *"The program will work with the training community to identify the training requirements for assessed manpower needs and established user population. Training shall support safe and efficient mission accomplishment."*

(d) Human Factors Engineering

1. *"Human factors engineering principles and design standards shall be applied to the design of the system. Designs will be consistent with human factors engineering criteria per references (*) or equivalent standards."* * Cite references (4-h) through (4-l) and/or related criteria, as appropriate to the system under consideration.

2. *"Human factors engineering will be employed during systems engineering over the life of the program to*

provide for effective human-machine interfaces, enhance personnel performance, ensure that systems and equipment are designed for the physical dimensions, capabilities and limitations of the user population(s) and to meet HSI, maintenance, safety and communications requirements. System designs shall minimize or eliminate system characteristics that require excessive cognitive, physical, or sensory skills; entail extensive training or workload-intensive tasks; result in mission-critical errors; or produce safety or health hazards. Designs will be consistent with human factors engineering criteria per references (**) or equivalent standards."*

*It is recommended that the "user community" be defined in the ICD/CDD/CPD Glossary. The "user community" includes but is not limited to: operators, maintainers, administrators, support personnel, supervisors, managers/command, trainers, and installers.

** Cite references (4-h) through (4-l) and/or related criteria, as appropriate to the system under consideration.

3. Reduction of Ergonomic Injuries. The CDD and CPD should state that equipment design and use procedures will minimize the potential for ergonomic injuries. Ergonomic injuries include damage to joints, muscles, and bones due to design features that require repetitive motion, stresses to neck and back muscles, excessive weight lifting and similar workplace activities where human musculoskeletal capabilities and limitations have not been addressed in the design."

(e) Environmental, Safety and Occupational Health (ESOH). *"For the system, safety considerations will be provided for in the program baseline to support sustainable operation and maintenance. The program will maintain a system safety process to identify and prevent ESOH hazards where possible, and shall manage ESOH hazards where they cannot be avoided."*

(f) Habitability. *"The program shall establish requirements for the physical environment (e.g., adequate space and temperature control) and, if appropriate, requirements for personnel services (e.g., medical and mess) and living conditions (e.g., berthing and personal hygiene) for conditions that have a direct impact on meeting or sustaining system performance or that have such an adverse impact on safety, quality of life and morale."*

(g) Survivability. *"The design shall address personnel survivability issues including protection against fratricide, detection, and instantaneous, cumulative, and residual nuclear, biological, and chemical effects; the integrity of the crew compartment; and provisions for rapid egress when the system is severely damaged or destroyed. The program shall address special equipment or gear needed to sustain crew operations in the operational environment."* (The document may need to cite the reference (4-o) requirement that capabilities documents incorporate force projection and survivability as key performance parameters (KPPs) and/or require derivative criteria).

e. CDD and CPD should state attributes that support mission performance, safety, reliability, maintainability and sustainability should be considered, with particular reference to the type of system. Capabilities should address vulnerabilities and shortcomings of legacy systems. Where feasible, attributes should be stated in terms that reflect the capabilities necessary to meet the military mission (or related support and sustainability) in the intended environment. These attributes should be measurable and testable. Requirements for operation in various climactic settings and operational environments should be described in a way that allows for a design that will support appropriate developmental and operational testing and evaluations.

f. CDDs and CPDs may need to cite specific performance requirements for other potentially applicable ESOH areas such as: hazards of electromagnetic radiation to ordnance (HERO), hazards of electromagnetic radiation to fuel (HERF) and hazards of electromagnetic radiation to personnel (HERP); noise and vibration; military flight operations flight assurance (MFOQA); aviation safety; uncontrolled electrical and mechanical energy; ordnance and explosives safety; lithium battery safety; laser hazards; fall and walking/working surfaces; confined spaces; and software safety. Guidance for language addressing some of these common ESOH hazards is provided below. Particular programs are likely to require attention to areas not described here.

(1) Hazards of Electromagnetic Radiation to Ordnance (HERO), Hazards of Electromagnetic Radiation to Fuel (HERF) and Hazards of Electromagnetic Radiation to Personnel (HERP). Suggested language for CDDs and CPDs: *"The system shall be able to safely carry and deploy the full spectrum of weapons and ordnance delineated herein without any Hazards of Electromagnetic Radiation to Ordnance (HERO) or Hazards of*

Electromagnetic Radiation to Fuel (HERF) restrictions except to ground operations. Hazards of Electromagnetic Radiation to Personnel (HERP) will be managed by a process that ensures personnel exposure below references (*) or equivalent standards." * Cite references (4-p), (4-q), and (4-r) and/or related criteria, as appropriate to the system under consideration.

(2) Noise and Vibration. References (4-s) and (4-t) establish criteria for personnel exposures and provide guidelines for including requirements for noise control through the JCIDS and system safety process. Occupational noise exposure is the most prevalent work-related health issue in DoD, the Navy, and in general industry. Noise control is crucial to avoiding hearing loss, associated manpower losses, and injury compensation costs (over $3.4 billion in ten years throughout DoD). Noise at or below occupational exposure limits may also affect communications necessary for mission performance. Noise and vibration are typically produced by the same mechanical factors and represent uncontrolled energy that may impact users. Reduction of mechanical vibration in lower frequencies is often closely linked with noise control. Whole body vibration can affect visual acuity, operator performance and target acquisition. Severe vibration, especially at critical frequencies, may lead to motion sickness. Whole body vibration in ships, or even combat vehicles, may be produced at a frequency well below audiometric threshold 20 Hz (cycles/second). Segmental (hand-arm) vibration can impair performance and is associated with a peripheral vascular and neurological syndrome known as Reynaud's syndrome that may lead to reduced function, significant discomfort and permanent impairment. Vibration is often a critical aspect of mechanical system stress and may accelerate equipment failure. For certain critical systems, it may be appropriate to address vibration in a separate section. These may include shock and vibration for high speed vessels and whole body vibration for aircraft and ground combat vehicles, especially rotary wing vehicles. Acquisition program attention to noise and vibration minimization can reduce system life cycle costs and enhance use of systems in areas otherwise restricted by environmental law or in areas otherwise subject to early detection and targeting by enemy forces. Suggested language for CDDs and CPDs is provided below:

(a) *"The system will minimize noise and vibration hazards to crews and support personnel working near the system or its supporting infrastructure through engineering controls*

(objective) or a combination of engineering, administrative procedures and protective equipment (threshold) to ensure personnel exposures are below 84 and maximum segmental and whole body vibration below the criteria provided by reference (*). The system will be designed so that effective communications are not disrupted by system or ambient noise and habitability standards will be met." * Cite references (4-s), (4-t) and/or related criteria, as appropriate to the system under consideration.

(b) *"Maximum segmental and whole body vibration (and shock) below the criteria provided by reference (*) or equivalent criteria, for a period of four hours (or other suitable interval, based on expected period of exposure and anticipated maintenance operations (for vibrating hand tools)".* * Cite reference (4-r) and/or related criteria, as appropriate to the system under consideration.

(3) Military Flight Operations Quality Assurance (MFOQA). Reference (4-u) establishes the requirement for Military Flight Operations Quality Assurance (MFOQA) in all future manned and unmanned aircraft acquisition. Legacy aircraft are excluded only when cost-benefit analysis demonstrates the need for exemption. Suggested language for CDDs and CPDs: *"The aviation system (aircraft and all related ground support) will provide Military Flight Operations Ouality Assurance (MFOQA) capability consistent with reference (4-u) that allows for interface consistent with HFE practice; related training, support and integration into the operations and support strategy and related equipment."*

(4) Aviation Safety. Reference (4-v) establishes policy on aviation safety system avionics to include flight incident recorders, flight data recorders (FDR), global positioning systems (GPS); ground proximity warning systems (GPWS) and integrated material diagnostic systems (IMDS). Therefore, it is recommended that acquisition capabilities documents cite the requirements for compliance with the technology described in this reference.

(5) Uncontrolled Electrical and Mechanical Energy. Uncontrolled electrical and mechanical energy can inflict trauma to operators and maintenance workers. Manpower-intensive administrative controls may be required if optimal control methods are not integrated into system design and development. Design for safety should eliminate or mitigate the risk of such injury during equipment operation and maintenance. Suggested

language for CDDs and CPDs: *"Mechanical isolation and lock-out of hazardous energy sources will be considered in design to eliminate the need for procedural isolation and minimize the risks to system and personnel safety."*

References

(4-a) DOD Directive 5000.1, The Defense Acquisition System, of 12 May 03
(4-b) DOD Instruction 5000.2, Operation of Defense Acquisition System, of 12 May 03
(4-c) SECNAVINST 5000.2C, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, of 19 Nov 04
(4-d) SECNAVINST 5100.10J, Department of the Navy Policy for Safety, Mishap Prevention, Occupational Health and Fire Protection Programs, of 26 Oct 05
(4-e) MIL-STD-882D, Standard Practice for System Safety, of 10 Feb 00
(4-f) Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3170.01E, "Joint Capabilities Integration and Development System," 11 May 05
(4-g) Chairman, Joint Chiefs of Staff Manual (CJCSM) 3170.01b, "Operation of the Joint Capabilities Integration and Development System," 11 May 05
(4-h) MIL-HDBK-46855A, Human Engineering Requirements for Military Systems, Equipment and Facilities, of 17 May 99
(4-i) MIL-STD-1472F, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, of 23 Aug 99
(4-j) ASTM F1337, Standard Practice for Human Engineering Program Requirements for Ships and Marine Systems, Equipment, and Facilities, of 01
(4-k) ASTM F1166-95a, Standard Practice for Human Engineering Design for Marine Systems, Equipment and Facilities, of 2006
(4-l) OPNAVINST 9640.1A, Shipboard Habitability Program, of 3 Sep 96
(4-m) National Aerospace Standard (NAS) 411, Hazardous Materials Management Program, of 19 Jan 95
(4-n) NAVSEAINST 3900.08A, Human Systems Integration (HSI) Policy in Acquisition and Modernization of 20 May 05
(4-o) Joint Chief of Staff (Joint Requirements Oversight Council) Memo JRCOM 120-05, Policy for Updating Capabilities Documents to Incorporate Force Protection and Survivability Key Performance Parameters (KPP), of 13 Jun 05

(4-p) OPNAVINST 5100.19D Change 1, Navy Occupational Safety and Health (NAVOSH) Program Manual for Forces Afloat, of 30 Aug 01

(4-q) OPNAVINST 5100.23G, Navy Occupational Safety and Health (NAVOSH) Program Manual, of 30 Dec 05

(4-r) American Conference of Governmental Industrial Hygienists (ACGIH), Threshold Limit Values (TLVs) guidelines for occupational exposure for chemical substances and physical agents and Biological Exposure Indices (BEIs) for Chemical Substances, of 2006 (or latest edition)

(4-s) DODI 4715.13, DoD Noise Program, of 15 Nov 05

(4-t) DODI 6055.12, DoD Hearing Conservation Program of 5 Mar 04

(4-u) DOD OSD Memo Military Flight Operations Quality Assurance (MFOQA) Process Implementation, of 11 Oct 05

(4-v) CNO Memo 13222 N88F/9U660308, Naval Aviation Policy on Aircraft Safety Systems Avionics, of 9 Nov 99