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

IN REPLY REFER TO
OPNAVINST 9410.5A
N62
04 JANUARY 1996

OPNAV INSTRUCTION 9410.5A

From: Chief of Naval Operations

Subj: INTEROPERABILITY REQUIREMENTS, TESTING, AND CERTIFICATION FOR TACTICAL NAVAL WARFARE SYSTEMS (TNWS)

Ref:
(a) DOD Directive 4630.5 of 12 Nov 92, "Compatibility, Interoperability, and Integration of Tactical Command, Control, Communications and Intelligence (C^3I) Systems"
(b) DOD Instruction 4630.8 of 18 Nov 92, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C^3I) Systems
(c) CJCS Instruction 6212.01 of 30 Jul 93, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems"
(d) JIEO Circular 9002 of 23 Jan 95 "Requirements assessment and Interoperability Certification of C4I and AIS Equipment and Systems"
(e) DOD Directive 8320.1 of 26 Sep 91, "DOD Data Administration"
(f) DOD Manual 8320.1-M-1 of 15 Jan 93, "DOD Data Element Standardization Procedures"
(g) SECNAVINST 5400.15 of 5 Aug 91, "Department of the Navy, Research, Development, and Acquisition Responsibilities"
(h) SECNAVINST 5000.2A of 9 DEC 92, "Implementation of Defense Acquisition Master Policy, Procedures, Documentation and Reports"
(i) OPNAVINST 5000.42D of 19 Apr 93, "OPNAV Responsibilities in the Acquisition Process"
(j) OPNAVINST 5401.6K of 17 Dec 93, "Naval Forces Tactical Development and Evaluation Program"
(k) Navy Interoperability Configuration Management Plan for Procedural (NICMP-P) Interface Standards, 10 May 91
(l) Naval Warfare Tactical Data Base (NWTDB) Management Plan of Sep 92
(m) MIL-STD 6040 "U.S. Message Text Formatting Program"
(n) MIL-STD 6011 "Tactical Digital Information Link (TADIL) Standards"
(o) Navy Interoperability Test Plan for Procedural Interfaces (NITP-P)
(p) Link-4A Operational Specification (OS-404 Series)
(q) Link-11 Operational Specification (OS-411 Series)
(r) Link-14 Operational Specification (OS-414 Series)
(s) Link-16 Operational Specification (OS-516 Series)
(t) NWP 10-1-12 (Series) "Maritime Reporting System"
(u) NWP 10-1-13 (Series) "Joint Reporting System"
(v) Operational Specification for Over-The-Horizon Targeting GOLD (OS-OTG) (Series)

(w) COMOPTEVFOR/NCTSI Memorandum of Agreement (MOA) of 27 Jun 94

Encl: (1) Definitions
(2) Acronyms

1. Purpose. To implement current requirements for interoperability, testing, and certification of Navy Command, Control, Communications, Computers and Intelligence Systems (C4I) in accordance with references (a) through (d). Additionally:

- Implement Navy C4I data administration in accordance with references (e) through (f);
- Implement an integrated management process for harmonizing the various C4I data element, data base structure, Message Text Format (MTF), and Tactical Digital Information Link (TADIL) standards and interface development and implementation efforts, and;
- Reduce long term Tactical Naval Warfare System (TNWS) acquisition costs by evolving to a joint and theater compatible information architecture which will be applied to both requirements and engineering processes.

The operational policy contained herein is issued in accordance with reference (g) and in amplification of references (h) through (k). Due to dramatic changes in C4I interoperability requirements, an extensive rewrite, of the original OPNAVINST 9410.5 produced both this instruction and reference (l) which defines Naval Warfare Tactical DataBase (NWTDB) requirements and responsibilities. Both instructions require close reading for a thorough understanding of new requirements.

2. Cancellation. OPNAVINST 9410.5 of 24 May 90, "Database Communication Standards Interoperability Requirements for Tactical Naval Warfare Systems".

3. Scope/Applicability. This policy applies to all TNWS, and associated database production, procurement, acquisition, and support agencies; including those Navy organizations acquiring systems under rapid prototyping and fleet initiative programs.

4. Definitions. Terms used in this instruction are defined in enclosure (1).

5. Background. Traditionally measured in terms of adequacy of communication and the ability to exchange data across an interface, interoperability of C4I systems now considers the information technology functional areas of information, information transfer, and information processing.

a. Interoperability requires that all systems involved in warfare support (command, sensor, intelligence, electronic warfare, weapons, mission planning, logistics, administrative, and training) be able to exchange data. Today, that is difficult and expensive because of non-compatible data element definitions, naming conventions, and structures. Program managers are forced to develop and maintain specialized interface

design specifications because information standardization efforts have been fragmented, community specific or operationally ineffective.

b. Joint services established the U.S. Message Text Formatting (USMTF) Program to achieve inter-service compatibility, interoperability, and enhanced operational effectiveness of tactical command and control systems. Through the USMTF Configuration Control Board (CCB), they have established and maintained MTF message standards which prescribe the message types and internal structures (sets, fields, and data elements to be used by the services and agencies for the exchange of tactical information in joint operations) as documented in reference (m). The USMTF program applies to all formatted, character-oriented, and related voice message reports used in support of joint and combined operations. It is DOD policy that USMTFs are the mandatory standard for all record message information exchange and C4I system data exchange in the DOD which shall be used in all defense conditions from peacetime through crisis, war and post-attack. Likewise, in the real-time digital communications environment, joint services established the Tactical Digital Information Link (TADIL) program and associated TADIL Configuration Control Board (CCB). The requirements group supporting bit oriented messages is the Joint Multi-TADIL Standards Working Group (JMSWG). The exchange of real time tactical digital information is by data link (TADIL) communication. Joint data link standards are documented in reference (n), and Joint Tactical Information Distribution System (JTIDS) Technical Interface Design Plan-Test Edition (JTIDP-TE). Joint data link standards apply to all U.S. Navy data link capable platforms as promulgated by N6 in NCTSI-developed Operational Specifications (references (o) through (s)).

c. Wth the advent of modern information technology, the new policy of using international standards and the increased emphasis on joint interoperability, C4I systems now exchange information using multiple message formats, data elements, and communications media. Database management, data exchange requirements and C4I systems interoperability requirements have become significantly more complex.

d. The "Joint C4I for the Warrior" and Navy "Copernicus" efforts set forth concepts, unifying themes, and principles for achieving C4I interoperability that is global, reliable, secure, and responsive to warfare operations. Interoperable automated databases and compatible data standards are essential to achieving these objectives. The Defense Information Systems Agency is developing the DOD Data Repository System (DDRS) which will be the authoritative source for normalized or standard data elements used in DOD systems. References (e) through (f) are key documents for implementing the DOD data administration procedures which determine the process for harmonizing DOD data elements. All DOD components are directed to support this effort.

6. Policy. Joint C4I interoperability is paramount. The process of establishing joint C4I requirements, implementing joint standards, configuration managing C4I standards, and testing and certifying C4I systems for standards conformance supports joint interoperability. References (a) through (c) mandate that C4I

systems achieve joint certification prior to Milestone III, or, for post Milestone III systems, prior to joint operational use. Navy C4I systems must acheive joint interoperability certification prior to operational evaluation unless granted a waiver by CNO.

a. For the purposes of compatibility, interoperability, and integration, all C4I systems developed for use in support of U.S. forces are defined to be for use in joint operations and must be certified "interoperable" with systems with which they have a requirement to exchange information.

b. New Navy C4I systems and changes to existing systems that must interact with or be integrated into the DOD C4I infrastructure will use joint information technology standards. Navy unique standards will be used only when no other standards satisfy C4I systems Information Technology (IT) requirement and when approved through the requirements review process in accordance with references (b) and (c). Approved procedural standards include Joint Interoperability of Tactical Command and Control Systems (JINTACCS) and/or Over-the-Horizon Targeting Gold (OTG) formats for information transfer and the NWTDB structures and data element for information and information processing. Reference (k) details JINTACCS message standard baselines and operating procedures within the Navy, as well as certain JINTACCS related Navy unique message standards.

c. IT standards change periodically. Generally, joint certification will require new or updated systems to satisfactorily comply with standards baselines existing during the development phase in order to achieve certification authority to go to Milestone III and/or field operational systems. When establishing the acquisition baseline, program offices should consider the evolving standards environment as well as the need to interoperate with legacy systems. Legacy system programs must implement current standards baselines with each software and hardware upgrade. Legacy systems that cannot/will not be upgraded must request and be granted an Interim Authority To Operate (IATO).

d. C4I systems testing will be conducted in accordance with references (a) through (d) and (o) to ensure compliance with established information, information transfer, and information processing standards. The complexity of end-to-end certification testing at both Navy and joint levels warrants early test agency involvement in developmental testing. The U.S. Military Communications Electronics Board Interoperability Test Panel (USMCEB-ITP) may grant an Interim Authority To Operate (IATO) to enable an evolutionary developed system to demonstrate concepts and train operators in support of operational testing. Given the global nature of current naval communications, new equipment must be laboratory tested, at a minimum, to preclude degradation of operational nets during interim operations. Rigorous testing in a laboratory environment will not only help ensure interoperability, but also preclude degradation of operational systems as new systems are introduced. IATO shall not be construed as approval for unrestricted fleet release of equipment and software.

e. Software Trouble reports (TR) must be submitted in accordance with MIL-STD 498, Appendix C.

(1) TRs delineate a malfunction, inadequacy or recommended change/enhancement to a product to meet documented requirements or increase efficiency and effectiveness of the product. TRs will be reviewd through normal Program Configuration Control Board (CCB) process in accordance with MIL-STD 973 and a library of TRs will be maintained. Program CCBs may change TRs sumbitted by field activities and developers. TRs Originated by an independent Test and Evaluation agent, per paragraph 7.e, 7.h. and 7.I of this instruction, can only be changed by that Testing Agency. Testing Agencies will provide a complete explanation associated with each TR submitted.

(2) The following TR priority definitions apply:

(a) Priority 1 - Prevent the accomplishment of an operational or mission essential capability. Jeopardize safety, security, or other requirement designated critical;

(b) Priority 2 - Adversely affect the accomplishment of an operational or mission essential capability and no work-around solution is known. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known;"

(c) Priority 3 - Adversely affect the accomplishment of an operational or mission essential capability but a work-around solution is known. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known;

(d) Priority 4 - Result in user/operator inconvenience or annoyance but does not affect a required operational or mission essential capability. Result in inconvenience or annoyance for development or support personnel, but does not prevent the accomplishment of those responsibilities;" and

(e) Priority 5 - Any other effect."

(3) Software problems are to be evaluated based on systems mission and how any problem impacts other systems in the C4I architecture. Examples are:

(a) Priority 1 - Data loss or corruption (unique attributes, positional data), miscorrelation, system halts, safety items, and failure to maintain a consistent track picture.

(b) Priority 2 - Net loading, communication interfaces, tracker errors, or data loss or corruption (non-unique data) for which there is no "work- around."

(c) Priority 3 - Same as priority 2 except there is a "work-around."

(d) Priority 4 - Human-machine interface (HMI).

(4) Software problems are evaluated based on systems mission and how the problem impacts other systems in the Naval and joint C4I architecture. The focus is not on TR priorities but on which TRs must be fixed. *"A priority 1 will result in a non-certification recommendation."*

7. Responsibilities.

a. Director of Space and Electronic Warfare (N6).

(1) Act as the Chief of Naval Operations (CNO) point of contact for C4I interoperability.

(2) Determine whether a program continues in its developmental cycle to OPEVAL and fleet release based on performance or test results.

(3) Issue information technology C4I procedural and technical standards for TNWS including:

(a) information standards (e.g., Operational Specifications (OPSPECS) for OTH-T Gold message formats);

(b) data link OPSPECS based upon joint standards for TNWS, i.e.; real time tactical digital information requirements (e.g.; OPSPECS for Link-4A, Link-11, Link-14, Link-16 and Link-22). Required protocols, procedures, and implementations shall be included to ensure Navy, joint, and international interoperability.

(c) NWTDB standards implementation guidance and direction;

(d) information processing standards (e.g., Battle Group DataBase Management (BGDBM) functional requirements, OTH-T System Level Specification - Ship Tracking Algorithm , OTH-T System Level Specification - Correlation Algorithm), and;

(e) information transfer standards (e.g., IDS-8648, IDS-8649, OTH-T System Level Specification - Communications).

(4) Adopt joint standards as Navy standards wherever possible.

(5) Represent fleet data requirements in information technology standards configuration management forums.

(6) Coordinate Navy position and submit recommendations to JCS (J-6), DISA/JIEO, USMCEB, Defense Intelligence Agency (DIA), National Security Agency (NSA) and Defense Mapping Agency (DMA) regarding integrated C4I interoperability standards.

(7) Certify compliance with joint interoperability standards to DISA upon satisfactory completion of interoperability testing by the Navy Center for Tactical Systems Interoperability (NCTSI) and Space and Naval Warfare Systems Command (SPAWAR).

(8) Request for IATO to the USMCEB ITP for new systems or software releases upon receipt of NCTSI, SPAWAR, and Commander, Operational Test and Evaluation Force (COMOPTEVFOR) assessments of potential impact upon operational networks.

(9) Plan, program, and budget adequate resources for NCTSI configuration management and certification test support for MTF, TADILS and Network Design Facility functional requirements.

(10) Chair the Implementation Action Council for Command and Control Systems (IMPACCCS) to ensure that approved Navy and joint procedural and technical interface standards are implemented in Navy systems in accordance with required implementation schedules.

b. Director Naval Intelligence (N2).

(1) Manage the submission and status of TNWS intelligence production requirements to DIA and NSA.

(2) Support N6 in Navy C4I data administration and data element harmonization.

(3) Plan, program and budget adequate resources to ensure Navy General Defense Intelligence Program (GDIP) and Tactical Cryptologic Program (TCP) systems implement joint and Navy C4I procedural and technical standards.

(4) Ensure GDIP and TCP systems comply with the interoperability testing requirements of references (a) through (d) and (o) and use approved Navy and joint procedural and technical standards.

c. Deputy Chief of Naval Operations for Resources, Warfare Requirements, and Assessments (N8) will:

(1) Ensure approved Mission Need Statements (MNSs) and Operational Requirements Documents (ORDs) for C4I systems are submitted to Joint Staff (J6I) for C4 interoperability certification.

(2) Ensure C4I system requirements documents address required information system interfaces and standards.

(3) Address joint and combined tactical information interoperability capabilities in the Program Objective Memoranda (POM) appraisal.

d. CNO Resource and Program Sponsors.

(1) Plan, program and budget adequate resources to transition legacy C4I systems to approved joint or Navy information standards during major upgrades, or as feasible, but not later than the year 2000.

(2) Address information interoperability requirements in MNSs and ORDs.

(3) Ensure C4I systems are compliant with information standards prior to Milestone II, and ensure systems are tested and certified by NCTSI and SPAWAR for interoperability prior to submission to the Joint Interoperability Test Command (JITC) for final C4I certification and OPEVAL.

(4) Ensure resources are available for funding test systems, test platforms and testing support for all phases of TNWS information interoperability life cycle: acquisition, system and equipment implementation, configuration management, developmental testing for compliance with interoperability requirements and certification testing for compliance with interoperability requirements.

e. COMSPAWARSYSCOM.

SPAWAR interoperability testing is conducted in order to check for data loss. This is done by testing for (1) proper data transfer via satellite communications, (2) tactical data systems' tracking data algorithms being used correctly, (3) track or position deletion, merge or edited being replicated properly where it should be both ship to ship, or workstation to workstation; and (4) data being correlated correctly to the correct track in the data base and plotted on the correct place on a TDP's (Tactical Display Processor) map. SPAWAR responsibilitiy is to:

(1) Coordinate the implementation of interoperability standards in C4I systems through the Force Warfare System Engineering Board (FWSEB); specifically,

(a) Develop and manage a C4I configuration status accounting and audit process to verify compliance with configuration management policies for information technology standards.

(b) Participate in standards and interoperability working groups that provide a forum for producer and fleet concerns.

(2) Develop and maintain (for approval and promulgation by CNO (N6)) TNWS technical interface standards.

(3) Develop for CNO (N6) publication the following plans of action by which this instruction and other DOD interoperability policies will be carried out:

(a) In coordination with NCTSI, the Navy Interoperability Program Management Plan (NIPMP), including a coordinated plan and implementation schedule of information technology standards by existing TNWS. Include in the NIPMP a schedule showing implementation dates, platform or platform group and implementation planning record (IPR) number, for the specific tactical data exchange capabilities required in the implementation appendices of references (m) through (v).

(b) Navy Interoperability Test Plan for Technical Interfaces (NITP-T).

(c) Navy Interoperability Configuration Management Plan for Technical Interface Standards (NICMP-T)

(4) Review TNWS documentation and provide inputs to system design reviews, preliminary design reviews, and critical design reviews to ensure consideration of interoperability requirements early in the development life cycle.

(5) Establish the organization and criteria necessary to ensure that program development activities implement joint messages as promulgated in NCTSI-developed OPSPECS. Ensure common tactical data system functions and procedures whenever possible to provide for capability between operating forces.

(6) Establish the organization and criteria necessary to verify compliance with information processing standards (e.g., BGDBM functional requirements, OTH-T System Level Specification-Ship Tracking Algorithm, OTH-T System Level Specification-Correlation Algorithm, OTH Detection, Classification and Targeting System Specification) and information transfer standards (e.g., IDS-8649, OTH-T System Level Specification-Communications).

(7) In coordination with NCTSI and COMOPTEVFOR, conduct information technical interface certification. Provide the results of testing to CNO (N6), copy to Navy Center for Tactical Systems Interoperability (NCTSI) and COMOPTEVFOR, for representation to DISA prior to Operational Evaluation

(OPEVAL). Coordinate with acquisition program managers and Navy programming centers. The goal is to ensure correct design and implementation of appropriate technical interoperability standards.

(8) Support certification testing by NCTSI, prior to OPEVAL, of procedural interface standards when implemented in new TNWSs.

(9) Conduct developmental interoperability testing to support a recommendation for IATO when schedules will not permit full certification testing prior to use on operational networks. This testing will be designed to rapidly assess, in a laboratory environment, the risk of degradation to operational networks if the system is granted IATO. Interoperability certification will be conducted in TNWS configurations intended for operational use. Coordinate the effort with acquisition program managers, Navy programming centers, COMOPTEVFOR and NCTSI. Provide test results expeditiously to cognizant programs to allow timely incorporation of required changes into the system.

(10) Coordinate with NCTSI to conduct parallel or mutual testing of systems, if feasible, to reduce the laboratory testing lead time for programs to reach operational testing.

(11) Ensure each Operational Requirement Document (ORD) addresses a method for determining the essential elements of information required to satisfy mission functionality.

(12) Apply Warfare Systems Architecture and Engineering processes to support acquisition managers in identifying interoperability issues, including Theater Intelligence Architecture Program (TIAP) compatibility, through use of Force Systems Engineering Plan (FSEP) and the associated resolution of interface, force performance and test requirements, as well as direct fleet liaison.

(13) Ensure the intent of references (a) through (d) is reflected in appropriate interface documentation.

(14) Support NCTSI allied interoperability testing as required.

f. Systems Development Managers (Systems Commanders (SYSCOMs), Program Executive Officers (PEOs), and Direct Reporting Program Managers (DRPMs)).

(1) Ensure C4I systems comply with this instruction.

(2) Ensure approved joint and Navy information specifications, standards and formats (e.g., TADIL, MTF, OTG, and NWTDB formats and OPSPECS) together with CNO approved information processing and information transfer specifications and standards are incorporated into the design of TNWSs as appropriate.

(3) In each ORD and at each design review specify what other C4I systems the system under consideration is expected to interface with, and which interoperability standards have been planned for or incorporated. When compliance with existing standards cannot be accomplished within programmatic constraints, provide an explanation and the impacts on interoperability to CNO, OPTEVFOR, NCTSI and SPAWAR, and formally request waiver of the above requirements from CNO (N6).

(4) Place subject systems and specifications under approved configuration management. Ensure the impact of systems design on other interfacing systems or equipment is mutually documented and agreed upon with the other interfacing acquisition program managers, prior to executing the acquisition programs.

(5) Ensure each ORD addresses the requirements for compatibility and interoperability with joint and combined communication security, and Defense Communications Systems (DCS), or other non-tactical data systems or equipment.

(6) Ensure interoperability and compatibility are considered in program budgets. Specifically, include in fiscal planning, funds for implementation of information standards throughout the life cycle of the system.

(7) Ensure mutually documented and agreed interservice, interagency and international capabilities are considered before new development efforts begin.

(8) Coordinate with NCTSI and SPAWAR for identification of interoperability requirements. Incorporate interface testing issues and criteria for Navy, and joint testing early in Defense Acquisition Board (DAB)/non-DAB OR and Developmental Testing/Operational Testing (DT/OT) plan formulation phases. Forward a copy of the Test and Evaluation Master Plan (TEMP) and DT plans to NCTSI and SPAWAR. Program and schedule resources to support coordination of interface standards and review TEMPs/MNSs/ORDs and DT plans as required.

(9) Obtain certification of compliance with CNO-approved implemented information procedural interface standards from NCTSI and implemented information technical interface standards from SPAWAR before new TNWSs are presented to DISA as complying with joint interoperability standards by CNO(N6). Program and schedule resources to support Navy and joint interoperability certification testing prior to OPEVAL. If TNWSs cannot be certified interoperable prior to OPEVAL due to development delays or constraints, Program Managers shall apply for IATO in writing to CNO(N6) via NCTSI. Schedule interoperability certification by NCTSI at the earliest opportunity to minimize the time period of the IATO.

(10) Obtain re-certification of joint compliance with implemented information processing, and information transfer standards from NCTSI and SPAWAR

when software versions are updated or when certification or recertification has not been accomplished within the preceding 36 months.

g. Fleet Commanders in Chief.

(1) Ensure C4I systems developed under rapid prototyping and fleet initiative programs incorporate only approved technical and procedural interface standards and data standards.

(2) Ensure rapid prototype and fleet initiative systems are not integrated with other C4I systems without being properly tested by NCTSI and SPAWAR and certified by JITC.

(3) Advise CNO (N6), OPTEVFOR, NCTSI, SPAWAR of all TNWSs being developed under rapid prototyping and fleet initiative programs and provide them with system description and implementation.

h. COMOPTEVFOR.

(1) Ensure joint interoperability is included for evaluation as critical operational issues in all operational test and evaluation plans and documents. Operational test results will be cited in the Evaluation Report (ER) (OPNAV REPORT SYMBOL 3960-12) and provided to the Chief of Naval Operations, Program Manager, SPAWAR 32, NCTSI and Office of Naval Intelligence (ONI) upon completion of each operational test phase and database fill requirements.

(2) Address interoperability at appropriate Navy Program Decision Meetings (NPDM).

(3) Coordinate with NCTSI and SPAWAR when either of them is conducting certification testing prior to OPEVAL.

(4) Ensure SPAWAR technical standards testing and NCTSI procedural standards testing are completed prior to OPEVAL.

i. Navy Center for Tactical Systems Interoperability (NCTSI)).

NCTSI interoperability testing is conducted to ensure a common tactical picture between Tactical Naval Warfare Systems (TNWS), and across Joint and Allied interfaces. This is accomplished through standards compliance and multiple interface or distributed system testing to ensure accurate presentation of tactical data is shared by all systems on a network or data link. This procedural testing includes accuracy of retransmission, data forwarding rules, and correct interpretation and display of tactical message standards. Systems communicating over multiple interfaces will have all interfaces examined during interoperability certification. This ensures data is properly fused or correlated, and

accurate tactical display is presented to the system operator. Track accountability and database integrity testing is conducted to ensure all participating systems in the network or data link maintain an equivalent tactical picture. NCTSI will further;

(1) Act as the primary Navy activity responsible for technical support to CNO for configuration control of Navy and joint interoperability documentation and development of interoperability certification testing criteria.

(2) Develop, in coordination with the fleet and the systems commands, TNWS procedural interface and information standards for approval and issuance by CNO. These standards are published in references (m), (n), and (p) through (v).

(3) Produce and maintain for CNO publication, the appropriate OPSPECS and Standard Operating Procedures (SOPs) for CNO-validated procedural interface standards. Ensure OPSPECS, NWTDB and OS-OTG conform to joint TADIL, and USMTF standards. Where conflicts between governing standards exist, identify them to CNO and work to resolve them in appropriate forums.

(4) Establish and chair the Operational Interoperability Requirements Groups (OIRG) and Technical Interoperability Standards Groups (TISG). Membership will be drawn from operational commanders, program sponsors, program managers, NWTDB functional database managers, and others as necessary. Each primary activity should provide a representative who is knowledgeable and authorized to speak/negotiate for that activity. Additional information and guidance regarding these forums can be found in reference (k).

(5) Establish, operate, and maintain the Navy Network Design Facility.

(6) Develop for CNO publication the following plans of action by which this instruction and other DOD interoperability policies will be carried out:

(a) Navy Interoperability Configuration Management Plan for Procedural Interface Standards (NICMP-P). The NICMP-P details the initiation, processing analysis, testing approval, implementation and status accounting process needed to control and maintain the JINTACCS message standard baselines and operating procedures within the Navy.

(b) Navy Interoperability Test Plan for Procedural Interface Standards (NITP-P).

(7) Establish the organization and criteria necessary to verify TNWS program compliance with Navy and joint procedural information and information processing (e.g., TADIL OPSPECS, OTG OPSPECS, JINTACCS) interface standards.

(8) Conduct developmental interoperability testing of CNO approved procedural standards as implemented by TNWSs. This testing shall be requested by the acquisition program manager or Navy programming center, and will not interfere with certification testing. Test results are provided directly to the program manager or Navy programming center. Associated developmental testing costs are the responsibilityof the program manager or Navy programming center.

(9) Conduct certification testing of TNWS required implementation of established procedural interface standards and certify interoperability of such systems to CNO prior to OPEVAL. Coordinate this effort with acquisition program managers and Navy programming centers. Interoperability certification will be conducted in TNWS configurations intended for operational use.

(10) Re-certify that TNWSs correctly implement TADIL and USMTF procedural interface information standards prior to fleet introduction of modified/enhanced system software, especially those systems implementing TADILs and USMTFs whose software is modified due to message standard updates (e.g., repromulgation of reference (m) or (n)), increased functionality, or when the system has not been certified within the previous 36 months.

(11) Coordinate with SPAWAR to conduct parallel or mutual testing of systems, if feasible, to reduce the laboratory testing lead time for programs to reach operational testing.

(12) Act as the Navy Participating Test Unit Coordinator (PTUC) for joint MTF and TADIL test certification. Coordinate the Navy's participation in the joint certification test program for procedural interfaces as described in references (c) and (d). Act as the Navy voting representative to the Joint Analysis Review Panel (JARP).

(13) Represent CNO (as specifically assigned by N6) in joint and allied forums for establishment and maintenance of procedural interface standards.

(14) Act as Navy tactical systems representative at the Defense Intelligence Data Element Standards Committee (DIDESC).

(15) Review the NWTDB Standards and Structures Manuals for CNO (N6).

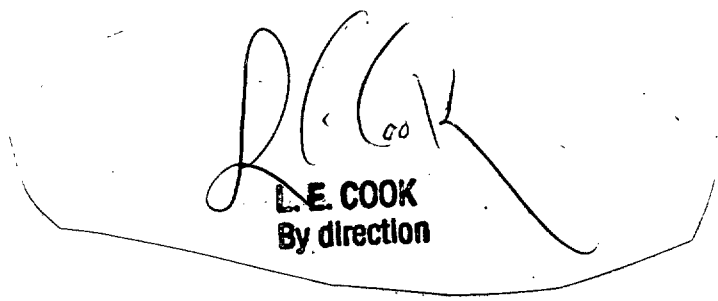
(16) Act as the Navy voting representative to the joint TADIL and USMTF Configuration Control Boards.

(17) Coordinate with fleet and system commands the development of data link network design.

(18) Conduct allied interoperability testing of CNO approved procedural interface standards requested by allied governments provided an IPO approved Foreign Military Sales (FMS) contract case is in place.

(19) Conduct joint and combined interoperability testing for procedural interfaces as described in references (c) and (d).

(20) Perform assigned additional duty (ADDU) for COMOPTEVFOR as interoperability testing agent for OT&E of Navy C4I systems in accordance with reference (w).



Distribution:
See Next Page

Distribution:
SNDL

A1	(Immediate Office of the Secretary (ASSTSECNAV RD&A AND C4I, EW, Space, only))
A1J1A	(PEOTACAIR)
A1JIB	(PEOASWASM)
A1J1C	(PEOCMPANDUAV)
A1JID	(PEOSPACOMMSENS)
A1J1E	(PEOSURFSHIPASWSYS)
A1J1F	(PEOSUBCBTWPNSYS)
A1J1G	(AEGIS PROG MGR)
A1J1I	(DRPM AAA (SSN21))
A6	(CMC (C4I only))
B2A	(Special Agencies, Staffs, Boards, and Committees (JCS J6, J2 and J3))
B2E	(Defense Mapping Agency Components and Elements (DMAHTC, only))
B3	(College and University (Commandant Industrial College of the Armed Forces, only))
21A	(Fleet Commanders in Chief (N2, N3 AND N8, only)
23A1	(Naval Force Commander LANT (EWOPFAC, only))
24A1	(COMNAVAIRLANT)
24A2	(COMNAVAIRPAC)
24D2	(COMNAVSURFPAC)
26F3	(COMOPTEVFOR)
50A	(Unified Commands (USCINCLANT J2, J3, J6 and USCINCPAC J2, J3, J6, only))
C4EE	(CNA)
C4L	(DNL)
C20C	(NRL Det (Stennis Space Center, only))
C43A	(NSGD PNCLA FL)
C81A	(NISE-East Det St. Inigoes, MD)
D30	(NAVINFOSYSMGTCEN)
E3A	(NRL)
FD1	(COMNAVOCEANCEN)
FD2	(NAVOCEANO)
FD3	(FLENUMOCEANCEN)
FD4	(OCEANCEN)
FD5	(NAVOCEANCOMCEN)
FE1	(COMNAVSECGRU (G32, G52))
FE4	(NAVSECGRUACT)
FF38	(USNA)
FF42	(NAVPGSCOL)
FF44	(NAVWARCOL)
FF52	(NCTSI)

Distribution continued: (See page 17)

FG1	(COMNAVCOMTELCOM (00, 03))
FKA1A	(COMNAVAIRSYSCOM (00, 05, 546))
FKA1G	(COMNAVSEASYSCOM (00, 06, 06KC, 06KR, 06K2))
FKP1E	(NAVUNSEAWARCENDIV (Newport RI))
FKP4A	(NAVSURFWARCEN COASTSYSTA)
FKP4E	(NAVSURWARCENDIV (Bethesda MD, Dahlgren, VA))
FKQ3	(COMSPAWARSYSCOM (00,10, 30, 40, 70, 80, 90)
FKQ6C	(NCCOSC RDTE DIV (Codes 431, 451, 452))
FKR3E	(NAVWPNEVALFAC)
FKR3I	(NAVTRASYSCEN)
FKR6A	(NAVAIRWARCENDIV (Warminster, PA Patuxent River))
FKR6B	(NAVAIRWARCENWPNDIV (China Lake CA, only))
FN1	(COMNAVSPACECOM)
FS1	(COMNAVINTCOM (06, 63))
FT1	(CNET)
FT22	(FCTC)
V12	(CG MCCDC)
V28	(CG MARCORSYSCOM)
A3	(CNO N09, N1, N2, N3/N5, N6C, N61, N62, N63, N64, N65, N7, N8, N80, N81, N82, N83, N84, N85, N86, N87, N88, N89, N096, OP-07, N090, N091)

Definitions

Certification. A statement attesting an interface has been verified as performing to an approved specification, or standard.

Data Element. (1) A named unit of data. It can be used to describe the atomic level of data, whether computerized or manual, as viewed by the user.

(2) In database usage, a named identifier of the entities and attributes that are represented in a database. (American Nation Standards Institute (ANSI) X.3.138-1988 and FIPS Pub 156 definition)

(3) In joint service usage, a basic unit of information having a meaning and subcategories (data items) of distinct units and values.

Data Fill. The actual data (or lack of) in the data element fields.

Data Translation. The computer conversion of one data element format into another format. (e.g., truncation of the 30 character ship name field into a 26 character field for use by a hardware and/or software constrained system)

Information Architecture. A database scheme of information categories (data sets) containing standardized data elements with designated data sources. The information architecture in the NWTDB Data Standards and Structures Manuals is a guide for defining essential elements of information to support operational functionality, and for internal system design to achieve a common relational database. The NWTDB structure is hardware and software independent.

Information Standards. The standardization of data elements, database structure, Message Text Formats (MTFs) and Tactical Digital Information Links (TADILs).

Interface. A boundary or point common between two or more similar or dissimilar command and control systems, subsystems, communications systems or equipment, or other entities across which necessary information flow takes place. A joint interface implies that the boundary is shared by two or more service/agencies. A combined interface is shared by two or more U.S. services/agencies. A combined interface is shared by entities from one or more US service/agency and one or more allied nation.

(1) Technical Interface. The functional, electrical, and physical characteristics necessary to allow the exchange of information across and interface between different C4I systems or equipment (JIEO Circular 9002).

a. Technical Standards. A specification for accomplishing transfer of information across an interface. Technical interface standards define:
the functional and physical requirements of an interface between systems (Interface Requirement Specification (IRS)); a detailed design of the requirements within the IRS

(Interface Design Document (IDD)); and, the functional, physical, and electrical interface characteristics (Warfare System Controlled Interface Documents (WSCIDs)).

(2) Procedural Interface. The methods and procedures employed to establish an interconnection within and between systems and/or equipment and to transfer information within or between systems and/or equipment (JIEO Circular 9002).

a. Procedural Standards. A specification for accomplishing exchange of information across an interface (e.g., OPSPEC 411, OPSPEC 516, OTG). Procedural interface standards define: the form or format in which information is to be exchanged; the prescribed information exchange language, syntax, vocabulary to be used in the information exchange; and, the protocols that govern information exchange.

Interoperability. The ability of systems, units or forces to provide services to, and accept services from other systems, units or forces, and to use the services so exchanged to enable them to operate effectively together (JCS Pub 1).

Joint Interoperability of Tactical Command and Control Systems (JINTACCS). The Joint program encompassing approved standards for machine readable bit-oriented TADIL and man/machine readable character oriented MTF messages.

Message Text Format (MTF). An approved standardized communication method using man/machine readable messages. MTF is characterized by its standardized, character-oriented message formats and transmission characteristics. United States Message Text Formats (USMTF) are JCS approved and mandated for both joint and intra-service usage. U.S. Navy tactical warfare systems also implement Navy unique MTFs. (e.g., OTH-T GOLD).

Naval Warfare Tactical DataBase (NWTDB).

(1) The management process to evolve to the common tactical data base that meets the needs of the Composite Warfare Commander and supports Naval, Joint, and Combined operations.

(2) The authoritative tactical data base, or subsets thereof, distributed by designated producers in accordance with the information architecture contained in the functional volumes which comprises the NWTDB Data Standards and Structures Manuals. Up-front harmonization of standards and structure permits the merging of data from multiple designated producers.

OTH-T GOLD (OTG). Over-the-Horizon Targeting GOLD, a CNO-approved man/machine-readable character-oriented message standard for information exchange between tactical systems.

Tactical Digital Information Link (TADIL). A JCS approved standardized communications link suitable for the transmission of machine readable only information. A TADIL is characterized by its standardized, bit-oriented message formats and transmission characteristics.

Tactical Information Interoperability. The ability of tactical naval warfare systems to use approved joint and Navy information standards, especially JINTACCS, NWTDB and/or OTH-T GOLD formats.

Tactical Naval Warfare System. Any C3 Intelligence (includes surveillance) or combat system that supports naval warfare.

ACRONYMS

BGDBM	Battle Group Data Base Management
C4I	Command, Control, Communications, Computers, and Intelligence systems
CCB	Configuration Control Board
CNO	Chief of Naval Operations
COMSEC	Communications Security
DAB	Defense Acquisition Board
DCS	Defense Communications System
DDRS	Defense Data Repository System
DIA	Defense Intelligence Agency
DIDESC	Defense Intelligence Data Element Standards Committee
DISA	Defense Information Systems Agency
DMA	Defense Mapping Agency
DOD	Department of Defense
DOP	Development Option Paper
DT	Developmental Testing
ER	Evaluation Report
FSEP	Force Systems Engineering Plan
FWSEB	Force Warfare Systems Engineering Board
GDIP	General Defense Intelligence Program
IATO	Interim Authority to Operate
IMPACCCS	Implementation Action Council for Command and Control Systems

IDD	Interface Design Document
IDS	Interface Design Specification
IOC	Initial Operational Capability
IRS	Interface Requirements Specification
IT	Information Technology
ITP	Interoperability Test Panel
JARP	Joint Analysis Review Panel
JIEO	Joint Interoperabilty and Engineering Organization
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JITC	Joint Interoperability Test Center
JMSWG	Joint Multi-Tadil Standards Working Group
JTIDP	JTIDS Technical Interface Design Plan
JTIDS	Joint Tactical Information Distribution System
JTIDP-TE	JTIDS Technical Interface Design Plan-Test Edition
MNS	Mission Need Statement
MTF	Message Text Format
NCTSI	Navy Center for Tactical Systems Interoperability
NICMP	Navy Interoperability Configuration Management Plan
NICMP-P	Navy Interoperability Configuration Management Plan for Procedural Interface Standards
NICMP-T	Navy Interoperability Configuration Management Plan for Technical Interface Standards
NIPMP	Navy Interoperability Program Management Plan
NITP	Navy Interoperability Test Plan
NITP-P	Navy Interoperability Test Plan for Procedural Interface Standards

NITP-T	Navy Interoperability Test Plan for Technical Interface Standards
NPDM	Navy Program Decision Meeting
NSA	National Security Agency
NWP	Naval Warfare Publication
NWTDB	Naval Warfare Tactical Data Base
OIRG	Operational Interoperability Requirements Group
ONI	Office of Naval Intelligence
OPEVAL	Operational Evaluation
OPSPEC	Operational Specification
OPTEVFOR	Operational Test and Evaluation Force
ORD	Operational Requirement Document
OT	Operational Testing
OTG	Over-the-Horizon Targeting Gold
OTH	Over the Horizon
OTH-T	Over-the-Horizon Targeting
POM	Program Objective Memoranda
SPAWAR	Space Warfare
SYSCOM	Systems Command
TADIL	Tactical Digital Information Link
TCP	Tactical Cryptologic Program
TEMP	Test and Evaluation Master Plan
TIAP	Theater Intelligence Architecture Program
TISG	Technical Interoperability Standards Group
TLWR	Top Level Warfare Requirement

TNWS	Tactical Naval Warfare System
USMCEB	Unite States Military Communications and Electronics Board
WSCID	Warfare System Control Interface Document.