



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

OPNAVINST 9410.5C
N2/N6
19 Feb 2013

OPNAV INSTRUCTION 9410.5C

From: Chief of Naval Operations

Subj: NAVY TACTICAL COMMAND, CONTROL, COMMUNICATIONS,
COMPUTERS, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE
INTEROPERABILITY PROCEDURAL INTERFACE STANDARDS
REQUIREMENTS, CERTIFICATION, AND TESTING

Ref: (a) DoD CIO Memo of 27 Mar 2012, Interim Guidance for
Interoperability of Information Technology and
National Security Systems
(b) DoD Directive 4630.05 of 5 May 2004
(c) DoD Instruction 4630.8 of 30 June 2004
(d) SECNAVINST 5000.2E
(e) CJCSI 3170.01H
(f) NAVSEAINST 9410.2A, NAVAIRINST 5230.2, and
SPAWARINST 5234.1
(g) Navy Interoperability Configuration Management Plan
for Procedural Interface Standards of July 2007
(NOTAL)
(h) MIL-HDBK-524, DoD Handbook Interoperable Systems
Management and Requirement Transformation of
26 Jun 2012 (NOTAL)
(i) COMNAVSURFORINST 3502.1D
(j) COMNAVAIRFORINST 3500.20D

1. Purpose. To provide guidance to echelon 1 to 3 commands relating to procedural interface standards, interoperability, certification of, and testing for naval command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems.

2. Cancellation. OPNAVINST 9410.5B.

3. Scope and Applicability. Per references (a) through (e), this guidance applies to all system development managers of tactical naval C4ISR systems which implement tactical data links (TDL) and other procedural interface standards which fulfill tactical data exchange requirements, to include those systems acquired via rapid prototyping and fleet initiative programs.

TDLs include link 4/11/16/22/ joint range extension application protocol A-B-C, multi-function advanced data link, integrated broadcast service, over-the-horizon targeting GOLD, variable message format, message text format, and any future advanced TDL. Procedural interfaces define an interconnection with and between systems and equipment to transfer information, and use common standard formats, language, syntax, vocabulary, and protocols that govern information exchange. The testing and certification accomplished under this instruction complement and are part of the warfare system certification decisions process defined in reference (f).

4. Guidance. Joint C4ISR interoperability requires the supporting processes of establishing requirements, implementing standards, conducting configuration management, and certifying C4ISR systems for standards conformance. References (a) through (c) mandate that C4ISR systems achieve joint certification prior to full rate production or prior to joint operational use.

a. New Navy systems and changes to existing systems that must interact with or be integrated into the Department of Defense (DoD) C4ISR infrastructure should use the current applicable joint information technology standards for the requirements noted in paragraph 3 above. These standards can be found in DoD Information Technology Standards Registry Online (DISR Online) at <https://gtg.csd.disa.mil>.

b. When establishing the acquisition baseline, program offices should consider the evolving C4ISR standards environment as well as the need to interoperate with legacy systems. Legacy system programs must implement current versions of joint approved military standards with each software and hardware upgrade. The use of the coordinated implementation provisions of reference (g), and the processes outlined in paragraph 5e(3) below, will mitigate the impact of technology refresh cycles on tactical naval C4ISR systems. Legacy systems that cannot or may not be upgraded, or systems that will be fielded in advance of Joint Interoperability Test Command (JITC) certification must request and be granted an interim certificate to operate (ICTO). Legacy system upgrades which do not affect a system's joint interfaces or interoperability will not require a JITC recertification.

c. Due to the complexity of interoperability certification, the DoD Chief Information Officer (CIO)- Interoperability Steering Group may grant an ICTO to enable an evolutionary system to demonstrate concepts and train operators in support of operational testing. At a minimum, new equipment must be laboratory tested to preclude degradation of operational networks during interim operations. An ICTO shall not be construed as approval for unrestricted fleet release of equipment or software. ICTOs shall be explicitly limited to the specific system requesting the ICTO and shall only be approved for a period of time set by the Interoperability Steering Group.

5. Responsibilities

a. Deputy Chief of Naval Operations for Information Dominance (CNO N2/N6) shall:

(1) Coordinate the Navy's position and submit recommendations to Joint Chiefs of Staff, DoD CIO, Defense Information Systems Agency, and National Security Agency regarding C4ISR interoperability standards.

(2) Plan, program, and budget adequate resources for Space and Naval Warfare Systems Command (SPAWARSYSCOM) Systems Center Pacific's (SSC Pacific) (Code 59) standards configuration management; interoperability certification testing, support, and associated test equipment; fleet validation and test support; and link 16 network design facility.

(3) Publish the Navy Interoperability Configuration Management Plan for Procedural Interface Standards with the assistance of SPAWARSYSCOM SSC Pacific Code 59.

b. Office of the Chief of Naval Operations (OPNAV) resource and program sponsors shall:

(1) Plan, program, and budget adequate resources to transition legacy C4ISR systems implementing procedural interface standards to approved joint or Navy information standards during major upgrades.

(2) Plan, program, and budget adequate resources for programs and initiatives requiring the use and implementation of

the joint Interoperable Systems Management and Requirements Transformation (iSMART) procedures, per reference (h), and tools for all new-start TDL platforms and systems.

(3) Address information interoperability requirements and verification plans in programmatic requirement documents.

(4) Plan, program, and budget adequate resources for testing support, per reference (d).

c. Commander, Navy Cyber Forces Command shall:

(1) Represent fleet issues and requirements in standards and interoperability working groups (e.g., Joint Multi-TDL Configuration Control Board (CCB), United States message text formats (USMTF) CCB, Technical Interoperability Standards Group (TISG), and Joint Multi-TDL Standards Working Group). Representation may be delegated to SPAWARSSYSCOM SSC Pacific Code 59 as required with adequate resources to fund the task requirements.

(2) Chair the Operational Interoperability Requirements Group to capture Navy component and fleet commander TDL requirements.

(3) Upon recommendation from SPAWARSSYSCOM SSC Pacific Code 59, approve C4ISR Message Implementation Plan for implementation by the appropriate program executive office (PEO).

d. Systems development managers (systems commanders, program executive offices, and direct reporting program managers) should:

(1) Use and implement the joint iSMART procedures and tools for all new-start TDL platforms and systems for use by the appropriate program managers. Legacy platforms should implement the iSMART procedures and tools contained in reference (h) to the maximum extent possible.

(2) Complete platform certification decisions prior to deployment per reference (f). The Naval Warfare Systems Certification Policy uses the interoperability certification accomplished under this instruction as one component of overall

platform capability, including other certifications such as weapon systems, aviation capability of ships operating aircraft, strike force, safety, and information assurance.

(3) Review and validate that applicable C4ISR systems comply with this instruction.

(4) Incorporate applicable joint and Navy information specifications, standards, and formats together with Chief of Naval Operations (CNO) approved information processing and information transfer specifications in the design on naval C4ISR systems, as appropriate.

(5) Budget required C4ISR interoperability plans, tests, and certifications as part of acquisition programming.

(6) Develop an information support plan for the system under development to fully document representative DoD architectural framework C4ISR system architecture behaviors and interfaces within the intended enterprise-wide architecture.

(7) Place subject systems and specifications under approved configuration management. Ensure the impact of the system under consideration on interfacing systems or equipment is documented and agreed upon with the other acquisition program managers, prior to initiating the acquisition program. Where identified by CNO N2/N6, ensure related TISG representation requirements are met.

(8) Review and validate that programmatic requirements address compatibility and interoperability with joint and combined communication security, and Defense Communications System or other non-tactical data systems or equipment per reference (a).

(9) Review inclusion of interoperability and compatibility standards in program budgets. Include the implementation of information standards throughout the life cycle of the system in fiscal planning.

(10) Prior to new development efforts, review that agreed upon joint, interagency, and allied coalition capabilities are included per reference (d).

(11) Coordinate with SPAWARSSYSCOM SSC Pacific Code 59 for identification of C4ISR mandated procedural interface standards (interoperability requirements).

(12) Complete Navy interoperability certification testing for new-starts by SPAWARSSYSCOM SSC Pacific Code 59 prior to milestone C for Navy systems. Plan, program, and schedule adequate resources to support Navy and joint interoperability certification.

(13) Incorporate interface testing issues and criteria, as identified in end-to-end and independent verification and validation testing, for Navy and joint testing early in the programmatic requirements documentation drafting, and developmental testing and operational testing plan formulation phases.

(14) Obtain, from SPAWARSSYSCOM SSC Pacific Code 59, re-certification of interoperability 48 months after previous certification, or when software version updates impact interoperability.

(15) Have programs submit a C4ISR Message Implementation Plan to SPAWARSSYSCOM SSC Pacific Code 59 for technical evaluation and forward to Navy Cyber Forces Command for approval prior to final coding.

e. Commander, SPAWARSSYSCOM

(1) As the budget submitting office, submit budget and funding requirements to CNO N2/N6 for SPAWARSSYSCOM SSC Pacific Code 59.

(2) As SPAWARSSYSCOM 5.0 chief engineer, ensure required C4ISR interoperability test planning and execution of events are properly reviewed by SPAWARSSYSCOM and SSC Pacific Code 59 technical authority and conducted per the SPAWARSSYSCOM systems engineering technical review process.

f. SPAWARSSYSCOM SSC Pacific Code 59 shall:

(1) Act as the primary Navy activity responsible for providing C4ISR interoperability services to Navy, joint, and allied forces.

(2) Establish specifications for Navy data link and C4ISR programs, and manage configuration of those specifications.

(3) Represent CNO in joint and allied forums for tactical C4ISR message standards.

(4) Act as the Navy voting member to the Joint Multi-TDL and USMTF CCBs and the Joint Symbology Standards Management Committee.

(5) Chair the TISG.

(6) Conduct tactical C4ISR verification and validation testing of fielded TDL systems installed on ships and aircraft as required by references (i) and (j). Identify TDL software problems and equipment malfunctions before units deploy.

(7) Operate and maintain the Navy's link 16 network design facility.

(8) Provide Navy representation on the U.S. Joint TDL Network Design Team per combatant command requirements as a voting member of the U.S. Network Management Sub-Group, Joint TDL Network Design Aid (JNDA) Integrated Product Team, and JNDA CCB.

(9) Conduct interoperability certification testing of C4ISR systems and provide a certification report directly to OPNAV, Naval Cyber Forces, and other activities that require the report prior to initial operational test and evaluation (IOT&E). Re-certification is required when an update that impacts interoperability is made to a previously certified C4ISR system, or after 48 months from the previous certification as per reference (a).

(10) Support PEO and direct reporting program managers efforts for joint interoperability certification of Navy C4ISR systems under test.

(11) Act as the Navy participating test unit coordinator, and serve as the Navy voting representative at joint analysis review panels.

(12) Provide the following mandated mission elements on a reimbursable basis (i.e., fee for service):

(a) Support interoperability of allied C4ISR systems when requested by allied governments provided an international program office-approved foreign military sales (FMS) agreement is in place.

(b) Support Commander, Operational Test and Evaluation Force (COMOPTEVFOR) as the interoperability testing agent for operational test and evaluation of Navy C4ISR systems.

(c) Comply with COMOPTEVFOR guidelines relating to independent operational testing.

(d) Apply the iSMART process where applicable to Navy implementation of C4ISR message standards.

(e) Ensure the appropriate iSMART documents are developed as well as support electronic standards management and requirement transformation toolset, per reference (h).

(f) Design, test and distribute Joint Tactical Information Distribution System/Multifunction Information Distribution System/Joint Tactical Radio System TDL research, development, test, and evaluation and FMS network designs as requested by program managers.

g. Fleet commanders shall:

(1) Incorporate approved technical and procedural interface standards and data standards into C4ISR systems developed under rapid prototyping and fleet initiative programs or obtain a waiver from the appropriate authority.

(2) Integrate rapid prototype and fleet initiative systems with other C4ISR systems only after those systems undergo testing and certification by SPAWARSSYSCOM SSC Pacific Code 59 and JITC.

(3) Advise CNO N2/N6 and SPAWARSSYSCOM SSC Pacific Code 59 of all Navy C4ISR systems being developed under rapid prototyping and fleet initiative programs.

h. COMOPTEVFOR shall:

(1) Include joint interoperability requirements and capabilities for evaluation as critical issues in all operational test and evaluation plans and documents. Cite operational test results in the evaluation report and provide results to CNO, Commander, Naval Cyber Forces, the program manager, SPAWARSSYSCOM, and SPAWARSSYSCOM SSC Pacific Code 59 upon completion of each operational test phase and database fill requirements.

(2) Address interoperability at appropriate Navy program decision meetings.

(3) Ensure Navy interoperability certification is successfully completed by SPAWARSSYSCOM SSC Pacific Code 59 prior to IOT&E and follow-on test and evaluation.

6. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy Manual 5210.1 of January 2012.



R. W. HUNT
Vice Admiral, U.S. Navy
Director, Navy Staff

Distribution:

Electronic only, via Department of the Navy Issuances Web site
<http://doni.documentservices.dla.mil>