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

IN REPLY REFER TO
3170
Ser N6N7/ 5U91622 2
27 May 05

From: Deputy Chief of Naval Operations, Warfare Requirements and Programs (N6/N7)

To: Distribution

Subj: FORCENET REQUIREMENTS/CAPABILITIES AND COMPLIANCE POLICY

Ref: (a) Naval Transformation Roadmap, 2003
(b) Naval Power 21
(c) Naval Operating Concept for Joint Operations
(d) FORCEnet Functional Concept, 7 February 2005
(e) Chief of Naval Operations Memorandum of 21 February 2002, Subj: Designation as Director of FORCEnet
(f) CJCSI 3170.01E, Joint Capabilities Integration and Development System, 11 May 2005
(g) CJCSI 6212.01C, Interoperability and Supportability of Information Technology and National Security Systems, 20 November 2003
(h) ASN(RD&A) Memorandum of 11 January 2005, Subj: Summary of FORCEnet EXCOMM of November 4, 2004

Encl: (1) FORCEnet Consolidated Compliance Checklist

1. Purpose. To establish initial policy and procedures for the definition of FORCEnet requirements / capabilities and an end-to-end process for their implementation and refinement to ensure applicable Navy programs, systems, and initiatives are compliant with the principles of Net-Centric Operations/Warfare (NCO/W).

2. Applicability. This policy applies to all Navy systems resourced by OPNAV (N6/N7) that exchange information with other systems. Applicability to all Department of the Navy programs will be addressed in a future SECNAV instruction.

3. Background.

a. As the operational construct and architectural framework for Naval Warfare in the Information Age, FORCEnet is the Navy and Marine Corps initiative to achieve NCO/W and Joint Transformation by providing robust information sharing and collaboration capabilities across the Naval / Joint force. FORCEnet is the centerpiece of Sea Power 21, and makes the other Sea Power 21 warfighting pillars (Sea Strike, Sea Shield, and Sea Basing) possible by integrating weapons, sensors, command & control, platforms, and warriors into a secure, networked, distributed combat force as part of the Global Information Grid (GIG). The FORCEnet vision is provided in references (a) through (d).

b. In reference (e), Chief of Naval Operations (CNO) assigned to the Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) the responsibility for leading FORCEnet efforts and for defining FORCEnet requirements.

4. FORCEnet Requirements / Capabilities and Compliance Process.

a. Compliance of individual Navy programs, systems, and initiatives with joint interoperability guidance is critical to Navy transformation from platform-centric stand-alone systems to a capabilities-based NCO/W environment. The development and implementation of FORCEnet requirements is focused on supporting joint interoperability requirements of the Joint Capabilities Integration and Development System (JCIDS) (reference (f)) and assists in further defining Naval implementation of the Net-Ready Key Performance Parameter (NR-KPP), detailed in reference (g). This is essential not only for development of effective warfighting capabilities, but also for the efficient management of Department resources.

b. Implementing FORCEnet necessitates a transformational approach to defining requirements / capabilities to allow FORCEnet to transcend traditional boundaries between networks, sensors, command and control, and weapons systems, while enhancing our focus on integration of the warrior. Accordingly, a more broad-based, collaborative, and integrated approach to development of these requirements / capabilities and technical

compliance must be instituted. Toward this end, N6/N7 will collaborate with other members of the FORCEnet "Triad" (Naval Network Warfare Command (NETWARCOM) and the Acquisition Community), and with key technical / acquisition forums such as the FORCEnet/C4I Virtual Systems Command and the FORCEnet Executive Committee (EXCOMM) when appropriate.

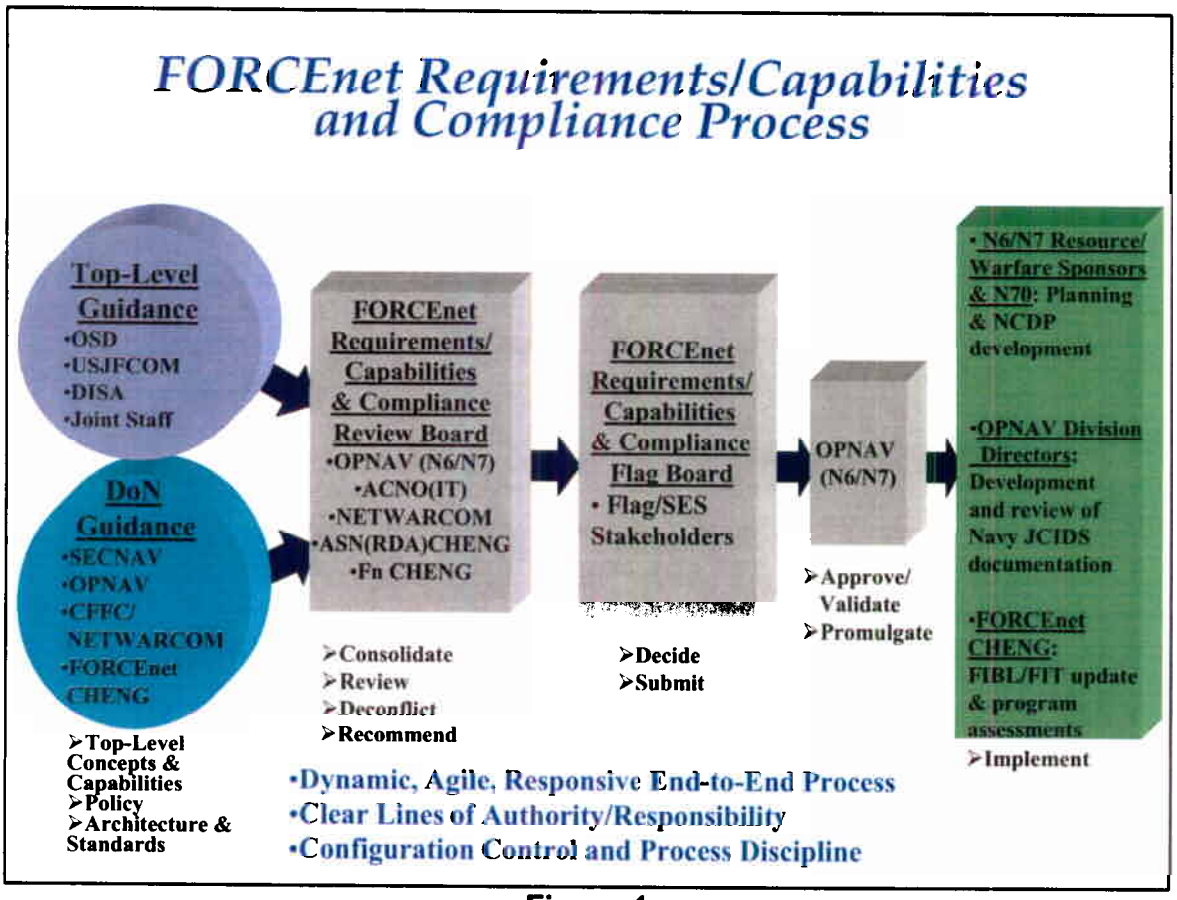


**Figure 1**

c. Figure 1 provides the planned FORCEnet Requirements / Capabilities and Compliance Process, which is comprised of the following steps:

(1) Collection of pertinent Top-Level guidance (e.g., from Office of the Secretary of Defense (OSD), U.S. Joint Forces Command (USJFCOM), Defense Information Systems Agency (DISA), and Joint Staff) and Department of the Navy (DoN) guidance

(e.g., from Office of the Secretary of the Navy (SECNAV), Office of the Chief of Naval Operations (OPNAV), Fleet Forces Command (FFC) / NETWARCOM, and Space and Naval Warfare Systems Command (SPAWARSYSCOM) / FORCEnet Chief Engineer (FORCEnet CHENG);

(2) Review of this guidance by a FORCEnet Requirements / Capabilities and Compliance (FRCC) Review Board, led by the Director for Net-Centric Warfare (N71) and consisting of Senior / O-6 level representatives of cognizant N6/N7 codes (e.g., N7C, N70, N75, N76, N77, N78). Representatives will be requested from the Assistant Chief of Naval Operations (Information Technology)(ACNO(IT)) (N098), NETWARCOM, ASN(RD&A)CHENG, FORCEnet CHENG, and other organizations deemed appropriate by N71. The FRCC Review Board will consolidate all applicable guidance, resolve any conflicting guidance, and develop recommended changes / updates to the FORCEnet Consolidated Compliance Checklist (FCCC) which will be forwarded to the FRCC Flag Board for review;

(3) The FRCC Flag Board, led by N71 and consisting of Flag / SES level representatives of the FORCEnet stakeholders, will review the proposed updates to the FCCC and resolve any issues identified by the FRCC Review Board. The FRCC Flag Board will forward its recommendations to N6/N7 for approval;

(4) N6/N7 will make any necessary adjustments to FRCC Flag Board recommendations and promulgate an update of the FCCC.

5. <u>FORCEnet Consolidated Compliance Checklist (FCCC)</u>.

a. The FCCC, enclosure (1), was developed by N6/N7 in response to Congressional direction to establish FORCEnet requirements. FCCC development was led by N71 in coordination with representatives of ACNO (IT), NETWARCOM, FORCEnet CHENG, ASN(RD&A)CHENG, Department of the Navy Chief Information Officer (DoN CIO), and Marine Corps Combat Development Command (MCCDC). It was endorsed by the FORCEnet Fleet Operational Advisory Group (OAG), supported in presentations to leadership of OSD, DISA, USJFCOM, and the Joint Staff, supported in JCIDS reviews with both the Net-Centric (NC) Functional Capabilities Board and the

Command & Control (C2) Functional Capabilities Board, and supported in briefings to Congressional staff. Accordingly, it is the initial baseline for development of expanded FORCEnet requirements / capabilities and will be updated using the process described in section 4 above.

b. The FCCC is a distillation of relevant DoD and DoN joint, net-centric, FORCEnet guidance and is organized in four sections:

(1) FORCEnet Operational Section, developed in coordination with NETWARCOM as the FORCEnet Operational Agent, is based on the FORCEnet Integrated Architecture Operational Views (OVs) being developed by NETWARCOM and MCCDC in coordination with the other FORCEnet stakeholders and OSD staff. The FORCEnet Integrated Architecture is being aligned with the GIG Integrated Architecture and will provide products which represent FORCEnet requirements / capabilities to support assessment of capabilities through the Naval Capabilities Development Process (NCDP). Closely related to the FORCEnet Integrated Architecture is the FORCEnet Capabilities List (FCL), also being developed by NETWARCOM and MCCDC in coordination with the other FORCEnet stakeholders. Both the FORCEnet Integrated Architecture and the FCL are based on concepts outlined by the CNO and the Commandant of the Marine Corps in reference (d). The FCL will map the FORCEnet capabilities in reference (d) to Joint capabilities, attributes, and measures in the Joint Functional Concepts (Net-Centric, Command and Control, and Battlespace Awareness), providing additional alignment of FORCEnet with Joint planning and JCIDS;

(2) FORCEnet System / Technical Section developed in coordination with FORCEnet CHENG, points to key joint, net-centric, and GIG technical guideposts and supporting implementation guidance and direction. These guideposts as well as FORCEnet architectures and Information Technology standards are further detailed in the "FORCEnet Technical Reference Guide for Program Managers," being developed by FORCEnet CHENG;

(3) FORCEnet Policy Section, developed in coordination with ACNO(IT) and other offices, provides a compendium of guidance in key FORCEnet policy areas. Of particular note is the Human Systems Integration (HSI) portion, as the warrior aspects will be a primary addition to NCDP planning for POM 08;

(4) FORCEnet Implementation Section, developed in coordination with ASN(RD&A)CHENG, references N6/N7 implementation guidance detailed in this memorandum as well as ASN(RD&A) acquisition guidance currently in draft. Promulgation of this N6/N7 memorandum and the referenced ASN(RD&A) memorandum fulfills FORCEnet EXCOMM planning addressed in reference (h).

6. Support to the Naval Capabilities Development Process(NCDP).

a. The NCDP is an N6/N7-led process developed to transform a threat-based, platform-centric requirements process into a capabilities-based assessment measured against "what it takes to win." It is aligned, organized, and integrated around Sea Power 21. The NCDP uses FORCEnet capabilities to assess program necessity, requirements, gaps, and overlaps, and provides a fiscal analysis of alternatives for achieving FORCEnet capabilities utilizing modeling and simulation, experimentation, science and technology, wargames, and lessons learned. The NCDP addresses the material component of FORCEnet capability.

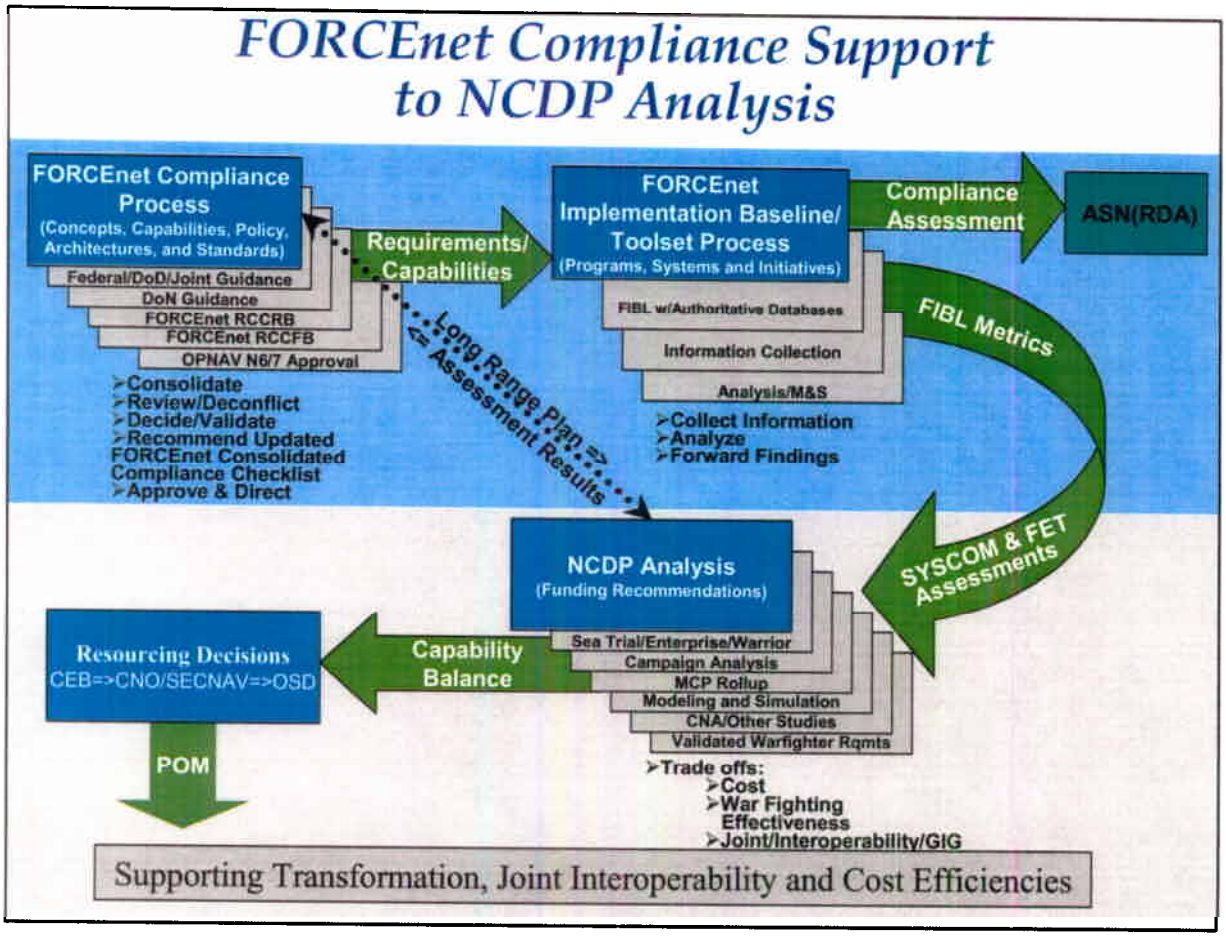


**Figure 2**

b. The FORCEnet Requirements / Capabilities and Compliance Process shown in figure 1 will support the NCDP, enhancing resourcing decisions by adding information on joint interoperability, GIG transition, and other key elements to the current tradeoff of warfighting capability and cost. As shown in figure 2, the FORCEnet Requirements / Capabilities and Compliance process will provide validated FORCEnet compliance criteria to the FORCEnet Implementation Baseline (FIBL) / FORCEnet Implementation Toolset (FIT) process (led by FORCEnet CHENG). Pursuant to FORCEnet EXCOMM planning and ASN(RD&A) direction detailed in reference (h), the FIBL / FIT process will assess individual DoN acquisition programs and initiatives

against FORCEnet / FCCC criteria and assign them to categories based on their compliance. The results of this assessment will undergo operational review by the FORCEnet Enterprise Team (FET) which is led by NETWARCOM with N6/N7 and Acquisition Community representation. Recommendations from the FET will be provided to appropriate N6/N7 Resource Sponsors, identifying non-compliant systems for potential consolidation or termination in the Integrated Sponsor's Program Proposal.

7. FORCEnet Compliance Governance.

a. N6/N7 will enforce FORCEnet compliance via synthesis of FORCEnet requirements / capabilities into Navy JCIDS documents during development and review of those documents, and into programmatic decisions made during the NCDP.

b. As detailed in reference (h), the Acquisition Community will enforce FORCEnet compliance via the FIBL / FIT process.

c. As detailed in reference (h), the Fleet will enforce FORCEnet compliance via the NETWARCOM-led FET process. Additionally, N6/N7 will work with NETWARCOM to implement FORCEnet compliance enforcement in the OAG process, and will work with Commander, Fleet Forces Command (CFFC) to enforce FORCEnet compliance in the Sea Trial process.

8. Action.

a. Director for Net-Centric Warfare (N71) is responsible for the oversight and maintenance of this policy, the FCCC, and related FORCEnet requirements / capabilities and compliance process. N71 will:

(1) Establish, convene, and chair the FRCC Review Board and FRCC Flag Board;

(2) Through the FRCC Review Board and FRCC Flag Board, develop proposed updates to the FCCC and submit them to N6/N7 for approval / validation and promulgation. The first update to the enclosure (1) FCCC resulting from this process should be submitted to N6/N7 NLT 07 July 2005;

(3) Work with NETWARCOM, MCCDC, and other FORCEnet Stakeholders to develop the FORCEnet Integrated Architecture Operational Views and with FORCEnet CHENG and FORCEnet Stakeholders to develop FORCEnet Integrated Architecture System and Technical Views to support alignment with joint integrated architectures;

(4) Work with NETWARCOM to develop the decomposition of FORCEnet capabilities in reference (d) to support their alignment with JCIDS via joint functional capabilities and to support their use by the NCDP. Initial use of this construct will apply to the NCDP for POM 08;

(5) Work with NETWARCOM to refine the process used for enforcement of FORCEnet compliance, and for support to the NCDP, via the FET process;

(6) Work with ASN(RD&A) to ensure processes are in place to review net-centric compliance of programs during Acquisition / Milestone Reviews, including refining methods to utilize the FIBL in these reviews;

(7) Work with ASN(RD&A)CHENG to align and consolidate FORCEnet-related processes, documentation, and databases;

(8) Work with FORCEnet CHENG to develop system / technical guidance that is consistent with the criteria in the FCCC and subsequent updates;

(9) Work with N70, N6/N7 Warfare Sponsors, and N6/N7 Resource Sponsors to incorporate this policy in the NCDP;

(10) Liaison across N6/N7 offices to ensure that all applicable JCIDS documents are reviewed for compliance with this policy prior to submission to N8;

(11) Continue work with cognizant Navy offices, OSD, and the Joint Staff to consolidate checklists, data calls, and databases across the Department of Defense;

(12) Work with ASN(RD&A) to transition this policy to a SECNAV Instruction.

b. N6/N7 Division Directors shall use the FCCC (enclosure (1)) as a guide and work with N71 when reviewing Navy JCIDS documents to ensure that Navy systems are FORCEnet compliant. Directors shall use the FIBL for assessments of compliance to the maximum extent possible. Discussions between N6/N7 Action Officers and individual Program Managers are encouraged to ensure understanding of the information contained in the FIBL;

c. FORCEnet CHENG is requested to update the FIBL / FIT with FCCC criteria, in accordance with FORCEnet EXCOMM planning and ASN(RD&A) direction detailed in reference (h).

9. Cancellation Contingency. This memorandum shall be retained until incorporation into a SECNAV Instruction.

JOSEPH A. SESTAK, JR.
Deputy Chief of Naval Operations
Warfare Requirements and
Programs (N6/N7)

Distribution:
CNO (N7C, N70, N71, N75, N76, N77, N78)

Copy to:
CNO (N1, N2, N3/N5, N4, N8, N091, N098)
DoN CIO
ASN(RD&A)
ASN(RD&A)CHENG
CFFC
CG MCCDC
COMNAVNETWARCOM
COMNAVAIRSYSCOM
COMNAVSEASYSCOM
COMSPAWARSYSCOM
COMNAVWARDEVCOM
Office of Naval Research

# FORCEnet Consolidated Compliance Checklist

(*denotes draft)

| | | Meets | Meets w/ Comment | Does Not Meet | Signature / Date |
|---|---|---|---|---|---|
| FORCEnet Operational Criteria | ❑ FORCEnet Integrated Architecture Operational Views *<br>- *OPNAV POC*: Mr Duncan Macdonald (703) 601-1403 | | | | |
| | ❑ FORCEnet Capabilities<br>- *Ref*: FORCEnet Functional Concept<br>- *OPNAV POC*: Mr Pete Blackledge (703) 601-1429 | | | | |
| | ❑ FORCEnet Capabilities *(cont'd)*<br>- *Ref*: FORCEnet Capabilities List *<br>- *OPNAV POC*: Dr Mike Bell (703) 601-1424 / Mr Edgar Bates (703) 601-1405 | | | | |
| FORCEnet System / Technical Criteria | ❑ FORCEnet Integrated Architecture System And Technical Views (SV, TV) *<br>- *OPNAV POC*: Mr Duncan Macdonald (703) 601-1403 | | | | |
| | ❑ Navy Enterprise Open Architecture (NEOA), conforming to Open Architecture Computing Environment (OACE) Technologies and Standards (T&S) and OACE Design Guide<br>- *Ref*: Open Architecture Technologies & Standards / Design Guidance v1.0<br>- *OPNAV POC*: Mr Duncan Macdonald (703) 601-1403 | | | | |
| | ❑ DoD Information Technology Standards Repository (DISR)<br>- *Ref*: OSDM 22 Dec 04<br>- *OPNAV POC*: Mr Duncan Macdonald (703) 601-1403 | | | | |
| | ❑ Internet Protocol (IP) based with transition to IPv6 planned<br>- *Ref*: OSDM 22 Aug 96<br>- *OPNAV POC*: Mr Duncan Macdonald (703) 601-1403 | | | | |
| | ❑ Global Information Grid (GIG) Mission Area Capabilities<br>- *Ref*: Initial Capabilities Document for Global Information Grid Mission Area, JROCM 202-02 of 22 Nov 02<br>- *OPNAV POC*: Mr Bill Martin (703) 604-7046 | | | | |
| | ❑ Global Information Grid (GIG) Enterprise Services (ES)<br>- *Ref*: Initial Capabilities Document for Global Information Grid Enterprise Services, JROCM 051-04 of 22 Mar 04<br>- *OPNAV POC*: Mr Bill Martin (703) 604-7046 | | | | |
| | ❑ Net-Centric Operations & Warfare Ref Model (NCOW RM)<br>- *Ref*: Net-Centric Operations & Warfare Ref Model v1.0<br>- *OPNAV POC*: Mr Bill Martin (703) 604-7046 | | | | |
| | ❑ Net-Centric Enterprise Services (NCES)<br>- *Ref*: DepSecDef Memorandum, Global Information Grid Enterprise Services (GIG ES): Core Enterprise Services – U18556-03 of 10 Nov 03<br>- *OPNAV POC*: Mr Bill Martin (703) 604-7046 | | | | |
| | ❑ Net-Centric Enterprise Solutions for Interoperability (NESI)<br>- *Ref*: Net-Centric Implementation Framework V 1.0.1 of 04 Feb 05<br>- *OPNAV POC*: Mr Bill Martin (703) 604-7046 | | | | |
| | ❑ Net Ready Key Performance Parameters (NR KPP)<br>- *Ref*: CJCSI 3170.01/6212.01C<br>- *OPNAV POC*: Mr Bill Martin (703) 604-7046 | | | | |

# FORCEnet Consolidated Compliance Checklist

(*denotes draft)

| | | Meets | Meets w/ Comment | Does Not Meet | Signature / Date |
|---|---|---|---|---|---|
| | ❑ ASD(NII) Net-Centric Checklist (NCC)<br>- *Ref*: OASD/NII Net-Centric Checklist (NCC) ver 2.1.3 of 12 May 04<br>- *OPNAV POC*: Mr Bill Martin (703) 604-7046 | | | | |
| | ❑ Transformational Communications Architecture (TCA)<br>- *Ref*: TCA 2.0<br>- *OPNAV POC*: CDR Jim Coffman (703) 601-1223 | | | | |
| | ❑ Joint Tactical Radio System (JTRS) Software Compliant Architecture (SCA)<br>- *Ref*: ASD(C3I) 28 Aug 98, 17 Jun 03<br>- *OPNAV POC*: Mr Joe Trainor (703) 601-1233 | | | | |
| | ❑ Teleports<br>- *Ref*: DoD Teleport Gen 2 ORD, 04 May 05<br>- *OPNAV POC*: Ms. Deb Gowans, (703) 601-1224 | | | | |
| | ❑ Joint Battlemangament Command and Control Roadmap<br>- *Ref*: JBMC2 Roadmap<br>- *OPNAV POC*: LCDR Jody Grady (703) 601-1422 | | | | |
| FORCEnet Policy Criteria | ❑ Human Systems Integration (HSI)<br>- *Ref*: (See Attached Compliance Action List)<br>- *OPNAV POC*: Ms Kathy Dufresne (703) 601-1427 | | | | |
| | ❑ Electromagnetic Environmental Effects (E3) / Spectrum Supportability (SS)<br>- *Ref*: (See Attached Compliance Action List)<br>- *OPNAV POC*: Mr Dave Harris (703) 601-1361 | | | | |
| | ❑ Information Assurance (IA)<br>- *Ref*: (See Attached Compliance Action List)<br>- *OPNAV POC*: CDR Michael Coleman (703) 601- 1456 | | | | |
| | ❑ Data Strategy (DS)<br>- *Ref*: (See Attached Compliance Action List)<br>- *OPNAV POC*: Mr Tim Traverso (703) 855-4956 | | | | |
| | ❑ Geospatial and Time Standards (GTS)<br>- *Ref*: (See Attached Compliance Action List)<br>- *OPNAV POC*: Mr Phil Vinson (703) 601-1484 | | | | |
| FORCEnet Implementation Criteria | ❑ N6/N7 Memorandum, Subj: *FORCEnet Requirements / Capabilities & Compliance Policy*<br>- *OPNAV POC*: Mr Pete Blackledge (703) 601-1429 | | | | |
| | ❑ ASN(RD&A) Memorandum, Subj: *DoN Acquisition Policy for Implementing FORCEnet Capabilities**<br>- *OPNAV POC*: Mr Pete Blackledge (703) 601-1429 | | | | |

*Refer all FORCEnet Consolidated Compliance Checklist comments, inquiries, and requests to:* peter.blackledge@navy.mil.

# FORCEnet Compliance Action List
# - Human Systems Integration (HSI) -

- ❑ DOT_LPF (to include all HSI domains) issues adequately addressed (to included approved and funded where necessary). HSI considered as a factor in meeting the capability gap through non-materiel solutions. ICD contains HSI implications and constraints. (CJCSI 3170.01E, DoDI 5000.2).

- ❑ Roles of operators, maintainers and support personnel in the operational tasks and level of human performance required to meet the military objective defined and included in the architectures and standards. (DoDI 5000.2).

- ❑ HSI included in the source selection of the system/capability. (CJCSI 3170.01E, DoDI 5000.2)

- ❑ System/capability meets the HSI certification criteria of the developing System Command. (NAVSEA, NAVAIR, SPAWAR, MCSC guidance).

- ❑ **Total System Approach**. HSI implemented early in the acquisition process and as part of systems engineering. If necessary, complete a top-down functional analysis, DOTMLPF evaluation (to include allocation of tasks to hardware/software/humans), and metrics to measure and test and redesign the system. Human Factors Engineering (HFE) requirements match system demands to human capabilities. Human performance limits that affect system design and operation, and risks they present, identified. Warfighter/Fleet involved in the program's HSI efforts. HSI efforts integrated into the systems engineering processes. HSI initiatives adequately funded. (DoDD 5000.1 E1.29, DoDI 5000.2 E7.1).

- ❑ **Usability** – Program measures ease of use. Deficiencies adequately addressed. Program verifies optimum performance or identifies where system changes are needed. Program includes appropriate measures of safety, HFE, and survivability along with any Manpower, Personnel, and Training implications. (DoDI 5000.2 E7.2, MIL-STD 1472F)

- ❑ **Human Performance** – Human performance requirements that contribute to total system performance and mission success are identified, and associated metrics developed. Sensory, cognitive and physical requirements of the system/capability are identified and addressed. System/capability enhances Situational Awareness. Objectives relative to individual or group decision-making are met. Plan established to address continuing deficiencies. System capabilities are matched to human processing capabilities. (DoDI 5000.2 E7.3, MIL-STD 1472F)

- ❑ **Maintainability** - System/capability human performance objectives related to maintainability are identified and met. Document/plan specifies maintainability requirements in terms of system analyzability, changeability (to include system redesign if necessary), stability, testability, and portability. (MIL-STD 1472F, MIL-HDBK 470A)

- ❑ **Manpower** – The broad manpower requirements for the minimum (and maximum) number and appropriate mix (military, civilian and contractor) of operators, maintainers and support personnel identified and validated to ensure optimum system performance for the lowest cost. System/ capability reduces workload or manpower. System/capability meets the requirements for manning optimization or for ensuring human performance in a reduced manning environment. Required knowledge, skills and abilities (KSAs), aptitudes and physical characteristics of operators, maintainers and support personnel identified and validated. System/capability matches system requirements to the number of people required (manpower) and the experience/skill-set required for a given classification (personnel) to operate, maintain, and use the system. Manning concept assessed for feasibility and affordability (dollars and manpower). Assessment/gap analysis performed to determine if resources in the current personnel inventory are adequate to meet future needs. Affordability assessments defined in the context of realistic projections of dollars and manpower likely to be available in the future. (OPNAVINST 1500.76, DoDI 5000.2 E7.5).

- ❑ **Ergonomics** - Document/plan defines constraints or limitations on size or layout of system, equipment and/or workspace. Document/plan defines ergonomic requirements for visual displays and their images, keyboards and other I/O devices, workstations, and the operational environment. (MIL-STD 1472F, MIL-HDBK-759C)

- ❑ **Training** - System/capability requires a specific level of training and amount of time required to maintain currency of skills. Training reflects KSAs identified through systems engineering task analysis. Training allocated across all billets. Training support package and logistics (e.g., simulators, training devices, new learning techniques, simulation technology, embedded training) is identified and validated. Requirements for individual, collective and joint training for operators, maintainers and support personnel is identified and validated. Training effectiveness metrics developed. (OPNAVINST 1500.76, CJCSI 3170.01E, DoDI 5000.2)

- ❑ **System Safety and Occupational Health** – System eliminates, reduces and/or mitigates the potential for injury, illness or disability and death of operators, maintainers and support personnel. (DoDI 5000.2, USC 4321, MIL-STD 882D)

- ❑ **Personnel Survivability** – System/capability reduces the risk, prevents and/or increases the odds of surviving fratricide, personal detection or targeting, or confinement within an attacked entity. (DoDI 5000.2 E7.7, DoDD 5000.1).

- ❑ **Habitability** – System/capability provides personnel support services adequate for the number and type of operators, maintainers and support personnel required. (DoDD 5000.2 E7.7)

# FORCEnet Compliance Action List
# -Electromagnetic Environmental Effects (E3)/
# Spectrum Supportability (SS)-

- **Integrated Process Team:** Acquisition or development of a spectrum dependent program/system shall have an established Spectrum Supportability (SS) and Electromagnetic Environmental Effects (E3) Working Level Integrated Process Team (IPT). (OPNAVINST 2450.2)

- **E3 Performance:** Acquisition or development of a spectrum dependent program/system shall have an established E3 performance and verification requirements. (SECNAVINST 5000.2)
- **Electromagnetic Environment:** Acquisition or development of a spectrum dependent program/system shall have defined the intended operating Electromagnetic Environment (EME). (OPNAVINST 2450.2, MIL-STD-464)

- **Test & Evaluation Strategy:** Acquisition or development of a spectrum dependent program/system shall have defined the Test & Evaluation (T&E) strategy for system and platform, that addresses:Electromagnetic Compatibility (EMC)
    - Electromagnetic Vulnerability (EMV)(CJCSI 6212.01)

- **Application for Equipment Frequency Allocation:** Acquisition or development of a spectrum dependent program/system shall have an Approved DD Form 1494 (Application for Equipment Frequency Allocation). Additionally:
    - No spectrum dependent system/program shall proceed into System Development and Demonstration Phase without a Spectrum Supportability determination unless granted by the Milestone Decision Authority (MDA)
    - No spectrum dependent system/program shall proceed into Production and Deployment Phase without a Spectrum Supportability determination unless granted by USD (AT&L) or waiver granted by ASD (NII)
    - No spectrum dependent "off the shelf" or other non-developmental system shall be procured without a Spectrum Supportability Determination.

  (DODD 4650.1, OPNAVINST 2400.20)

- **Spectrum Supportability Determination:** The assessment as to whether the electromagnetic spectrum necessary to support the operation of a spectrum-dependent equipment or system during its expected life cycle is, or will be, available (that is, from system development, through developmental and operational testing, to actual operation in the electromagnetic environment). The assessment of "spectrum supportability" requires, at a *minimum*:
    - Receipt of equipment spectrum certification,
    - Reasonable assurance of the availability of sufficient frequencies for operation from Host Nations, and
    - Consideration of EMC.

  (DODD 4650.1, OPNAVINST 2400.20).

- **Program / System Documentation:** Program/system documentation addresses E3 and SS requirements and compliance criteria. (CJCSI 3170.01, DOD 5000.2, DODD 3222.3, DODD 4650.1, OPNAVINST 2450.2)
- **Hazards of Electromagnetic Radiation to Ordnance:** A Hazards of Electromagnetic Radiation to Ordnance (HERO) Assessment and/or Survey is funded. (CJCSI 3170.01, DODD 3222.3, OPNAVINST 2450.2)

- **Hazards of Electromagnetic Radiation to Personnel and Fuels:** A Hazards of Electromagnetic Radiation to Personnel and Fuels (HERP/HERF) Survey is funded. (CJCSI 3170.01, DODD 3222.3, DODINST 6055.11, OPNAVINST 2450.2)
- **System Electromagnetic Compatibility Certification**: A System Electromagnetic Compatibility (EMC) Certification Survey funded. (CJCSI 3170.01, OPNAVINST 2450.2)
- **Other E3/Spectrum Supportability Analysis:** Other requisite E3/SS Analysis is funded as appropriate to include:
    - Electromagnetic Emission Control (EMCON)
    - Emissions Security (EMSEC) (compromising emanations, formerly called TEMPEST)
    - Electromagnetic Pulse (EMP)
    - Lightning Protection
    - Precipitation Static (P-Static)
    - Electrostatic Discharge (ESD)

  (CJCSI 3170.01, OPNAVINST 2450.2)

- **Commercial Item /Non-Developmental Item Determination:** Determination made regarding feasibility and impact of Commercial Item (CI)/Non-Developmental Item (NDI). (SECNAVINST 5000.2, DODD 4650.1, OPNAVINST 2450.2)
- **Integrated Topside Design Analysis:** Integrated Topside Design analysis funded on all intended platforms. (SECNAVINST 5000.2, OPNAVINST 2450.2)
- **Shore Site E3/Spectrum Supportability:** Shore site E3/SS analysis is funded and performed in support of new equipment/system installations at all shore sites. Shore site E3/SS analysis includes:Ashore Electromagnetic Environmental Effects Analysis and Certification
    - Ashore HERP/HERF/HERO Certification
    - Ashore Spectrum Supportability Analysis and Certification

  (DODINST 6055.11, OPNAVINST 2450.2, OPNAVINST 5100.23)

# FORCEnet Compliance Action List
# - Information Assurance (IA) -

- ❑ IA planning consistent with DoN IA policy. (SECNAVINST 5239.3A)
- ❑ IA strategy on file and approved by the DoN CIO. (Clinger-Cohen Act)
- ❑ Certification and Approving Authorities (e.g. SPAWAR 05, PMW-160, NETWARCOM, SSO-Navy, DIA, CNO, local DDAA, etc.) engaged based on the classification of data processed by the system. (OPNAVINST 5239.1B)
- ❑ POA&M developed for completing the Certification & Accreditation (C&A) tasks associated with applicable DoD Information Technology Security Certification (DITSCAP) and/or DoD Intelligence Information System (DoDIIS) C&A process. (DoDI 5200.40, DoDI 8500.1, DCID 6/3)
- ❑ System Security Authorization Agreement (SSAA) developed in accordance with the applicable C&A guidance. (DoD 8510.1-M. DIA DoDIIS C&A Guide)
- ❑ Ensure IA requirements are addressed and visible in all investment portfolios and investment programs incorporating DoD information systems. (DoDI 8500.2, DCID 6/3)

# FORCEnet Compliance Action List
# - Data Strategy (DS) -

- **System Registration:** System is registered under the correct Functional Area Manager's (FAMs) functional area in the Department of the Navy (DoN) Applications and Data Management System (DADMS). (SECNAVINST 5000.36 (series)) Registration is necessary to establish linkage of system to associated operational activity taxonomy, system functions, applications, networks, databases and to trigger development of data standards and designation of authoritative data source(s) to support system data processing requirements.

- **System Data Documentation:** System metadata and associated documentation including data dictionary, data structure diagrams and data models must be registered in DADMS. (SECNAVINST 5000.36 (series)) Metadata documentation provides system data requirements baseline to be satisfied by designation of authoritative data sources by Functional Data Managers (FDMs), and ensures that data production is in fit and form corresponding to actual system requirements. System data documentation will provide a foundation to create a shared data environment for the Department of Navy.

- **System Data Interface Documentation:** System-to-system and system-to-database interfaces required to transfer system data is registered in DADMS. (SECNAVINST 5000.36 (series)) Data interface registration ensures continuity of data structures among and between systems and databases across data interface boundaries and helps prevent the unintended corruption of data through the process of data transfer. Data interface documentation will be used to provide a baseline for Net-Centricity data interoperability assessment for compliance to functional and enterprise data architecture requirements.

- **Implementation of Data Standards:** New system acquisition and development will ensure usage of existing data standards as recorded in DADMS. (SECNAVINST 5000.36 (series)) Programs will coordinate with the appropriate FDM when modifications to standards and/or new data standards are required. Legacy systems will employ data standards as recorded in DADMS to the extent possible and will attempt to migrate to approved data standards as an adjunct to programmed and/or un-programmed system updates as may occur across the system life-cycle. Adherence to data standards optimizes system performance and promotes systems interoperability.

- **Implementation of XML Standards:** Systems which exchange data via extended markup language (XML) will employ XML standards as outlined in the DoN XML Naming and Design Rules (NDR). (SECNAVINST 5000.36 (series)) Adherence to XML standards optimizes system performance and promotes systems interoperability. Adopting XML standards will facilitate the implementation of standards for interfaces and reduce development cost for interfaces.

- **Authoritative Data Sources:** Systems will use only those instances of data from databases that are designated in DADMS as authoritative data sources for the respective system. (SECNAVINST 5000.36 (series)) Use of authoritative data sources promotes shared understanding of data within the battlespace and reduces system-to-system data conflicts.

- **Program / System Data Documentation:** System documentation specified in this CAL in support of DoN / FORCEnet data management is/are updated consistent with programmed and/or un-programmed updates across the system life-cycle. (SECNAVINST 5000.36 (series)) Data management is an ongoing and dynamic process tied to the life-cycle of each supported system. As each system evolves, data must also evolve in lockstep to remain current and relevant

# FORCEnet Compliance Action List
# - Geospatial and Time Standards -

- Information that refers to a position on the Earth or in Space must indicate that position in terms of the standard geospatial reference frame defined by the World Geodetic System 1984 (WGS-84), as provided by the National Geospatial-Intelligence Agency (NGA).

- Any information that makes reference to time must be able to provide that time in terms of the standard temporal reference defined by Coordinated Universal Time (UTC) as maintained by the U.S. Naval Observatory (USNO) Master Clock, which is the standard for military systems.

- Military operators may make use of a mix of independent, self-contained, and externally referenced positioning, navigation, and timing (PNT) systems --- provided these systems can be traced to the DoD reference standards WGS-84 and UTC (USNO)