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

OPNAVINST 3811.1E
N2/N6
04 Jan 2012

OPNAV INSTRUCTION 3811.1E

From: Chief of Naval Operations

Subj: THREAT SUPPORT TO THE DEFENSE ACQUISITION SYSTEM

Ref: (a) SECNAVINST 5000.2E
(b) DoD Instruction 5000.02 of 8 December 2008
(c) CJCS Instruction 3312.01A
(d) CJCS Instruction 3170.01G
(e) DoD Directive 5000.01 of 12 May 2003
(f) Manual for the Operation of the Joint Capabilities Integration and Development System of Feb 2009
(g) DoD Instruction 5200.39 of 16 July 2008
(h) DoD Instruction 8260.2 of 21 January 2003
(i) OPNAVINST 3880.6A
(j) DoD Directive 5250.01 of 31 January 2008
(k) DoD Instruction 5000.61 of 9 December 2009
(l) SECNAVINST 5200.40
(m) SECNAVINST 5200.38A
(n) CJCS Instruction 8510.01A
(o) DoD Directive 5000.59 of 8 August 2007
(p) OPNAVINST 5200.34

1. Purpose. To issue mandatory procedures for Department of the Navy (DON) implementation of references (a) through (p) for intelligence threat support to DON and DON-led Joint Defense Acquisition System efforts.

2. Cancellation. OPNAVINST 3811.1D.

3. Background. Intelligence is key to understanding the potential current and future threat posed by foreign weapon and Information Technology (IT) system capabilities, and must be integral to U.S. system development and acquisition decisions. The provision of threat support to system selection and planning is vital to ensure the Navy and Joint forces remain capable of carrying out assigned missions.

For systems to achieve their intended capabilities, consideration of the threat must be continual throughout the life-cycle of each system. Threat considerations are inherent in all decisions from defining requirements and capabilities, through initial concept phases, planning, research, full-scale development, production, test and evaluation, deployment, and system upgrade. In concert with documentation and procedural requirements of references (a) through (h), a close relationship between the intelligence and system development communities is critical to ensure consideration of the threat throughout the system selection and planning process.

4. Applicability and Precedence. Per reference (a), this instruction applies to all DON organizations and to all DON Acquisition Category (ACAT) programs, including: Naval Intelligence and cryptologic ACAT programs; IT programs; and rapid deployment capability programs, as well as non-ACAT science and technology and engineering programs and studies. References (a) through (g) and this instruction take precedence over any issuances conflicting with them, except for policy, direction, or guidance embodied in current statute, regulation, the Defense Federal Acquisition Regulation Supplement, and the Navy-Marine Corps Acquisition Regulation Supplement.

5. Policy

a. Early consideration must be given to threat information in all system planning initiatives; Research, Development, Test and Evaluation (RDT&E); and acquisition activities. Navy requirements officers and project officials will ensure the capabilities of systems are specified sufficiently to counter and or defeat projected foreign threats. Program Managers (PM) are directed to work through their Scientific and Technical Intelligence Liaison Officer(s) (STILO), or in the absence of a STILO, the office of the Deputy Director of Naval Intelligence (OPNAV N2/N6I), to acquire, use and remain cognizant of changes to the threat which could have cost, schedule, performance, or operational impact on their systems or programs.

b. For all system development and acquisition programs, specific planning will be included for obtaining, updating and using threat support throughout the life-cycle of the program.

c. Reference (a) specifies that the only threat data and threat assessments authorized to support Navy system development and acquisition programs are those validated by or through OPNAV N2/N6I. Neither PMs nor their designated contractors shall develop or produce threat assessments. No threat support information will be used in acquisition documents, studies, or analysis that has not been specifically validated by or through OPNAV N2/N6I.

d. Office of Naval Intelligence (ONI) produced Capstone System Threat Assessment Report (CSTAR), System Threat Assessment Report (STAR) or system threat documentation supporting all Navy ACAT programs and non-acquisition science and technology and engineering programs and studies.

(1) ACAT ID programs requiring intelligence support will also be validated by the Defense Intelligence Agency (DIA).

(2) Non-ACAT ID programs that are designated by the Office of the Secretary of Defense test and evaluation oversight list requiring a STAR, or programs requiring system specific threat information, will be validated by or through OPNAV N2/N6I.

6. Responsibilities

a. DON Intelligence Component Commands

(1) In his or her role as the Director of Naval Intelligence, the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) is responsible to the Chief of Naval Operations (CNO) for managing and resourcing all aspects of intelligence throughout the Navy and has the responsibility for implementing procedures contained in reference (a) and this instruction.

(a) OPNAV N2/N6 Warfare Integration Directorate's Deputy for Program Integration (OPNAV N2/N6FP) is responsible for coordinating and ensuring intelligence certification of the acquisition program's Information Support Plan (ISP) is complete prior to submission to non-Navy entities (Intelligence Requirements Certification Office, Joint Staff, DIA, etc.)

(b) OPNAV N2/N6I is responsible for validating threat priorities for Navy research, development, and acquisition programs for the Office of the Chief of Naval Operations (OPNAV) components.

(2) Commander, ONI is responsible for life-cycle threat production and supporting validated and prioritized intelligence threat and intelligence collection requirements as directed by reference (a). ONI is responsible for the development of threat support material and provision of those products and information. This responsibility includes:

(a) Providing or facilitating the provision of current and future, non-U.S., intelligence and threat forecast products, data, and force information, supporting references (a) through (h).

(b) Producing threat data, CSTAR, STAR, or system threat assessments (STA) to support specific development and acquisition programs. The threat assessments provide the basic threat documentation for all Navy or Navy-lead Joint programs (this includes support to Marine Corps aviation as required by reference (a)). ONI will update program threat assessments biennially (every 24 months).

(c) Producing and identifying the appropriate STAR or STA product(s) to support Navy or Navy-led Joint programs that fall within Defense Acquisition Board (DAB) or Joint Requirements Oversight Council (JROC) review authority, as required by references (a) through (d).

b. DON Acquisition Component Commands. Systems Commands (SYSCOM), program executive officers, PMs, product directors, technology directors or initiative leads, and Research and Development (R&D) activities shall ensure the threat assessment and threat data used for developmental test and evaluation and support to live fire test and evaluation of a program is the correct and current assessment and data. Acquisition and R&D activities shall coordinate and maintain dialogue with OPNAV N2/N6I (as appropriate) to establish the proper intelligence support for each program. Specifically, PMs or project leads shall:

(1) Coordinate program intelligence support requirements through the STILO Program within reference (i).

(2) Work with OPNAV N2/N6FP to conduct, document and populate the multiple intelligence, surveillance, and reconnaissance supportability and sustainability analyses identified in references (a) through (e) and (g), and this instruction. The PM and OPNAV N2/N6FP shall jointly determine the intelligence content, and include intelligence costs within life-cycle program costs. Intelligence costs must include intelligence infrastructure analysis, creation of intelligence content of the ISP, and support for operations and sustainment of an ISP.

(3) In conjunction with OPNAV N2/N6I, ensure the threat capabilities information in the Test and Evaluation Master Plan (TEMP) is prepared using the current CSTAR, STAR, and or STA, if it exists, and other approved threat information in support of fulfilling reference (a) requirements.

c. Navy Operational Test and Evaluation (OT&E) Commands. Director, Test and Evaluation and Technology Requirements, and Commander, Operational Test and Evaluation Force (COMOPTEVFOR) shall ensure the threat assessment and threat data used for OT&E of a program is the correct and current assessment of data as directed by references (a), (b) and (j) through (l). Necessary time and resources shall be planned and budgeted to ensure adequate testing is conducted to support decision makers and the users throughout the life-cycle of the acquisition program.

d. DON Requirements Sponsors. Per references (b) through (f) and (h), Joint Capabilities Integration and Development System (JCIDS) analyses and documents must consider future adversarial threat capabilities and scientific and technical developments. OPNAV and other Navy commands acting as requirements sponsors shall ensure JCIDS products utilize the most current and applicable threat assessment. The "Threat and Operational Environment" section of the Initial Capabilities Document (ICD), the Capability Development Document (CDD) and the capability production document (CPD) will be per references (c), (d) and (f).

7. Intelligence Threat Support to Navy Requirements, Acquisition and RDT&E Communities

a. ONI. Per the responsibilities articulated in paragraph 6a(2), ONI shall:

(1) Review all Navy ICDs, CDDs and CPDs (and Joint ICDs, CDDs and CPDs which involve the Navy) for the OPNAV N2/N6 during the JCIDS document staffing process to ensure threat information meets Department of Defense (DoD) and Chairman, Joint Chiefs of Staff requirements.

(2) Review and approve the threat-related sections of the TEMP. Evaluate the requirements for threat representations with available and projected assets and their capabilities and highlight major shortfalls in the ability to provide adequate characterization or accurate representation of specific threats listed in the CSTAR, STAR, or STA (or other DIA-, and Navy-approved products) within the test environment.

(3) Review all documents and studies for OPNAV N2/N6 prior to milestone reviews, ensuring the threat information meets DoD and Navy standards.

(4) Undertake the development, production, verification and validation of models and simulations of foreign threat weapon systems and tactics. ONI serves as the final DoD and Navy validation authority for Model and Simulation (M&S) representations of threats to U.S. Naval Forces. In this context, 'M&S representations' refers to all threat data and models, both as static logical-mathematical depictions and as those performed dynamically in simulation execution and interaction with other M&S representations.

(5) Have a representative on test and evaluation master plan working group (TPWG) as the intelligence representative.

b. Working Groups. Capabilities Based Assessments (CBA), Analyses of Alternatives (AoA), TPWG, working integrated product team, and overarching integrated product team will be supported by an ONI representative to the appropriate oversight board or study team. ONI threat validated by OPNAV N2/N6I will be provided for all Navy studies. OPNAV N2/N6I or ONI will obtain DIA validation of threat material supporting DAB- or JROC-level programs, as required by references (b) through (d).

(1) When requested or required, OPNAV N2/N6I or ONI will assist the PMs in obtaining DIA approval of defense planning scenario (DPS) and Multi Service Force Deployment (MSFD) threat scenarios and other threat data in the CBA or AoA to ensure that:

(a) All scenarios and threats are validated and reference materials meet DoD and Navy requirements.

(b) Baseline scenarios used in the CBA or AoA will be per references (d), (f), and (h), and should be based on the Quadrennial Defense Review, Strategic Planning Guidance (SPG) and DPS. The CBA may consider excursions from the SPG DPS when they would contribute to the analysis. To the greatest extent possible, the CBA will use DPS and/or MSFD scenario products to support scenario needs. In cases where no appropriate MSFD scenarios exist, the CBA study team must work closely with OPNAV N2/N6I or ONI to develop other scenarios or excursions to meet analytical needs.

(c) When requested or required, OPNAV N2/N6I or ONI will formally review and evaluate the threat and scenario portions of non-Navy-led and Navy-interest CBAs.

(2) Program offices or SYSCOMs may formally request a Threat Integrated Product Team (TIPT). ONI may assemble a dedicated TIPT to meet this request. If formed, the TIPT determines the nature and level of documentation and other required activities to ensure consistent, efficient cradle-to-grave threat support. ONI normally chairs the TIPT.

(3) TWGs are working-level integrated product teams, with similar membership as that of TIPTs, that are held as required to discuss threat issues and ensure consistent threat support to acquisition programs throughout their lifecycle.

c. CSTAR, STAR and STA. Commander, ONI produces CSTARs,

STARs, or STAs for Navy ACAT programs. CSTAR, STAR, or STA supplements follow the same review, and approval procedures as CSTAR, STAR, or STA.

d. Threat Models and Capabilities. All threat models and capabilities assessments must be maintained in a current and approved or validated status throughout the acquisition process. ONI shall serve as the authoritative DoD and Navy source for data and assessments concerning foreign maritime forces (organizations, units, entities, systems, processes and behaviors).

e. Liaison. Liaison between the requesting organization and OPNAV N2/N6I and ONI, via the organization's STILO is required until satisfaction of the requirement. This dialogue is particularly useful when intelligence collection action is initiated to fill information gaps or when alternative means of satisfaction, e.g. modeling or simulation, must be employed. The requestor should submit changes, additions or deletions to previously submitted requirements as soon as they become known.

f. Waiver to Mandated Threat Support Requirement. Determination that threat support is not required for a weapon development program is the responsibility of the OPNAV requirements sponsor in coordination with the program office, OPNAV N2/N6I, and ONI (as appropriate), and, in the case of ACAT ID programs, DIA. If the threat is determined not to be a factor, a statement to that effect will be included in appropriate program documentation, with a copy forwarded to COMOPTEVFOR.

8. Action

a. Activities shall ensure that the policies, procedures, documentation, and reports as required by this instruction and the references thereof are followed.

b. Activities shall review existing guidance and instructions and cancel or update to conform to this instruction and the references thereof are followed.

c. Activities shall distribute this instruction to appropriate command personnel.

9. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of November 2007.

Kendall L. Card

KENDALL L. CARD
Vice Admiral, U.S. Navy
Deputy Chief of Naval Operations,
Information Dominance

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