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

OPNAVINST 3960.15B
N94
27 Jul 2017

OPNAV INSTRUCTION 3960.15B

From: Chief of Naval Operations

Subj: VALIDATION OF NAVY THREAT SIMULATORS, TARGETS AND DIGITAL THREAT MODELS AND SIMULATIONS

Ref: (a) DoD Instruction 5000.02 of 7 January 2015
(b) DoD Instruction 5000.61 of 9 December 2009
(c) SECNAVINST 5200.40
(d) OPNAVINST 3811.1F
(e) DoD Threat Systems Program Plan
(f) MIL-STD-3022

1. Purpose. To establish policies, procedures and assign responsibilities for validation of Navy threat representations utilized in the test and evaluation (T&E) of Navy acquisition programs. This revision updates references and clarifies integrated product team membership and authorized sources of threat information. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 3960.15A.

3. Background. An acquisition program's milestones and acquisition decisions are frequently based on the results of testing developmental hardware against various forms of threat representations since the actual threat may be unavailable for T&E. Reference (a) requires threat representations used in operational test to undergo verification by the developer, validation by the Department of Defense (DoD) component, and accreditation by the operational test agency. References (b) and (c) establish policy and procedures and assign responsibilities for verification, validation, and accreditation of modeling and simulation (M&S) within the DoD and Navy respectively. Digital threat M&S policy, procedures, and responsibilities are specified in reference (d).

4. Scope and Applicability. This instruction is applicable to all Navy facilities, acquisition programs, and service providers associated with the procurement and use of threat representations for T&E.

5. Actions

a. Per reference (a), all threat representations, developed for use in operational testing of Navy acquisition programs should be validated using the procedures and format specified in references (e) and (f). Digital threat M&S must be validated per references (c), (d) and (f).

Threat representations that have not undergone validation during their development and initial operational capability (IOC) cycle are not exempt and must be validated if the systems are to be used to support T&E.

b. Training threat representations have historically not required validation for use in fleet training. However, training targets, if intended to be utilized in T&E, must follow the validation process defined in this instruction and reference (e).

c. Threat representations developed for operational test should be validated in conjunction with the threat representation’s IOC and should be re-visited throughout the life cycle to evaluate whether validation updates are required. For example, new intelligence may result in a revised assessment of the threat or a need to modify the representation to account for new threat capabilities. As such, an amendment to the original validation report or a new validation may be required to account for the revised intelligence estimate or modifications made to the threat representation. The IOC validation will be conducted at the completion of the acceptance testing of the representation in its final configuration based on measured data from verification or acceptance testing. The IOC validation report serves as the foundation for the accreditation decision. Validation reports issued in conjunction with IOC or following modifications to the threat representation will be funded by the developing program office.

d. When targets developed for training, are to be utilized in T&E, or when a new use or revised intelligence assessment is issued for an existing, validated threat representation, the program office, for the system under test, will be responsible for initiating and funding the validation of the representation against the specified threat if no previous formal validation has occurred or if an amendment or revision to the original validation report is required. This will require the production of validation documentation as described in reference (e) and (f). The scope of the validation effort should match the intended use.

e. For threat representations, an entity, independent of the developing agency; that possesses a thorough understanding of references (a) through (f), will manage the validation effort and serve as the validation Integrated Product Team (IPT) lead responsible for developing the validation report and coordinating data measurement efforts.

(1) A validation IPT should be established and comprised of an IPT lead and subject matter experts from the developing entity, appropriate warfare centers, the intelligence and T&E communities, the resource sponsor and the Test and Evaluation Threat Resource Activity (TETRA). The validation IPT should implement the procedures contained in references (e) and (f) to prepare and submit validation reports for review and approval.

(2) All efforts should be made to establish the validation IPT early in the threat representation’s development to ensure a complete and coordinated validation plan is prepared early in the development process. This will facilitate proper resourcing and data collection as

early as possible, minimize duplication of effort and increase the efficiency of developmental and acceptance testing. If planned far enough in advance and performed with the required objectivity, much of the data collected may be utilized for validation purposes.

(3) The Validation IPT will ensure the report documents, the parametric, characteristic, and performance differences between the threat representation and the current Defense Intelligence Agency, Office of Naval Intelligence, or other appropriate intelligence agency approved threat data; and explains the potential impacts of these differences during T&E.

f. Per reference (d), the only threat data and assessments authorized to support Navy systems development and acquisition programs are those validated by or through the Office of the Chief of Naval Operations, Deputy Director of Naval Intelligence (OPNAV N2N6I). Analysts from the Office of Naval Intelligence, or another appropriate intelligence agency, will participate as an IPT member in the development and review of validation reports to ensure the validity and accuracy of threat descriptions, threat data and associated capabilities emulated by the threat representation.

g. Validation reports will be reviewed and approved by the IPT lead, developing agency, appropriate intelligence agency, resource sponsor and TETRA. TETRA approval signifies independent oversight of the process and that the intelligence data was accurate, current, and derived from authorized sources. Upon approval, the validation report will be distributed to the test community and forwarded to TETRA for retention and inclusion in the DoD’s online Threat Systems Database. Unclassified verification, validation, and accreditation documents and unclassified metadata associated with classified validation documents will be submitted to the Navy Modeling and Simulation Office per reference (c).

h. The validation report does not constitute authorization to use the threat representation during developmental, operational, or live fire T&E. Accreditation for developmental, operational, and live fire testing will be conducted per local instructions and certify the threat representation for the intended use(s). Commander, Operational Test and Evaluation Force will review Navy validation reports for the purpose of accrediting threat representations for use in operational T&E.

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

7. Review and Effective Date. Per OPNAVINST 5215.17A, Director, Innovation, Technology Requirements and Test and Evaluation (OPNAV N94) will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5 year anniversary date, or an extension has been granted.

8. Reports Control. Reporting requirement contained within this instruction are exempt from reports control per SECNAV M-5214.1, part IV, subparagraph 7n.

DAVID J. HAHN
Director, Innovation, Technology Requirements
and Test and Evaluation

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, http://doni.documentservices.dla.mil/