

Army Regulation 381–11

Military Intelligence

Intelligence Support to Capability Development

**Headquarters
Department of the Army
Washington, DC
30 January 2019**

UNCLASSIFIED

SUMMARY of CHANGE

AR 381-11

Intelligence Support to Capability Development

This mandated revision, dated 30 January 2019—

- o Adds records management requirements in accordance with DA Pam 25-40 (para 1-5).
- o Aligns production of the Validated Online Lifecycle Threat with key decision points and clarifying waiver authorities in accordance with DODI 5000.02 (paras 1-6, 2-9, 2-10, 4-1, and 4-2).
- o Revises modeling and simulation terminology in accordance with AR 5-11 (paras 1-6, 2-9, 3-14, and glossary).
- o Changes the name of the Test and Evaluation Management Agency to Deputy Under Secretary of the Army, Test and Evaluation (para 2-2).
- o Identifies the requirement for a life cycle mission data plan in accordance with DODI 5000.02 (para 2-13g).
- o Revises responsibilities of the National Ground Intelligence Center in accordance with the Defense Intelligence Analysis Program (para 2-14).
- o Changes Capstone Threat Assessment to the Defense Intelligence Threat Library in accordance with DODI 5000.02 (paras 2-14a, 3-7, and glossary).
- o Changes use of Defense Planning Scenarios to the more encompassing Support for Strategic Analysis products (paras 3-8, 3-14, 3-15, and glossary).
- o Deletes the requirement for the initial threat warning assessment in accordance with DODI 5000.02 (formerly para 3-9).
- o Changes the System Threat Assessment Report to the Validated Online Lifecycle Threat and establishes a new format in accordance with Defense Intelligence Agency instruction 5000.02 (para 4-1).
- o Updates the list of required and related publications (app A).
- o Changes the definition of critical program information to align it with the current definition in DODI 5200.39 (glossary).
- o Changes the System Threat Assessment Report to the Validated Online Lifecycle Threat report in accordance with DODI 5000.02 (throughout).
- o Makes mandated changes to conform to Department of Defense policy and to reflect changes in Army organization prescribed by General Order 2017-01 and AR 10-87 (throughout).

Military Intelligence
Intelligence Support to Capability Development

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:


KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a mandated revision.

Summary. This regulation on intelligence support to capability development, using guidance from DODD 5000.01, DODI 5000.02, Chairman of the Joint Chiefs of Staff manual 3170.01, and Defense Intelligence Agency instruction 5000.002 provides policies, responsibilities, and procedures to ensure that threat considerations are incorporated into the Defense acquisition process and the Joint Capabilities Integration and Development System where the Army is the lead or supporting agency. It contains procedures for requesting intelligence threat support for various applications in the Army to include:

analyses, automated information systems, life cycle management, technology, studies, simulations, simulators, computer models, battle labs, combat and materiel development, training development, technology insertion, and rapid fielding.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to Department of the Army/Defense contractor personnel conducting research, development, or acquisition of materiel items or those conducting analysis using the full range of doctrine, organization, training, materiel, leadership and education, personnel, and facilities.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G-2. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and

must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25-30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11-2 and identifies key internal controls that must be evaluated (see app C).

Supplementation. Supplementation of this regulation and establishment of agency, command, and installation forms are prohibited without prior approval from the Deputy Chief of Staff, G-2 (DAMI-FIT), 1000 Army Pentagon, Washington, DC 20310-1000.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G-2 (DAMI-FIT), 1000 Army Pentagon, Washington, DC 20310-1000.

Distribution. This publication is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Responsibilities • 1-4, page 1

Records management requirements • 1-5, page 1

Policy • 1-6, page 1

Chapter 2

Responsibilities, page 3

*This regulation supersedes AR 381-11, dated 26 January 2007.

Contents—Continued

Section I

Headquarters, Department of the Army, page 3

Assistant Secretary of the Army (Acquisition, Logistics, and Technology) • 2–1, *page 3*

Deputy Under Secretary of the Army • 2–2, *page 3*

Chief Information Officer/G–6 • 2–3, *page 3*

Deputy Chief of Staff, G–2 • 2–4, *page 3*

Deputy Chief of Staff, G–3/5/7 • 2–5, *page 4*

Deputy Chief of Staff, G–8 • 2–6, *page 4*

Other Army Staff elements • 2–7, *page 4*

Section II

Army Commands, Army Service Component Commands, and Direct Reporting Units, page 4

Commanders, Army commands, Army service component commands, and direct reporting units • 2–8, *page 4*

Commanding General, U.S. Army Training and Doctrine Command • 2–9, *page 5*

Commanding General, U.S. Army Materiel Command • 2–10, *page 5*

Commanding General, U.S. Army Space and Missile Defense Command/U.S. Army Strategic Command • 2–11, *page 6*

Commanding General, U.S. Army Test and Evaluation Command • 2–12, *page 6*

Section III

Other Army Elements, page 7

Program executive officers, program/project managers, and U.S. Army Training and Doctrine Command capability managers • 2–13, *page 7*

Commander, National Ground Intelligence Center • 2–14, *page 7*

Program Executive Officer for Simulation, Training, and Instrumentation • 2–15, *page 8*

Director, U.S. Army Materiel Systems Analysis Activity • 2–16, *page 9*

Chapter 3

Intelligence Threat Support, page 9

Section I

General, page 9

Purpose • 3–1, *page 9*

Guidance for threat preparation • 3–2, *page 9*

Section II

Intelligence Threat Support Structure, page 9

Threat integration staff officer and threat analyst • 3–3, *page 9*

U.S. Army Training and Doctrine Command Deputy Chief of Staff, G–2 • 3–4, *page 10*

U.S. Army Materiel Command, G–2 and U.S. Army Space and Missile Defense Command/U.S. Army Strategic Command intelligence officers • 3–5, *page 10*

Section III

Intelligence Threat Baseline, page 11

Intelligence threat baseline products • 3–6, *page 11*

Defense Intelligence Threat Library • 3–7, *page 11*

Strategic support analyses, joint country force assessments, and U.S. Army Training and Doctrine Command standard scenarios • 3–8, *page 11*

Section IV

Intelligence Threat Support Process, page 12

Threat steering group • 3–9, *page 12*

Threat accreditation working group • 3–10, *page 12*

Army threat representation validation working group • 3–11, *page 13*

Other intelligence support to test and evaluation • 3–12, *page 13*

Intelligence support to Army modeling and simulation • 3–13, *page 13*

Intelligence support to Army scenario development • 3–14, *page 14*

Intelligence support to Army studies and analysis • 3–15, *page 15*

Contents—Continued

Intelligence support to program protection • 3–16, *page 16*

Intelligence support to contractors • 3–17, *page 16*

Chapter 4

Intelligence Threat Support Products, *page 17*

Validated Online Life-cycle Threat Report • 4–1, *page 17*

Test and evaluation master plan • 4–2, *page 18*

Threat test support package • 4–3, *page 18*

Program protection plan • 4–4, *page 19*

Appendixes

A. References, *page 20*

B. Threat Test Support Package Formats, *page 23*

C. Internal Control Evaluation, *page 24*

Glossary

Chapter 1 Introduction

1–1. Purpose

This regulation prescribes Army policy and procedures and assigns responsibilities for—

- a. Integrating intelligence support into the capability development process.
- b. Providing multidisciplined intelligence (MDI) support to—
 - (1) The doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) capability development process.
 - (2) Responsibilities and procedures for intelligence support to—
 - (a) Research and development to include rapid fielding initiatives and international agreement programs.
 - (b) Modeling and simulation (M&S).
 - (c) Threat representation development for test and evaluation (T&E) events.
 - (d) Nondevelopmental item.
 - (e) Commercial off-the-shelf.
 - (f) Technology-based programs to include the advanced technology demonstration (ATD), advanced concept technology demonstration (ACTD), Army technology objective (ATO), cooperative research and development agreements, small business independent research, cooperative technology agreements, and horizontal technology integration efforts.
 - (g) Risk management in support of information technology (IT) security certification and accreditation (see AR 25–2).
- c. Ensuring that MDI support guides the Army’s warfighting capability development process through the 21st century.

1–2. References

See appendix A.

1–3. Explanation of abbreviations and terms

See the glossary.

1–4. Responsibilities

Responsibilities are listed in chapter 2.

1–5. Records management requirements

The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in the Army Records Information Management System (ARIMS)/RRS–A at <https://www.arims.army.mil>. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

1–6. Policy

a. *Intelligence*. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Intelligence information applied to capability development is referred to as “threat.” Quality intelligence is—

- (1) Timely, providing intelligence products to the combat and materiel developers in an expeditious manner and continually look for ways to streamline the validation and accreditation process.
- (2) Tailored, focusing on intelligence products on the needs of the combat and materiel developers and reduce extraneous information.
- (3) Digestible. Intelligence products must be easily read and understood. Formats must convey the main points clearly and ensure that the message is easily understood.
- (4) Clear regarding the known and unknown. Intelligence provides what is known, what is unknown, and the analysis that fills the gaps. Clearly identify the degree of confidence in assessments and facilitate the update of critical information requirements.

b. *Intelligence threat support*. Intelligence threat support consists of consideration and evaluation of intelligence information in order to conduct a threat assessment of an enemy or potential enemy’s current or projected capability to limit, neutralize, or destroy the effectiveness of any aspect of DOTMLPF. Threat support is a continuous process beginning with

concept development or rapid fielding and continuing through DOTMLPF life cycles in a collaborative environment and reassessed between multidisciplinary proponents.

c. Incorporating intelligence.

(1) Army customers will incorporate MDI in support of the capability development process in accordance with security restrictions specified in AR 70–1, AR 380–5, AR 380–381, and AR 381–10.

(2) Commanders will obtain intelligence from organic and supporting organizations to the maximum extent possible before requesting dissemination or production of intelligence products in accordance with this regulation.

(3) Requests for dissemination and submission of production requirements (PRs) will be expedited through command channels.

d. Intelligence integration into capability development.

(1) Intelligence threat support consists of consideration and evaluation of intelligence information in order to assess an enemy's or potential enemy's current or projected capability to limit, neutralize, or destroy the effectiveness of any aspect of DOTMLPF. Intelligence threat support is a continuous process that includes research and development, concept development, or rapid fielding and continuing through DOTMLPF life cycles in a collaborative environment with reassessment among multidisciplinary proponents.

(2) DODD 5000.01 states that intelligence and understanding threat capabilities are integral to system development and directs the program/project manager (PM) to keep threat capabilities integrated into program documents throughout the acquisition process.

(3) DODI 5000.02 outlines the statutory and regulatory information requirements of which the Validated Online Life-cycle Threat (VOLT) report, life cycle mission data plan (LMDP), and program protection plan (PPP) are regulatory information requirements in support of specific acquisition milestones. The instruction outlines various acquisition documents.

(4) Defense Intelligence Agency directive 5000.200 and Defense Intelligence Agency instruction (DIAI) 5000.002 contain guidance on threat support to major defense acquisition programs. DIAI 5000.002 outlines the standard VOLT format.

(5) CJCSI 3170.01I and the Joint Capability Integration and Development System (JCIDS) Manual outline the process to produce capability proposals that consider the full range of DOTMLPF and where to incorporate threat information in capabilities documents.

(6) DODI 8260.2 prescribes the analytic baseline for strategic analysis. It implements policy, assigns responsibilities, and prescribes procedures for generating, collecting, developing, maintaining, and disseminating data on current and future U.S. and non-U.S. forces in support of strategic analyses conducted by the DOD.

(7) Policies for threat support to capability development as they pertain to the Army are listed below:

(a) Intelligence and threat are command responsibilities. Army commanders, combat developers (to include Training and Doctrine Command capability managers (TCMs)), materiel developers (to include program executive officers (PEOs) and PMs), designated accreditation authorities or capability developers (to include the six M&S-enabled communities: acquisition, analysis, experimentation, intelligence, test and evaluation, and training), study directors, and Research Development and Engineering Centers (RDECs) and research laboratories at all levels will ensure that MDI is applied, integrated, funded, and properly staffed in the capability development process and the IT security certification and accreditation process.

(b) MDI, which includes scientific and technical intelligence characteristics, capabilities and limitations of foreign equipment, and general military intelligence (GMI) (organization, doctrine, force structure, and tactics of threat forces), will primarily be derived from data sources with production responsibility as outlined in the Defense Intelligence Analysis Program (DIAP). If other sources are used, such as unclassified open source publications or electronic online resources, their use will be noted in the program or system-specific threat bibliography. Analysis of MDI data to meet threat requirements is the responsibility of the supporting intelligence element.

(c) Combat and materiel development commands or activities and system development organizations will integrate required intelligence documentation. This includes threat assessments to support specific combat, materiel, automated information systems, and training development activities for which those commands are responsible.

(8) Members of the intelligence production community will provide intelligence support in response to PRs as specified under the DIAP.

(9) The threat support activity of each command and activity involved in the force, combat, and materiel development process will participate in a collaborative process to develop, review, and approve threat assessments written in support of command missions.

Chapter 2 Responsibilities

Section I

Headquarters, Department of the Army

2-1. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

The ASA (ALT) will—

- a.* Obtain and fund MDI support for research, development, and acquisition (RDA) requirements, including special task forces (STFs), special study groups (SSGs), study advisory groups (SAGs), study directives, analyses, technology efforts and direction and guidance documents for which the ASA (ALT) is responsible from earliest concept stages.
- b.* Request threat statements for Modified Integrated Program Summaries and in-process reviews for acquisition category (ACAT) I and II systems from the Deputy Chief of Staff (DCS), G-2 and ensure that the summaries prepared to support milestone decision reviews (MDRs) for ACAT I and II systems contain or reference Headquarters, Department of the Army (HQDA)-approved threat assessments or have received a waiver from the designated milestone decision authority (MDA) to the effect that there is no system-specific threat to the program.
- c.* Ensure that intelligence assets are programmed to support long-range planning initiatives and that plans reflect consideration of the threat.
- d.* Ensure threat information contained in program documents being submitted for Defense Acquisition Board (DAB) review have been reviewed by DCS, G-2.
- e.* Identify and submit command threat support requirements and request intelligence reports through DCS, G-2.
- f.* Obtain MDI support and guidance to technology base programs, to include ATD, ACTD, and international agreement programs. Ensure integration of approved MDI to support a developmental test (DT).
- g.* Provide coordination and approval for end user certificates as required for open commercial purchases of foreign manufactured military materiel desired by program managers in support of RDA.

2-2. Deputy Under Secretary of the Army

The DUSA will—

- a.* Monitor and advise the Secretary of the Army on Army test and evaluation efforts and policy to ensure that both are adequate and fully coordinated with the Office of the Secretary of Defense (OSD).
- b.* The Deputy Under Secretary of the Army (Test and Evaluation) (DUSA (TE)) will—
 - (1) Establish Army validation and accreditation policy for threat representations.
 - (2) Charter and chair validation working groups (VWGs) for threat representations.
 - (3) Coordinate with DCS, G-2 on requirements for MDI support to threat targets (excluding range targets), simulators, and simulations that fall under the auspices of the Threat System Working Group Program, STFs, and other guidance documents.
 - (4) Ensure that Army threat representations are validated and accredited in accordance with AR 73-1 and DA Pam 73-1.

2-3. Chief Information Officer/G-6

The Chief Information Officer/G-6 will—

- a.* Coordinate with DCS, G-2 on methodologies to include MDI support to emerging information systems and networks developed under the aegis of the PEO, Enterprise Information Systems.
- b.* Coordinate with DCS, G-2 to develop methodologies to provide MDI support to procurement of information systems that fall below DODD 5000.01 thresholds and technology insertions that are not considered procurements.

2-4. Deputy Chief of Staff, G-2

- a.* DCS, G-2 has Department of the Army (DA) and Army Staff (ARSTAF) responsibility for determining intelligence priorities, managing intelligence production by the National Ground Intelligence Center (NGIC) and the Army Counterintelligence Center (ACIC), and establishing MDI and program protection support policy, guidance, and funding for the Army. DCS, G-2 exercises this responsibility through the Foreign Intelligence Directorate (DAMI-FI), Counterintelligence (CI)/Human Intelligence Directorate (DAMI-CD), and the U.S. Army Intelligence and Security Command (INSCOM).
- b.* DCS, G-2 will—
 - (1) Serve on the Army Systems Acquisition Review Council (ASARC).

- (2) Serve on the Army Requirements Oversight Council (AROC).
 - (3) Serve as the ARSTAF proponent for intelligence and threat M&S efforts.
 - (4) Designate appropriate representatives to serve on STFs, SSGs, SAGs, general officer steering committees, and other intelligence efforts.
 - (5) Manage the Army intelligence support to capability development process.
 - (6) Convene study groups, working groups, threat steering groups (TSGs), and so on as required to develop and review M&S and ensure that intelligence data on threat doctrine, projections, developments, issues, and force employment used in these products are logical and consistent.
 - (7) Convene and chair quarterly meetings of the Army Technology Protection Working Group (ATWG). The ATWG will consist of representatives from INSCOM, ASA (ALT), U.S. Army Materiel Command (AMC), and the U.S. Army Space and Missile Defense Command (SMDC). The mission of the ATWG will be to ensure intelligence sharing and coordinate ongoing intelligence support to ASA (ALT) and AMC program and technology priorities.
 - (8) Integrate and synchronize security, intelligence, counterintelligence, foreign disclosure, and security countermeasures support to research and technology protection activities Armywide.
 - (9) Assign threat integration staff officers (TISOs) and threat analysts (TAs) to support capabilities development.
- c. The Commanding General (CG), INSCOM will—
- (1) Refer to AR 10–87 for the roles and responsibilities of INSCOM.
 - (2) Manage the Army dissemination and information sharing program in accordance with DOD and intelligence community directives.
 - (3) Provide training to Army organizations on processes for obtaining and disseminating intelligence products as required.

2–5. Deputy Chief of Staff, G–3/5/7

a. DCS, G–3/5/7 has DA and general staff responsibility for determining Army priorities for intelligence. This responsibility is executed through the activities of the Army Priorities Intelligence Needs Coordinating Group. The Army intelligence priorities are determined annually and are based on The Army Plan. The approved Army intelligence priorities are available by contacting DCS, G–3/5/7 (DAMO–SSP).

b. DCS, G–3/5/7 will—

- (1) Coordinate with DCS, G–2 on requirements and funding for MDI support to STFs, SSGs, study directives, analyses, and guidance documents.
- (2) Participate in DA-level TSGs for coordination of MDI as appropriate.
- (3) Coordinate with DCS, G–2 on appropriate MDI guidance and policy.
- (4) Coordinate with DCS, G–2 for training support requirements, including threat guidance and foreign materiel for training.

2–6. Deputy Chief of Staff, G–8

DCS, G–8 will—

- a. Coordinate with DCS, G–2 on appropriate MDI guidance and policy and coordinate with DCS, G–2 on requirements and funding for MDI support to programs, requirement study directives, analyses, and program guidance documents.
- b. Participate in DA-level TSGs for coordination of MDI as appropriate.
- c. Ensure DCS, G–2 (DAMI–FIT) has the current program schedule information for all program MDRs, DABs, AROCs, ASARCs, and other program decision points that may require a VOLT and/or threat test support package (TTSP) update.

2–7. Other Army Staff elements

The ARSTAF will submit requirements for MDI support to DCS, G–2 (DAMI–FIT) in accordance with this regulation.

Section II

Army Commands, Army Service Component Commands, and Direct Reporting Units

2–8. Commanders, Army commands, Army service component commands, and direct reporting units

Commanders, Army commands, Army service component commands, and direct reporting units will—

- a. Ensure each subordinate element registers intelligence product needs with the Army dissemination PM.
- b. Review annually all submitted intelligence PRs and registered statements of intelligence interest and cancel, revise, or reinstate.

- c.* Provide periodic assessments of how well intelligence production has addressed requirements relevant to the command's mission.
- d.* Ensure appropriate threat documentation is prepared and approved for nonstandard systems, developmental systems, nondevelopmental items, and commercial off-the-shelf technology or obtain a waiver from the appropriate authority.

2–9. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

- a.* Determine intelligence threat support requirements for capability development under TRADOC purview and provide requisite threat support in collaboration with other threat support activities and DCS, G–2. Also serve as liaison to DCS, G–2 and AMC G–2.
- b.* Assign threat managers (TMs) to support combat development activities at the proponent schools or centers of excellence.
- c.* Provide intelligence threat support to training development, concept development, and JCIDS documentation.
- d.* Develop initial VOLTs for all ACAT I/II programs prior to the development request for proposal (Dev RFP) unless designated otherwise by the TSG and update in accordance with guidelines in paragraph 4–2.
- e.* Prepare and validate initial VOLTs for ACAT III programs prior to Dev RFP if required by the TSG (see para 4–2).
- f.* Prepare TTSPs to support an operational test (OT) or combined DT and OT for all Army programs.
- g.* Provide threat input for the Test and Evaluation Master Plan (TEMP).
- h.* Develop threat and foreign portions of scenarios and force templates to support capability development.
- i.* Participate in onsite approval and validation of OT threat portrayals in coordination with the U.S. Army Test and Evaluation Command (ATEC) and operational assessments occurring in DT.
- j.* Chair or participate in TSGs as appropriate. Participate in T&E working integrated product team (WIPT) and threat accreditation working groups (TAWGs).
- k.* Provide or review and approve threat and foreign intelligence used in TRADOC-sponsored or conducted studies (for example, analysis of alternatives (AoAs)), models, scenarios, databases, simulations, and systems.
- l.* Prepare, review, and approve operational environment (OE), threat, and opposing forces products and depictions for Armywide training.
- m.* Identify and submit command threat support requirements using the Community On-Line Intelligence System for End-Users and Managers (COLISEUM).
- n.* Consistent with AR 5–11, ensure requirements of the OE are represented across all M&S-enabled communities. OE requirements are defined by a framework of political, military, economic, social, information, infrastructure, physical environment, and time.

2–10. Commanding General, U.S. Army Materiel Command

The CG, AMC will—

- a.* Determine intelligence threat support requirements for capability development under AMC purview and provide requisite threat support in collaboration with other threat support activities and DCS, G–2. Also serve as liaison to DCS, G–2 and TRADOC G–2.
- b.* Provide foreign intelligence officers (FIOs) at the appropriate Life Cycle Management Command (LCMC), U.S. Army Research, Development and Engineering Command (RDECOM), RDECs, and laboratories to serve as the primary source of MDI support to PEO/PMs and technical and laboratory directors.
- c.* Chair or participate in TSGs as appropriate and participate in T&E WIPTs, VWGs, and TAWGs.
- d.* Revise VOLTs for all ACAT I/II programs from the Dev RFP and throughout the remaining life cycle unless designated otherwise by the TSG. Update in accordance with guidelines in paragraph 4–1.
- e.* Prepare and validate VOLTs for ACAT III programs from Dev RFP and throughout the remaining life cycle if required by the TSG (see para 4–1).
- f.* Ensure integration of approved MDI in DT. Prepare TTSPs for DTs that support MDRs and ensure realistic MDI portrayals.
- g.* Coordinate with PMs/PEOs and DCS, G–2 to ensure appropriate funding is provided for MDI support of Army RDA programs.
- h.* Determine intelligence documentation requirements for programs under AMC purview.
- i.* Provide MDI support and guidance to technology base programs, to include ATD, ACTD, and ATO programs.
- j.* Provide threat input to program management documents (for example, TEMP and DT plans).
- k.* Where intelligence gaps exist, prepare and submit requirements for new intelligence using COLISEUM.
- l.* Provide technology assessments in support of international cooperative programs, foreign comparative testing, technology protection and export control activities.

- m.* Identify and submit command threat support requirements using COLISEUM.

2–11. Commanding General, U.S. Army Space and Missile Defense Command/U.S. Army Strategic Command

The CG, SMDC/ARSTRAT will—

- a.* Identify and submit threat support and documentation requirements for space and missile defense programs under SMDC/ARSTRAT purview to national intelligence production centers and DCS, G–2.
- b.* Support TRADOC in the development of initial VOLTs, VOLT updates, and TTSPs for T&E as appropriate.
- c.* Participate in appropriate TSGs, TAWGs, and VWGs as required.
- d.* Submit to DCS, G–2 a listing of proposed targets and munitions to be used in live-fire tests for approval.
- e.* Be responsible for engineering, development, acquisition, fielding, and capability accounting for threat representations and major range instrumentation necessary for T&E of space and missile programs (which are not under the purview of the Program Executive Office for Simulation, Training, and Instrumentation (PEO–STRI)). Develop threat representations for foreign materiel as necessary.
- f.* Identify surrogates or develop simulators or simulations instead of foreign materiel as required for those requirements not under the purview of PEO–STRI.
- g.* Support NGIC in developing program-specific threat and T&E documentation for development programs under SMDC purview.
- h.* Provide FIOs to designated PEO/PMs to serve as their primary source of MDI support to development programs and as their liaison to TRADOC G–2, and the national intelligence community.
- i.* Coordinate, prepare, and review with TRADOC elements and then forward to DCS, G–2 all threat statements developed for issues related to the integration of space programs and strategic and national missile defense programs.
- j.* Provide intelligence support to the SMDC/ARSTRAT Future Warfare Center and its Force Development Integration Center as required.
- k.* Assist DCS, G–2 with the integration of capabilities development by serving as a liaison to the Missile Defense Agency.
- l.* Prepare and update existing VOLTs for space and missile defense programs that are or will fall under SMDC/ARSTRAT purview.

2–12. Commanding General, U.S. Army Test and Evaluation Command

The CG, ATEC will—

- a.* Coordinate test planning with TRADOC and AMC to ensure that a validated threat will be used in planning all Operational Test Command and Developmental Test Command managed activities.
- b.* Participate in TSGs to ensure that MDI requirements to support testing are identified as early as possible after program initiation.
- c.* Review and monitor all ATEC-managed testing activities and coordinate with DCS, G–2 (DAMI–FIT), AMC, and TRADOC to ensure that the threat represented in testing conforms to the approved threat to the maximum extent feasible and that all shortfalls and their impacts are documented.
- d.* Coordinate with DCS, G–2, NGIC, AMC, and TRADOC to ensure that best available intelligence is used to determine threat system technical parameters and threat force doctrine, tactics, techniques, and procedures. The ATEC threat coordinator will ensure that appropriate intelligence data and approved threat assessments are integrated into DT and OT. Also participate in DA-level TSGs, as appropriate.
- e.* Participate in DUSA (TE)-chaired VWGs in accordance with DA Pam 73–1.
- f.* Employ Army-validated threat representations in Army testing in accordance with the TTSP. Ensure that threat representations to be used for DT (including contractor tests) and OT (including limited user tests) are validated and accredited (see DA Pam 73–1).
- g.* Accredite threat models and simulations used for specific DT (including contractor tests) and OT (including limited user tests).
- h.* Chair TAWGs in support of OT and combined DT/OT to obtain approval of the threat representation accreditation report (see DA Pam 73–1 for threat considerations in testing).
- i.* Coordinate with DCS, G–2 (DAMI–FIT), AMC, and TRADOC for threat input for TEMPs.

Section III

Other Army Elements

2–13. Program executive officers, program/project managers, and U.S. Army Training and Doctrine Command capability managers

The PEO, PM, and TCM will—

a. Incorporate MDI data at the earliest opportunity and throughout the acquisition life cycle of a program. Combat and materiel developers must acquire, use, and remain cognizant of changes to the threat that could have significant impact on their programs. Specific planning will be included for obtaining, updating, and using intelligence support throughout the life cycle of the program.

b. Coordinate and fund MDI support through the appropriate TRADOC TM (combat developers) or AMC FIO (PEO/PM and other materiel developers).

c. Ensure DCS, G–2 (DAMI–FIT) has current program schedule information for all program MDRs, DABs, ASARCs, AROCs, and other program decision points that may require intelligence support.

d. Incorporate threat statements into the various JCIDS documents as outlined in DODD 5000.01, CJCSI 3170.01I, AR 70–1, AR 71–9, and AR 73–1.

e. Provide system description to supporting intelligence activities. Accurate and thorough system descriptions drive development of a program’s VOLT and ensure quality analysis. Review system descriptions during the VOLT update process.

f. Develop and approve Critical Intelligence Parameters (CIPs) for each program, in coordination with supporting TM/FIO.

g. Establish an LMDP for each intelligence mission data (IMD)-dependent program and establish a risk management process to determine impact of IMD shortfalls to system capabilities (see DODD 5250.01 for the requirement for an LMDP).

h. Identify critical program information (CPI) necessary to ensure appropriate program protection planning. If CPI is present in the system, ensure a PPP supported by a multidiscipline counterintelligence threat assessment (MDCITA) is completed in accordance with milestones listed in DODI 5000.02 (see AR 70–77 for program protection process).

i. Coordinate M&S planning with DCS, G–2 (DAMI–FIT) to ensure appropriate intelligence threat representation on the M&S integrated product team (IPT).

j. Coordinate test plans requiring threat input with the supporting TRADOC or AMC intelligence organization.

k. Address threat risk management in presentations to the ASARC and DAB.

l. Participate in TSGs and TAWGs as appropriate.

m. Notify DCS, G–2 (DAMI–FIT and DAMI–CD) of the technical capabilities, limitations, and quantities of systems developed under Army auspices that become co-development programs with a foreign government or are identified for foreign military sales.

n. Notify PEO–STRI of any threat representations needed to support test events (see DA Pam 73–1 for guidance on instrumentation, targets, and threat simulators).

o. Ensure only validated and accredited threat representations are used in test events supporting an MDR (see DA Pam 73–1).

p. Coordinate all instances of DD Form 254 (Department of Defense Contract Security Classification Specification), indicating a requirement for intelligence with the supporting TRADOC TM, AMC LCMC FIO, or RDECOM FIO in accordance with local procedures.

2–14. Commander, National Ground Intelligence Center

Under the DIAP, the Defense Intelligence Agency (DIA) has delegated to NGIC the analysis and production responsibilities to support the intelligence needs of the Department of the Army, as well as other warfighting, policy, acquisition, and force modernization customers. DIAP also assigns to NGIC the key enterprise role of producing threat assessments and providing service validation for DOD and Army acquisition programs. NGIC also has collection management, analysis, and production responsibilities for the Army under the direction of DCS, G–2. The Commander, NGIC will—

a. Develop threat documentation, including assigned threat modules as part of the Defense Intelligence Threat Library (DITL) in coordination with DIA and DCS, G–2 (see DIAI 5000.002 for procedures to produce DITL modules).

b. Provide threat data as required to DCS, G–2 TSG for capability development programs, ACTDs, ATDs, and other efforts such as Army warfighting experiments.

(1) Support intelligence activities in developing and updating threat modules and VOLTs.

(2) Support TSGs, T&E WIPTs, VWGs, and TAWGs under T&E WIPT auspices as requested. Coordinate with the appropriate TISO to support.

(3) Notify DCS, G-2 (DAMI-FIT and DAMI-CDC) in the event that information is acquired indicating a potential significant vulnerability of a major component of the operational force structure or a major acquisition program.

(4) Provide intelligence threat support to special access programs (SAPs) in coordination with DCS, G-2 (DAMI-CD). Coordinate with DCS, G-2 (DAMI-FIT) on the presentation of annual threat briefings at working and Vice Chief of Staff Special Access Program Oversight Committee meetings.

c. Represent the Army at intelligence community briefings to maintain currency on evolving threats to Army forces and systems.

d. Ensure intelligence support to acquisition programs, including the satisfaction of PRs and CIPs, the production of science and technical intelligence (S&TI), the management of both foreign materiel acquisition and exploitation activities, and necessary threat capability and parametric databases, is developed and maintained.

e. Perform intelligence studies and threat documentation supporting M&S and T&E in support of the Army acquisition decision process.

(1) Provide representatives to DA, PEO/PM, and Army commands to support VWGs and TAWGs for threat representations.

(2) Function as the authority for all threat data surrogate system data usage in support of Army T&E and analytical modeling efforts in coordination with DCS, G-2 and the U.S. Army Materiel Systems Analysis Activity (AMSAA).

(3) Provide foreign weapon systems data to the Army Research Laboratory and AMSAA for the production of weapon system performance information for use in Army T&E and analytical efforts.

(4) Review and approve the foreign weapon system performance information produced by AMSAA.

(5) Provide foreign weapons systems data to PEO-STRI for production of threat representations that support T&E and training.

(6) Support TRADOC and DCS, G-2 (DAMI-CD), as required, in reviewing models and simulations to ensure that threat representation is in consonance with validated intelligence documentation and threat data accurately reflects system capabilities.

f. Produce and disseminate all-source intelligence as an integrated MDI product from multiple intelligence collection disciplines and function as either a primary or a collaborative production center in accordance with the DIAP.

g. Produce intelligence to satisfy Army responsibilities under Title 10.

h. Participate as directed in the DIAP. As a primary production center, prepare a production center response to every PR assigned by a validation office.

i. Assist in the development of MDI and its application in selected combat and materiel developers' acquisition programs, studies, DT, OT, combat training center opposing forces portrayal, and models and simulations.

j. In coordination with TRADOC, assist and focus on model sensitivity, decision logic performance, data input, scenario use, tactics, and doctrine.

k. Develop threat analysis and forecasting methodologies.

l. In coordination with DCS, G-2 (DAMI-FIT) and INSCOM, support intelligence-related foreign materiel acquisition and exploitation (see AR 381-26).

m. Serve as the focal point for Army Staff studies and coordinate DCS, G-2 representation to STFs, SSGs, SAGs, general officer steering committees, and other study efforts requiring S&TI support.

n. Provide analytical support to PMs during Critical Program Information Assessments.

o. Provide IMD, level of data availability, and IMD production costing for the IMD Center, acquisition, and operational use (see DODD 5250.01).

2-15. Program Executive Officer for Simulation, Training, and Instrumentation

The PEO-STRI will—

a. Oversee engineering, development, acquisition, fielding, life cycle management, and capability accounting for Army threat representations, threat training simulators/simulations and major range instrumentation, other than those provided by SMDC. Develop threat representations in lieu of foreign materiel as necessary.

b. Identify candidate threat representations and submit for accreditation when validated threat representations are unavailable. Determine the functional equivalent for threat systems in lieu of vulnerability, effectiveness, and performance estimates for specific threat systems and munitions, where the required information for the specific threat is not yet available.

c. Coordinate with DCS, G-2 on requirements for MDI support for development, updating, and validation/ accreditation of threat representations.

2–16. Director, U.S. Army Materiel Systems Analysis Activity

The Director, AMSAA will coordinate with DCS, G–2 to ensure provision of appropriate MDI support to DA-sponsored force development studies.

Chapter 3 Intelligence Threat Support

Section I

General

3–1. Purpose

The purpose of intelligence threat support is to ensure that force, concepts, doctrine, training, organization, technology, and materiel systems the Army is developing provide the capabilities needed to carry out the Army's missions in the network-centric warfare environment. To achieve this purpose, threat support must be timely, consistent, and continuous.

a. Timeliness ensures threat considerations are provided to combat and materiel developers and risk managers throughout all phases of the development cycle in order to properly influence the requirement for and development of force, concepts, doctrine, training, organization, technology, and materiel systems.

b. Consistency requires that all users work from a standard, approved intelligence baseline.

c. Continuous threat support ensures that the threat is considered from concept development and continues throughout the life cycle of a materiel system (to include automated information systems) from identification of a deficiency, through and including post development product improvements and horizontal technology integration. It ensures organizational and doctrinal developments are supported throughout their conceptual phases and after implementation.

3–2. Guidance for threat preparation

a. Intelligence threat support will be initiated early in the operational needs or capability development process. Early intelligence support ensures that the impact of the threat is considered during the entire capability development process. An intelligence support program consists of the following:

(1) *Intelligence threat support structure.* The collaborative process begins with the TISO, TRADOC G–2, and AMC G–2. It can include DCS, G–2 (DAMI–CD), ACIC, SMDC/ARSTRAT G–2 and support from the intelligence service centers.

(2) *Intelligence baseline.* The intelligence baseline comprises appropriate DOD, national intelligence community, and Army intelligence products (documents, databases, models, simulations, concepts, and scenarios).

(3) *Intelligence support process.* These are procedures used to apply intelligence data to capability development and to receive updates that impact a program.

b. The sponsor will identify intelligence threat support requirements in coordination with DCS, G–2. The intelligence support activity at each command level is responsible for coordinating and providing support to combat and materiel developers for the application of threat in support of programs and studies conducted within the command.

c. The basis or start point for developing the threat in support of a specific program, system, or study is intelligence community data sources, to include a variety of DOD threat databases maintained as part of the DIAP. Because the relationship between a U.S. concept, capability, system, or program and the OE/threat is dynamic and reflects changes in tactics, doctrine, technological advancements, and developing intelligence, intelligence support activities of proponent commands must keep abreast of these developments and ensure they are accounted for in evolving documentation.

Section II

Intelligence Threat Support Structure

3–3. Threat integration staff officer and threat analyst

TISO/TA roles for threat integration for programs and studies include but are not limited to:

a. Representing DCS, G–2 and serve as primary HQDA staff point of contact for intelligence support.

b. Coordinating implementation of Army policy relating to intelligence support.

c. Coordinate with DOD, DIA, and other service intelligence agencies on all aspects of intelligence support to Army-specific or joint service acquisition programs.

d. Establishing a TSG for each program (see para 3–9).

- e.* Attending other services' intelligence coordination meetings and serving as the DCS, G-2 representative for Army approval of the threat in other services' VOLTs.
- f.* ACAT ID, coordinating VOLT validation with DIA and its participation in the TSG.
- g.* ACAT IC/II, establishing and chairing TSG and coordinating validation of VOLT by DCS, G-2 after collaborative development.
- h.* Representing DCS, G-2 on all ACAT I, II, and selected OSD/congressional oversight system T&E WIPTs and TAWGs to ensure timely intelligence support, and supporting the T&E WIPT chairman as the threat integrator in order to assist in generating and articulating requirements for intelligence support.
- i.* Providing intelligence threat support for ACTDs, ATDs, and selected ATOs.
- j.* Providing S&TI information to the ARSTAF.
- k.* Reviewing CIPs that impact on the effectiveness, survivability, or security of U.S. systems.
- l.* Reviewing PRs that support CIPs and monitor responsiveness to requirements generated as a result of VOLT development to support the acquisition life cycle of major automated information systems.
- m.* Coordinate review of threat statements and assessments contained in JCIDS documents supporting Army programs and analysis.
- n.* Representing the Army at intelligence community briefings to maintain currency on evolving threats to Army forces and systems.

3-4. U.S. Army Training and Doctrine Command Deputy Chief of Staff, G-2

TRADOC G-2 roles and duties include:

- a.* Providing direction, management, oversight, and support to TRADOC and intelligence activities in support of TRADOC mission commanders at the Centers of Excellence and Schools for OE support to training and capability developments; and review and validate TM produced intelligence products for training and developments to ensure consistency across TRADOC and full integration of all aspects of the OE.
- b.* Studying, designing, producing, coordinating, maintaining, and applying current and future OEs and validates OE replication and design for Army and joint services wargames and experiments, requirements definition, concept development, models, and simulations and acquisition.
- c.* Acting as the responsible official for the Army Opposing Forces Program.
- d.* Providing threat T&E management for the command; provide T&E support, including all related document preparation, for Headquarters, TRADOC and Combined Arms Center associated test activities; oversee/assist the provision of threat support to other operational (and DT/OT combined) tests as directed; and coordinate with DIA; DCS, G-2; ATEC; AMC; and SMDC/ARSTRAT, as appropriate.
- e.* Developing and coordinating (in accordance with JCIDS requirements) OE and threat products that serve as the benchmarks for all systems or capability development.
- f.* Participating in TSGs (or other deliberative bodies) and chair them as required.
- g.* Where appropriate to support the TRADOC capability manager, assigning a TM whose duties will include but are not limited to—
 - (1) Serving as the TCMs primary source of MDI support throughout the capability development process.
 - (2) Participating in TSGs for coordination of MDI support to the force, combat, and materiel development process as appropriate.
 - (3) Producing initial TTSP and updates.
 - (4) Researching and providing information on emerging threats.
 - (5) Participating in IPTs, including the T&E WIPT in preparation for OT and combined DT/OT.
 - (6) Preparing and updating VOLTs for all acquisition programs prior to Dev RFP the direction of the TSG.

3-5. U.S. Army Materiel Command, G-2 and U.S. Army Space and Missile Defense Command/U.S. Army Strategic Command intelligence officers

- a.* The AMC, G-2 supports capability development throughout the entire life cycle of Army RDA programs from basic research through acquisition until the decommissioning of the program.
- b.* AMC, G-2 supports the structure within AMC major subordinate commands, RDECs, and laboratories within RDECOM. The FIOs provide MDI and threat support to PEOs, RDECs labs, and contractors. The SMDC/ARSTRAT G-2 provides similar support to a number of intelligence officers within SMDC/ARSTRAT elements. FIO and SMDC/ARSTRAT intelligence officer duties include but are not limited to—
 - (1) Serving as the primary source of MDI support for the PEOs/PMs, RDECs, and labs throughout the research phases of research and development projects and the entire life cycle of assigned materiel development programs.
 - (2) Participating in program IPTs including the T&E WIPT.

- (3) Participating in TSGs for coordination of MDI support to the force, combat, and materiel development process as appropriate.
- (4) Integrating appropriate intelligence data and approved threat assessments in DT and supporting TRADOC G-2 and the ATEC threat coordinator in the integration of appropriate intelligence data and approved threat assessments in OT.
- (5) Providing threat statements and appropriate threat guidance in acquisition documents.
- (6) Documenting and submitting PRs that support CIPs and other intelligence requirements identified by PEO/PMs, RDECs, and labs, and monitoring PRs, reviewing them annually, and disseminating any information resulting from a PR.
- (7) Preparing TTSPs for DT test events that employ threat.
- (8) Preparing/updating VOLTs for all acquisition programs in support of the Dev RFP and throughout the remaining life cycle, at the direction of the TSG.
- (9) Assisting in the threat input and systems lay down for M&S.
- (10) Researching, analyzing, and providing intelligence-derived information on current and future threat capabilities.
- (11) Coordinating through intelligence channels for acquisition of foreign materiel and technologies in support of RDA.
- (12) Serving as liaison between the intelligence community and PEOs/PMs, RDECs, and labs.
- (13) Coordinating MDI support to technology and program protection activities.
- (14) Coordinating GMI, current intelligence, and intelligence support on force protection and counterterrorism to the LCMC and RDEC commanders.
- (15) Serving as the single point of contact for the local foreign military intelligence collection activities.

Section III

Intelligence Threat Baseline

3-6. Intelligence threat baseline products

- a.* Intelligence products are publications, automated databases, reports, measurements and signatures files, models and simulations, and electronic media that address foreign force capabilities in the near term (0 to 5 years), midterm (5 to 10 years) and long term (10 to 20 years or greater). Timelines for intelligence products that support DOD Information Assurance Certification and Accreditation Process activities are near term (0 to 12 months), mid-term (12 to 18 months), and long term (over 18 months).
- b.* Baseline products are essential for sustaining consistent threat throughout the capability development process and represent the start point for assessments developed prior to initiating specific requests for support.
- c.* Programs requiring CI threat products will submit the appropriate request through their local FIO. Only programs with a CPI validated by DCS, G-2 (DAMI-CD/Army Research Technology Protection Center (ARTPC)) are authorized to request MDCITA from the ACIC.

3-7. Defense Intelligence Threat Library

- a.* The DITL composed of the threat modules is the DOD intelligence community's official assessment of the principal threat systems and capabilities that a potential adversary might reasonably bring to bear in an attempt to defeat or degrade U.S. systems and capabilities.
- b.* The DITL is a primary source of intelligence threat for preparation of threat portions of JCIDS documents and VOLTs. Data in the threat module is considered validated for use in the capability development process upon module publication (see DIAI 5000.002 for procedures to manage the DITL).
- c.* Modules are NOT meant to replace VOLTs, which are system specific. They are a starting point for evaluating the impact of baseline intelligence on development of a specific capability.

3-8. Strategic support analyses, joint country force assessments, and U.S. Army Training and Doctrine Command standard scenarios

- a.* DODI 8260.2 direct DOD components to prepare analytic baselines in support of strategic analysis. These analytic baselines are provided in Support for Strategic Analysis (SSA) products. While service components are encouraged to use SSA products whenever possible, this does not prohibit using other scenarios. When the threat or OE described in a validated VOLT are not represented in an available SSA products, TRADOC may develop scenarios that are linked to other validated sources.
- b.* Multiservice force deployment (MSFD) products are DOD-approved theater campaign sets of ally and threat scenario data describing the full spectrum of conflict for future postulated scenarios outlined in the SSA products. The MSFD provides the red and blue concept of operations and D-day/H-hour force lay downs.

c. Joint country force assessment (JCOFA) provides the database of force structure and equipment that populates the MSFD and SSA products.

d. TRADOC standard scenarios are developed by the TRADOC Analysis Center. A TRADOC standard scenario normally uses the documentation provided in an analytic baseline, in most cases an SSA product and an MSFD database, to document reasonable and feasible combat operations in a joint context derived from the analytic baseline. These operations are framed at the tactical and operational level and provide a basis for analyzing force development and materiel options available. Excursions to the base case are routinely developed to determine cost and risk boundaries as well as to ensure that threat cases described in the VOLT are examined.

Section IV

Intelligence Threat Support Process

3–9. Threat steering group

a. *General.* The TSG is the primary deliberative and working body to coordinate and validate intelligence threat support. It assigns threat support tasks and responsibilities and provides intelligence support to combat and materiel development programs. It is composed of representatives from the Army's combat and materiel development activities, T&E organizations, and the intelligence community to coordinate the provision of timely, consistent, and approved intelligence support for capability development initiatives. There may be a variety of types of TSG, with the system-specific TSG being the most common.

b. *System-specific threat steering group.*

(1) *Purpose.* To coordinate threat support requirements for specific programs.

(2) *Authority.* ACAT ID is DIA; ACAT IC/II is DCS, G–2; ACAT III is TRADOC or AMC (depending on the milestone).

(3) *Members.* DIA (ACAT ID), TISO/TA, TRADOC G–2, AMC G–2, SMDC/ARSTRAT G–2 (if required), TM, FIO, Director of Operational Test and Evaluation (DOT&E), service intelligence center analysts, other S&TI centers (as needed), ATEC, and combat and materiel developers. Other programs of particular DA interest may require an HQDA-level TSG chaired by the appropriate TISO.

(4) *Frequency.* As required by DODI 5000.02 major milestones.

(5) *Charter.* The TSG establishes the forum in which intelligence input for VOLTs, TTSPs, TEMPs, and other related intelligence support documents are developed. Staffing of intelligence products is done in a collaborative environment and conducted virtually or via video/teleconferences when possible.

c. *Threat steering group I.*

(1) *Purpose.* To begin VOLT production or update and provide a means for intelligence and threat support input from the intelligence community for a specific program (see DIAI 5000.002 on conduct of TSGs).

(2) *Product.* Draft VOLT for staffing.

d. *Threat steering group II.*

(1) *Purpose.* To finalize VOLT, adjudicate comments, and resolve discrepancies.

(2) *Product.* Final VOLT. Final draft copy provided to validation authority along with comment resolution matrix. If there are no outstanding threat issues, the appropriate authority issues a validation memorandum.

e. *Other threat steering group actions.* The TSG chair will—

(1) Coordinate the review and validation of threat assessments for use in JCIDS documents.

(2) Coordinate review of M&S databases, scenarios, and analyses for correct application and interpretation of threat with the support of DCS, G–2 (DAMI–FIA).

(3) Review TEMP for threat requirements.

(4) Coordinate development of TTSP to support testing.

(5) Coordinate threat input into the AROC/ASARC to include status of intelligence certification.

3–10. Threat accreditation working group

a. The TAWG is established under the auspices of the T&E WIPT and conducted in accordance with AR 73–1 and DA Pam 73–1 to accredit threat representations for use in T&E. The ATEC threat coordinator or evaluator chairs the TAWG. DCS, G–2 (DAMI–FIT) coordinates threat support.

b. Membership includes ATEC Headquarters (Threats); PM; supporting TM and FIO; Tester, Army Evaluation Center; DCS, G–2; Threat Simulator Management Office (TSMO)/Targets Management Office (TMO); and threat representation developer (if different from TSMO/TMO).

c. Threat systems used to support T&E are subject to an accreditation process that identifies, analyzes, and documents the differences between the threat representation and the HQDA- or DIA-validated intelligence assessment of the actual threat system. Differences between threat representations and DIA-validated intelligence threat are documented and analyzed in threat representation accreditation reports issued by the TAWG. All differences affecting test issues are noted as potential test limitations.

d. The TISO/TA ensures the actual threat system data parameters are clearly laid out in the threat representation accreditation report. The TISO/TA assists in defining differences between the actual threat and the threat representation parameters and in defining the impacts of those differences on the test.

3–11. Army threat representation validation working group

a. Threat representation VWGs are conducted in accordance with AR 73–1 and DA Pam 73–1 to support development of accurate threat representation for T&E of Army capabilities. Army threat representation VWGs (with the exception of structures) are chaired by DUSA (TE) with an associated planning committee chaired by TSMO.

b. Structures should be standardized, characterized, and validated by region as being representative of that region to ensure consistency when measuring a munition's lethality during T&E events. The Army Regional Structural Validation Working Group will be chaired by the Army Research Laboratory-Survivability Lethality Analysis Directorate (ARL/SLAD) with support from NGIC and the Standard Military Operations in Urban Terrain Target and Testing Board. The structural working group will coordinate with the Army VWG (see AR 73–1 and DA Pam 73–1).

c. Membership as necessary will be from DUSA (TE); DCS, G–2; ATEC; PEO/PM as appropriate; NGIC (or appropriate intelligence production center); PM Instrumentation, Targets and Threat Simulators; AMC; DIA, ARL/SLAD (for structures) and DOT&E Test and Evaluation Threat Resource Activity.

d. DOD VWGs are chaired by the DOT&E Test and Evaluation Threat Resource Activity. Validation of threat representations is required to support tri-Service testing.

3–12. Other intelligence support to test and evaluation

a. *Development and acquisition of threat representations.*

(1) Passive or destructive testing will be coordinated with TMO.

(2) Other threat representations will be coordinated with TSMO if unclassified acquisition of threat targets are required that are not available from the TMO. The TSMO will also provide information on threat representations available in the Army inventory and can build to specifications when funded by the PM. Threat representations must be validated and accredited in accordance with AR 73–1 and DA Pam 73–1 before use in OT, DT (when data supports an MDR), or combined OT/DT.

b. *Foreign materiel acquisition.* Refer to AR 381–26.

3–13. Intelligence support to Army modeling and simulation

a. *General.* The Army M&S strategy establishes six M&S communities: acquisition, analysis, experimentation, intelligence, test & evaluations, and training. Multidiscipline intelligence support is required for M&S in each of these communities. Support will be consistent with DODI 5000.61; AR 5–11; DCS, G–2 Threat Data and Model Development and Validation Concept of Operation; the Army intelligence M&S strategy; and DCS, G–2 M&S action plan. TRADOC G–2, in coordination with DCS, G–2, is responsible for examining M&S in all domains to ensure that OE representation are adequate to the M&S use case.

b. *Threat modeling and simulation requirements.* Each community may have different but consistent requirements for threat S&TI data, GMI data, and M&S. Early identification of threat M&S requirements is essential to ensure timely and effective intelligence threat support. Beginning in the Army requirements determination process, senior intelligence officers and FIOs/TMs at all levels will assist integrated concept teams, combat, training, materiel developers, managers of ATOs, experiments, and demonstrations (ATD, ACTD) to identify threat M&S requirements.

c. *Threat modeling and simulation reuse.* Threat M&S reuse is essential to reduce duplication of M&S development efforts, reduce development time and costs, and improve consistency of threat representations within and across M&S communities. Threat community representatives (intelligence production center analyst, senior intelligence officer, FIO, TM) will assist combat, training, and materiel developers, testers, and their M&S developers to reuse threat data and M&S to the maximum extent possible. The Defense Intelligence Modeling and Simulation Catalog and related databases are key to accomplishing this. Army threat community representatives will obtain assistance from the NGIC M&S Office as the point of entry to the DIAP community's M&S and intelligence production resources. Specifically, senior intelligence officers, FIOs, and TMs will assist combat, training, and materiel developers, testers, and their M&S developers in—

(1) Preventing unwarranted duplication of threat M&S and maximizing reuse.

- (2) Ensuring intelligence data products are available to support M&S development.
- (3) Posting information to the Defense Intelligence M&S catalog on threat products under development (available at website <https://www.msco.mil/dodtools/dodenterprisemanagementtools/mscatalog.aspx>).
- (4) Updating M&S Catalog with validated threat M&S products.
- (5) Identifying threat M&S products that may have cross-domain application.
- (6) Participating in threat product verification and validation.

d. Verification, validation, and accreditation. Verification, validation, and accreditation (VV&A) of threat M&S will be conducted in accordance with AR 5–11 and DODI 5000.61. For threat models used in T&E, consult AR 73–1, DA Pam 73–1, and applicable DOD guidance. Whenever data or models of foreign systems, entities, phenomena, processes, behaviors, or forces are used in M&S to support acquisition decisions, regardless of the scope or level of the application, the threat community representative must participate in the validation process to ensure that threat information is DIA-validated and its use produces the intended results.

(1) The threat community will participate in the cooperative development, coordination, and approval of VV&A plans for any M&S that includes threat representation, in validation activities as specified in the plan, and in the accreditation of the M&S as appropriate, regardless of domain enabled community.

(2) Threat model validation will be carried out in parallel with threat model development. The threat community representative, as part of the VWG, will collaborate with the developer, the independent VV&A organization or activity, and appropriate customers to ensure that the product reflects the threat with fidelity appropriate to its intended use. The threat community representative will participate in validation activities defined in the VV&A plan. The threat community representative plays a coordinating role in development and publication of the validation report. At the conclusion of the validation process, the threat community representative will formally concur or nonconcur for the record on the validation report prior to the document's submission for formal approval. Nonconcurrences will be supported with substantial written rationale that will be included in a reserved section of any report that is submitted.

(3) After the threat model has been developed and validated, product description and administrative data are provided to Defense Intelligence Modeling and Simulation Resource Repository. The developer stores the model in the appropriate online repository.

(4) The threat community will assist the ATEC M&S accreditation action officer as part of the ATEC M&S accreditation process to ensure that threat data; performance characteristics; and tactics, techniques, and procedures emulated within the M&S are accurate and current intelligence community holdings.

3–14. Intelligence support to Army scenario development

a. Army analytic, training, testing, and research agencies require basic guidelines regarding precursory events, timelines, and threat employment concepts, in addition to data on threat force structure and weapon systems characteristics. This family of threat scenarios contains current SSA products as well as other threat scenarios based on TRADOC input.

b. To achieve accuracy, commonality, and consistency of the threat in scenarios, the following guidelines apply to the development of threat force scenarios:

(1) SSA products provide services with a plan for development of necessary military capabilities to maintain the nation's security. SSA products contain planning scenarios intended to provide a general illustrative sequence of events on which to base force development planning for a 20-year time frame, assess risk to programmed forces, and a common set of U.S. friendly force assumptions for use in computing readiness, sustainability, mobility, and modernization of resources. While SSA product compliant scenarios are desirable for analyzing contributions of materiel systems to combat, in some cases, they do not capture the threats outlined in the VOLT. When the threat in the SSA product is insufficient to provide a robust, capabilities-based threat needed to stress the system under test, then excursions or alternate scenarios may be developed which are based on the threat contained in the validated VOLT for that program. In those cases, TRADOC will ensure that scenario excursions from the base case(s) are developed to capture threats enumerated in the VOLT. Excursions should be clearly labeled and a full description of the amended order of battle or OE will be included as a part of the scenario excursion documentation. As a part of the TTSP review (see para 4–3), DCS, G–2 (DAMI–FIT) will coordinate a review to ensure that the threat used in the TTSP directed scenario, trials, and vignettes are representative of the VOLT.

(2) DCS, G–2 (DAMI–FIA) will review SSA product assumptions for impact on threat and provide input to the DOD scenario development process. TISO/TAs will coordinate inputs, including those from DCS, G–2 (DAMI–FIA) and other non-Army staff agencies, on scenario areas of concern affecting the programs for which they are responsible.

(3) Use TRADOC standard scenarios (high and low resolution) in studies and analyses to identify Army force modernization needs encompassing doctrine, organization, training, leadership, and materiel. Threat scenarios developed by TRADOC and reviewed by DCS, G–2 through the TSG process will serve as the base for Army combat and materiel development studies, unless otherwise directed by DA. TRADOC will use the SSA products, threat operational concepts developed by NGIC, and threat data derived from DIAP sources to develop standard scenarios. In cases where NGIC has

not produced operational concepts or tactical doctrine is unavailable, TRADOC may use the opposing forces doctrine prescribed in the approved TC 7–100 series. This generalized doctrine is representative of worldwide adversary’s tactical operations and provides a base to ensure consistency when real-world threat doctrine is not available. NGIC will review the TC 7–100 series periodically to ensure that opposing forces tactical doctrine is generally suitable. Army schools, centers, and activities involved in force and materiel development will use these approved scenarios for analyses. If threat excursions are employed, highlight them clearly in study reports.

(4) DCS, G–2 guidance to the Concepts Analysis Agency on global force employment scenarios will be based on specific study and model requirements. Generally, NGIC-developed threat operational concepts will serve as the start point for scenario development to provide a common threat basis for annual planning and programming studies conducted for the ARSTAF. DCS, G–2 will convene TSGs as needed to review results of analyses and to ensure that intelligence data on threat doctrine and force employment are logical and consistent.

3–15. Intelligence support to Army studies and analysis

a. General. Army studies conducted in accordance with AR 5–5 will include a process to identify requirements for threat and intelligence support. This process will apply to each of the eight categories of studies: Manpower and personnel; concepts and plans; operations and force structure; installations and logistics; science, technology, systems, and equipment; management; intelligence; and international security.

(1) Study directives and plans prepared by HQDA elements in accordance with AR 5–5, whose goal is to provide policy guidance or implementation, will be coordinated in draft with DCS, G–2 (DAMI–FI), to ensure that threat ramifications have been considered during the development process. Each study directive or plan will include, as a minimum, a section outlining potential threats to the process or system to be developed. The threat section will include a description of the threat that could reasonably be expected, and conditions or situations where the threats would likely manifest themselves.

(2) The study sponsor (ARSTAF element, field operating agency, or major command) may form a SAG consisting of representatives from Army elements having a clear functional interest in the study topic or use of the results. All SAGs with identified threat and intelligence requirements will have an intelligence representative. DCS, G–2 will provide a representative to SAGs formed for DA-directed studies. The SAG chairperson or study director will submit PRs for production support through the intelligence staff of the sponsoring agency. If the sponsoring agency has no intelligence staff, the PR will be submitted to DCS, G–2 (DAMI–FI). The SAG chairperson will identify intelligence requirements and provide a copy of the minutes of each meeting to DCS, G–2 (DAMI–FI).

b. Analysis of alternatives. The AoA is a critical document in the acquisition cycle that relies upon the use of modeling and simulation. It is normally incorporated in the program’s capability development document as an appendix.

(1) *Threat-related sections.* Threat-related sections of the AoA will be prepared and updated as required to meet the MDR process. Threat-related sections will be limited to SECRET or below. Higher level supplements may be added as needed. Threat-related section structure and format are dependent on the AoA scope and coordinated with the TSG.

(2) *Content and sources.* The threat assessment will be based on the VOLT or other DIAP threat data sources and in sufficient detail to identify, with a reasonable degree of assurance, conditions that might exist when employing the new U.S. system. As a minimum, the threat-related section should include broad considerations (such as nature and size of opposing forces or low- versus high-intensity conflicts), as well as detailed inputs (strength of kinetic energy projectile attacks, precision munitions employed, information warfare, precision munitions countermeasures employed, and so forth). Underlying assumptions concerning threat should not conflict with assumptions in SSA products.

(3) *Scenarios.* An AoA is used to determine the efficacy of changes in force design and equipping across a range of military operations. In most cases, a range of scenarios must be used to determine risk and cost boundaries. The commander performing the AoA will determine the scenario(s) to be used. The SAG associated with the AoA will review scenario selection. Scenarios used in an AoA will from SSA products and use the associated JCOFA and MSFD. The commander will request a waiver through DCS, G–2 in cases where existing SSA products are inadequate to address VOLT threats that will require development of a noncompliant scenario.

(4) *Approval and validation.* If the AoA was conducted using SSA products and validated intelligence, no further approval is necessary. A copy of all threat-related AoA documentation will be provided to DCS, G–2 for the record. If a non-SSA scenario is used, DCS, G–2 must review and coordinate DIA approval of all AoA threat-related sections.

c. Plans and strategy documents. Other Army plans and strategy documents (for example, The Army Enterprise Strategy and the Command and Control Protect Program Management Plan) will include a process to identify requirements for threat and intelligence support.

d. Other studies.

(1) The science and technology program covers a wide range of areas required for defense applications. The basic research and exploratory development stage provides the foundation on which all else is built for development and exploi-

tation of technological opportunities. In response to military needs, or in development of new military capabilities, technology is matured and applications are examined in the advanced development stage in order to establish the feasibility and military utility before acquisition decisions are made. Threat considerations must be included early in the development and throughout the life cycle of ACTD, ATD, and other technology efforts.

(2) ACTDs are test or demonstrations of mature technologies for potential rapid acquisition. ACTDs are an integral part of requirements definition and driven primarily by user requirements rather than by technologies. During ACTD planning, all factors which are essential to a major acquisition program will be considered. If the user is not prepared to acquire the system, ACTDs may be terminated and placed "on the shelf" for later use. If the user does want to acquire the system, the ACTD demonstrator may be modified so as to be made suitable for operational use and transitioned to the formal acquisition process at MS A, B, or C as appropriate.

(3) ATDs are undertaken to apply technology to military problems. ATDs assess the maturity of technologies and their potential for transition of new concepts into the formal acquisition process. ATD technologies may be applied across several systems.

(4) Other technology efforts not formally established as either ACTDs or ATDs may have potential application to military systems and may require threat input as appropriate.

(5) DCS, G-2 (DAMI-FIT) will work closely with the Army Science Board and the Assistant Secretary of the Army for Research, Development and Acquisition to ensure threat is considered in all demonstrations and other technology efforts as appropriate.

(6) The AMC G-2, through RDECOM and other subordinate FIOs, will ensure threat is integrated throughout the entire RDA process.

(7) ACIC is responsible for all Army counterintelligence analytical production worldwide related to technology protection. Army organizations requiring analytical support for technology protection issues should task the ACIC for support using procedures outlined in DIAP.

e. Battle labs. TRADOC established Army battle labs as a means to develop capabilities for a force projection Army that begins where battle appears to be changing and that encourages experimentation via simulations and prototypes using real Soldiers and real units to determine technology insertion or new requirements. The TRADOC G-2 is the lead for providing threat support for the battle labs in coordination with TMs on site and ensuring their threat portrayal is consistent with the threat portrayal for materiel development. DCS G-2, NGIC, and AMC provide support through TRADOC G-2 or TMs as requested.

3-16. Intelligence support to program protection

a. DCS, G-2 (DAMI-CD/ARTPC) coordinates technology protection engineers to assist the PM in identification of the CPI. If CPI is present, a PPP is required. The program is responsible through the local FIO to request MDCITA support from the ACIC. The ACIC will be responsible for the production of all counterintelligence related threat products to Army research, technology, acquisition programs.

b. The ACIC is responsible for production of the MDCITA for all Army acquisition programs with CPI. ACIC will produce MDCITA only upon the request of the program via a validated PR. The ACIC will manage production of counterintelligence threat analysis which supports ATDs, ACTDs, ATOs, and accelerated fielding initiatives identified by DCS, G-2 (DAMI-CD/ARTPC).

c. The ACIC will task appropriate intelligence centers for foreign S&TI data to support the MDCITA process. The ACIC will task appropriate national and service level CI agencies for supporting data for input to the MDCITA.

d. The ACIC will establish and maintain the Army's all-source database of foreign intelligence service threat activity directed at the U.S. Army, its personnel, programs, technologies, activities, and installations or facilities worldwide. The ACIC will provide all Army commands with counterintelligence analytical support for their technology protection programs. Analysis will be based on information that resides in the ACIC database.

e. The ACIC will produce a counterintelligence baseline analytical threat document. The foreign intelligence and security services threat assessment will document foreign intelligence service threat to deployed against U.S. Army forces and equipment worldwide. These assessments will document the various foreign services, their historical backgrounds and methods, and activities both inside the specific countries or regionally.

3-17. Intelligence support to contractors

Intelligence organizations supporting government contractors will establish procedure(s) to ensure that intelligence provided is current, approved, fulfills contract requirements, and is disseminated in accordance with DOD and DA security policies (see AR 380-5).

Chapter 4 Intelligence Threat Support Products

4-1. Validated Online Life-cycle Threat Report

a. Purpose. The VOLT is a statutory requirement to support policy makers and decision makers in Congress, OSD, and service RDA and T&E communities throughout a program's life cycle. It builds on the initial threat support to offer detailed information and analysis applying to a particular program, system, or family of systems. The VOLT summarizes the approved threat for combat and materiel developers, developmental and operational testers, and evaluators for all systems. It provides an assessment of the capabilities of potential adversaries to neutralize or degrade a specific U.S. system, or system concept. It is the primary threat reference used in preparation of threat portions of JCIDS documents, TEMPs, or TTSPs.

b. Format. Refer to DIAI 5000.002, Enclosure E4 for the VOLT format.

c. Requirement. Major Defense Acquisition Program and Major Automated Information System programs require a unique, system-specific VOLT report to support capability development and program manager assessment of mission needs and capability gaps against likely threat capabilities at initial operational capability (IOC). A designated VOLT is required for all programs unless waived by the MDA though they need not be system-specific. Programs on the DOT&E Oversight List require a unique, system-specific VOLT, unless waived by both the MDA and the DOT&E. Army ACAT ID program VOLTs require DIA validation. Army ACAT I/II programs and those on the DOT&E Oversight List require a DCS, G-2 validated VOLT. ACAT III programs generally do not require a VOLT because of the broad nature of the threat unless directed by the TSG. ACAT III threat assessments will rely on other appropriate assessments as coordinated by the TSG.

d. Timing. VOLTs are produced to support specific acquisition events as required by DODI 5000.02.

e. Submissions.

(1) *Initial submission.* The appropriate threat support activity as designated by the TSG, develops the initial VOLT.

(2) *Updates.* The appropriate threat support activity as designated by the TSG develops VOLT updates after Dev RFP.

(3) *Review and validation.*

(a) Acquisition category ID. Collaborative review via TSG. Validation authority is DIA. DCS, G-2 will forward the final draft VOLT to DIA along with comment resolution information.

(b) Acquisition category IC/II. Collaborative review via TSG. Validation authority is DCS, G-2. DIA receives an information copy via distribution.

(c) Acquisition category III (when applicable). Collaborative review via TSG. Validation authority is TRADOC or AMC (depending on milestone). DCS, G-2 receives an information copy via distribution.

(4) *Out-of-cycle changes.* The VOLT sponsor will publish out-of-cycle changes when there is a significant change in threat to the system or targets to be engaged by the system. All changes will be coordinated for review and validation as required for initial VOLTs, as outlined in paragraph 4-1e(1). Breaches in CIPs are flash traffic to the TSG and PM. The TSG will notify DIA of CIP breaches for ACAT ID programs.

(5) *Procedures for staffing and posting.* The VOLT sponsor will utilize the DAMI-FIT Knowledge Collaboration Center on Army Knowledge Online (secret internet protocol router network (SIPRNET)) for staffing and posting of final validated VOLTs and will coordinate with DCS, G-2 (DAMI-FIT) for posting and access. The DAMI-FIT Knowledge Collaboration Center is accessible on SIPRNET.

f. Family of systems Validated Online Life-cycle Threat. In light of increasing emphasis on integration, it is increasingly common for Army systems to operate largely or entirely as part of a system of systems or a family of systems. Individual VOLTs may not adequately capture the integrated nature of these systems or impacts of various threats that may not affect the system itself, but may affect the system or family of systems in which it operates. DCS, G-2 (DAMI-FIT) will consider requests to develop family of systems VOLTs to provide a comprehensive threat assessment for all systems in a given system of systems or family of systems that face a common operational threat environment, targets to be countered, and partially or entirely similar system-specific threats and emergent technologies.

g. Special access programs. SAP programs may require a VOLT or SAP annex to an existing VOLT. Threat support for SAPs and sensitive activities will be under provisions of AR 380-381. DCS, G-2 is responsible for recommending to the SAP Oversight Committee whether a program or activity warrants protection as a SAP.

h. Waivers. In the event that a program or system is not affected by a threat or is substantially similar to another system, the combat or materiel developer may submit a VOLT waiver request. The waiver will specifically state reasons why the particular system does not require a system-specific VOLT based upon its functionality and concept of employment. The waiver may be permanent until revoked based upon new intelligence or a change in ACAT level or it may be valid only until the next MDR. VOLT waivers for ACAT ID will be submitted to the Under Secretary of Defense for Acquisition via DCS, G-2 (DAMI-FIT) and the Army Acquisition Executive. VOLT waivers for ACAT IC or ACAT II programs will be

submitted to the Army Acquisition Executive via DCS, G-2 (DAMI-FIT). Waivers for programs on the DOT&E Oversight List will be submitted via the DOT&E to the MDA. The official with regulatory authority for a program must approve the waiver.

4-2. Test and evaluation master plan

a. Purpose. The TEMP is the initial document where the intelligence community has input into the resourcing phase for T&E activities for a program. It is imperative that intelligence be involved in TEMP development from the start to ensure adequate threat portrayal and resources to support test events.

b. Requirement. Representatives from DCS, G-2; TRADOC; AMC; PEO-STRI; ATEC System Team chair; and the program office in the form of a TSG will establish threat representation requirements for each T&E event in a program's life cycle.

c. Preparation. The TSG develops threat input into the TEMP as outlined in AR 73-1 and DA Pam 73-1. The threat portrayed in the TEMP is based on the latest validated VOLT, but focuses on the particular purpose of a test event such as a DT seeking to verify certain specifications have been met or an OT to verify that certain key performance parameters have been met.

(1) Threat for testing included in the TEMP must provide sufficient detailed intelligence information, including appropriate scenario information, to enable the PM to adequately resource the threat projected to exist at a post-IOC date and support the evaluator's analysis of results.

(2) Determination of threat year and scenario selection will be made by the T&E WIPT based on recommendations of the system proponent and the TSG.

d. Approval. Approval is a review process that confirms all changes and comments required by the validating authority have been incorporated in the final TEMP document. Final approval of a TEMP is completed once the TEMP has OSD approval.

4-3. Threat test support package

a. Purpose. The TTSP is the baseline threat document for a specific test to describe the threat to be portrayed, specific guidance on threat targets and countermeasures, and how the threat fits into the overall T&E requirements.

b. Format. Refer to appendix B.

c. Requirement. When there is an identified Army-approved or DIA-validated threat to a program, that threat must be portrayed during the program's T&E process and a TTSP prepared if data from the test supports a MDR.

(1) If a DIA-validated threat portrayal is required for the test (ACAT ID), the appropriate command and or agencies must review, validate, and approve the TTSP following the same pattern as for the VOLT (see para 4-2).

(2) A TTSP is not required for a DT or OT that does not require replication of a specific threat. Determination of the requirement for an operationally realistic threat portrayal will be made by the T&E WIPT based on the recommendation of the evaluation organization and the TSG. If the T&E WIPT determines that a TTSP is not required for a specific program, TRADOC (for OT or combined DT/OT) or AMC (for DT) will prepare a memorandum for record to that effect with copy furnished to DCS, G-2 (DAMI-FIT). Specific testing requirements will be determined by the T&E WIPT.

d. Preparation. TRADOC is responsible for production of the TTSP to support OT (or combined DT/OT) events to include live-fire T&E in an OE. AMC will produce a TTSP for DT events. The TSG will coordinate development of the TTSP to ensure that DT and OT threat support is synchronized and that wherever possible the U.S. Army can test once and use the data repeatedly. Threat portrayed in the TTSP is based on the latest validated VOLT, but focuses on the particular purpose of the test (such as a DT seeking to verify certain specifications have been met or OT to verify that certain key performance parameters have been met).

(1) A TTSP must provide sufficient detailed intelligence information, including appropriate scenario information, to enable the tester to accurately portray the threat projected to exist at a post-IOC date and support the evaluator's analysis of the results.

(2) If intelligence other than that which is contained in the VOLT is needed for the TTSP, other validated sources can be used to supplement the VOLT or a PR submitted.

(3) Determination of threat year and scenario will be made by the T&E-IPT based on recommendations of the system proponent and the TSG.

(4) Limit TTSP classification to SECRET or below. Higher level supplements may be added as needed.

e. Timing. Initial TTSP development will follow TEMP timelines developed during the initial T&E WIPT meeting based upon guidance from TRADOC and the TSG. The TTSP must be approved through the TSG prior to each DT or OT requiring threat portrayal and provided to ATEC System team chair. Continuous coordination between the threat proponent, evaluator, and tester is strongly recommended.

f. Approval. Approval is a review process that confirms all changes and comments required by the validating authority have been incorporated in the final document. Approval of a TTSP does not automatically mean that the threat representations being planned for use have been accredited for use in that test. Threat representation validation and accreditation follow separate T&E community procedures (see DA Pam 73-1).

(1) DCS, G-2 (DAMI-FIT) approves all DT/OT TTSPs for Army ACAT I and for programs on the DOT&E Oversight List after intelligence community validation.

(2) TRADOC or AMC validates and approves TTSPs supporting ACAT II/III programs with copy furnished to DCS, G-2 (DAMI-FIT).

4-4. Program protection plan

a. Purpose. The purpose of PPP is to identify CPI and the most effective means to protect CPI following a risk management approach (see AR 70-77).

b. General.

(1) The PPP identifies CPI for protection from foreign collection activity and develops protection measures necessary to ensure a combat system's effectiveness throughout its life cycle. The PPP addresses CI threat or, more specifically, the foreign intelligence services targeting and collection directed at technology research and development programs.

(2) The PPP will contain an ACIC-produced or validated MDCITA that supports protecting CPI. The MDCITA describes those foreign governments, entities, or other foreign interests that have an interest, requirement, and capability to collect information about technology programs and associated critical technologies during the acquisition cycle. The assessment evaluates historical, initial, and finished intelligence reports of subversion and espionage directed against the Army; foreign intelligence service data, and extensive reviews of open source information. The assessment includes an analysis of foreign intelligence service technical collection capabilities which could be directed at RDA including production facilities and activities related to U.S. Army technology production. This assessment highlights potential countries and foreign companies which have the interest and collection capability to go after U.S. technology programs and their associated critical information. The PPP will contain a technology assessment control plan and a system security engineering approach. A delegation of disclosure authority letter is required if the system will be sold to foreign governments.

(3) Tailored and executable guidance is developed by the program protection IPT and disseminated and maintained for record at the program office.

c. Requirement. A program must have a validated DCS, G-2 (DAMI-CD/ARTPC) CPI. A PR must be submitted using COLISEUM. A valid PR for the ACIC to produce an MDCITA must contain the answers to the ACIC 30-question MDCITA questionnaire.

d. Preparation. The PPP is prepared by the PM with onsite assistance of DCS, G-2 (DAMI-CD/ARTPC). All MDCITA request are for one-time production. All dissemination is via posting to the ACIC Web site on the Joint Worldwide Intelligence Communication System. For additional information on PPP, refer to DODI 5000.02, Enclosure 3; AR 70-77; and DA Pam 70-3.

e. Timing. The PPP is required to support specific acquisition events as required by DODI 5000.02.

f. Approval. Approval is a review process to confirm that all changes and comments required by the validating authority have been incorporated in the final document. DCS, G-2 (DAMI-CD/ARTPC) approves all MDCITAs prior to MS B.

Appendix A

References

Section I

Required Publications

AR 5–11

Management of Army Models and Simulations (Cited in para 2–9*n*.)

AR 10–87

Army Commands, Army Service Component Commands, Direct Reporting Units (Cited in para 2–4*c*(1).)

AR 70–77

Program Protection (Cited in para 2–13*h*.)

AR 73–1

Test and Evaluation Policy (Cited in para 2–2*b*(4).)

AR 380–381

Special Access Programs (SAPS) and Sensitive Activities (Cited in para 1–6*c*(1).)

AR 381–26

Army Foreign Materiel Program (S//NF) (Cited in para 2–14*l*.)

DA Pam 73–1

Test and Evaluation in Support of Systems Acquisition (Cited in para 2–2*b*(4).)

DIAI 5000.002

Intelligence Threat Support for Major Defense Acquisition Programs (Cited on title page.) (Available on Army Knowledge Online at <https://www.us.army.mil/suite/doc/6807774>.)

DODD 5250.01

Management of Intelligence Mission Data (IMD) in DOD Acquisition (Cited in para 2–13*g*.) (Available at <http://www.esd.whs.mil/dd/>.)

DODI 5000.02

Operation of the Defense Acquisition System (Cited on title page.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (<https://armypubs.army.mil/>). DOD publications are available on the OSD website (<http://www.esd.whs.mil/dd/>).

AR 5–5

Army Studies and Analyses

AR 11–2

Managers' Internal Control Program

AR 25–2

Information Assurance

AR 25–30

The Army Publishing Program

AR 70–1

Army Acquisition Policy

AR 71–9

Warfighting Capabilities Determination

AR 380–5

Department of the Army Information Security Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–67
Personnel Security Program

AR 381–10
U.S. Army Intelligence Activities

AR 381–20
Army Counterintelligence Program

CJCSI 3170.01I
Joint Capabilities Integration and Development System (JCIDS) (Available at www.jcs.mil/library.)

DA Pam 5–11
Verification, Validation, and Accreditation of Army Models and Simulations

DA Pam 25–40
Army Publishing Program Procedures

DA Pam 25–403
Guide to Recordkeeping in the Army

DA Pam 70–3
Army Acquisition Procedures

Defense Intelligence Agency directive 5000.200
Intelligence Threat Support for Major Defense Acquisition Programs. (Available on AKO at <https://www.us.army.mil/suite/doc/6807773>.)

Defense Modeling and Simulation Office
VV&A Recommended Practices Guide (Available at <https://vva.msco.mil>.)

DODD 5000.01
The Defense Acquisition System

DODD 5000.59
DOD Modeling and Simulation (M&S) Management

DODI 5000.61
DOD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)

DODI 5200.39
Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)

DODI 5205.11
Management, Administration, Oversight of DOD Special Access Programs (SAPs)

DODI 8260.2
Implementation of Data Collection, Development, and Management for Strategic Analyses

DODI 8580.1
Information Assurance (IA) in the Defense Acquisition System

FM 3–0
Operations

FM 3–12
Cyberspace and Electronic Warfare Operations

General Order 2017–01
Assignment of Functions and Responsibilities Within Headquarters, Department of the Army

JP 3–12
Cyberspace Operations (Available at http://www.jcs.mil/doctrine/dod_dictionary/.)

Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)

(Available at www.dau.mil)

OSD Memorandum

From the Director of Operational Test and Evaluation, dated 3 Apr 18, Subject: Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs (Available at <http://www.dote.osd.mil>.)

TC 7-100.2

Opposing Force Tactics

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

The following forms are available on the Army Publishing Directorate website (<https://armypubs.army.mil/>) unless otherwise stated. DD forms are available on the OSD website (<http://www.esd.whs.mil/directives/forms/>).

DA Form 11-2

Internal Control Evaluation Certification

DA Form 2028

Recommended Changes to Publications and Blank Forms

DD Form 254

Department of Defense Contract Security Classification Specification

Appendix B

Threat Test Support Package Formats

B–1. Developmental threat test support package

a. Threat employed in formal government DTs and live-fire tests, contractor tests, and combined Government/ contractor tests will be documented in a developmental TTSP prepared by the PM's supporting intelligence organization, coordinated with the TSG, and approved by DCS, G–2 (for ACAT I/II) or AMC, G–2 (for ACAT III).

b. At minimum, the developmental TTSP will—

- (1) Identify the system, test plan, test organization, Government/contractor point of contact, location, and date.
- (2) Describe the threat (scenarios, weapon systems, targets, surrogates, simulators, computer models/ simulations) to be employed in the test and rationale.
- (3) Describe significant differences, if any, between actual threat and test threat and assess the impact on test threat realism.
- (4) Identify the system threat assessment report, intelligence source documents, and validation/accreditation reports pertaining to test threats.

B–2. Operational threat test support package

a. *Part I, Threat Test Requirements.* Part I provides the threat definition and expected threat to be portrayed during test to the TCM/PM and ATEC. It will be approved by the TRADOC assistant G–2–Threats (ATIN–LE), with copy furnished to DCS, G–2 for DIA validation (ACAT ID programs), and will contain the following information:

- (1) Section 1, Introduction.
- (2) Section 2, Test and evaluation criteria.
- (3) Section 3, Threat.
 - (a) Threat to system under test.
 - (b) Threat to be countered (targets).
 - (c) Threat applied countermeasures.

b. *Part II, Threat Test Planning and Documentation.* Part II is the foundation for the Threat Operational Test Readiness Statement. It will be approved by the TRADOC assistant G–2–Threats (ATIN–LE), with copy furnished to DCS, G–2 for DIA validation (ACAT ID programs), and will contain the following information under Section 4:

- (1) Threat test scenario.
- (2) Threat test concept.
- (3) Limitations:
 - (a) Threat.
 - (b) Test.
- (4) Requirements for frequency clearance.
- (5) Target-firer matrix and critical pairs.
- (6) Accreditation of threat representation and targets.
- (7) Threat description of test trials and vignettes.
- (8) Threat minimum start and end trial criteria.
- (9) Threat training plan.
- (10) Threat operational live-fire trials.

c. *Part III, Threat Test Execution and Reporting.* Completion of Part III occurs during and after the test. The majority of information to be included in the executive summary will be derived from Part II. Threat portrayal during test will be approved by the TRADOC assistant G–2–Threats and will contain the following information:

- (1) Annex A, record of threat portrayal conducted in test trials and vignettes.
- (2) Annex B, record of threat portrayal conducted in live-fire trials.
- (3) Annex C, status of threat approval and validation for threat test portrayal and test data.
- (4) Annex D, threat insights from test observation and review of data.
- (5) Annex E, remaining threat test requirements for program (from the TEMP).
- (6) Annex F, threat assessment from test portrayal (given test results, how should the threat for next test be portrayed).
- (7) Annex G, threat milestones and dates.
- (8) Annex H, threat test documentation (memorandums).
- (9) Annex I, figures, tables, and graphs.
- (10) Annex J, bibliography.
- (11) Annex K, distribution list.

Appendix C

Internal Control Evaluation

C–1. Function

The function covered by this evaluation is the administration of intelligence threat support to capability development and includes key controls for intelligence threat support management, records management, and publishing.

C–2. Purpose

The purpose of this evaluation is to assist senior intelligence officers in evaluating key intelligence threat support internal controls. It is not intended to cover all controls.

C–3. Instructions

Answers must be based on the actual testing of key internal controls (such as document analysis, direct observation, and sampling). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

C–4. Test questions

a. Responsibilities (see chap 2). Have MDI requirements been coordinated with the appropriate threat intelligence agency (all)?

b. Intelligence threat support activities (see chap 3).

(1) Has the organization assigned a TISO to support all ACAT programs within a functional area (HQDA)?

(2) Has the organization identified the supporting threat intelligence agency (TCM, PEO, PM)?

(3) Have threat intelligence requirements to support a program been outlined (TCM, PEO, PM)?

(4) Has the organization identified the threat integrator and notified them of upcoming IPTs (PEO, PM)?

(5) Has the organization conducted a TSG for all ACAT programs (HQDA, TRADOC, AMC)?

c. Intelligence threat support products (see chap 4).

(1) Do ACAT I/II programs have a valid VOLT published within 2 years (TCM, PEO, PM)?

(2) Has initial threat support been completed for ACAT III programs and appropriate intelligence baseline resources identified (TCM, PEO, PM)?

(3) Have developmental and operational tests requiring threat representations coordinated development of a TTSP (TCM, PEO, PM)?

C–5. Supersession

Not applicable.

C–6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to Deputy Chief of Staff, G–2 (DAMI–FIT), 1000 Army Pentagon, Washington, DC 20310–1000.

Glossary

Section I

Abbreviations

ACAT

acquisition category

ACIC

Army Counterintelligence Center

ACTD

advanced concept technology demonstration

AMC

U.S. Army Materiel Command

AMSAA

U.S. Army Materiel Systems Analysis Activity

AoA

analysis of alternatives

AR

Army regulation

ARIMS

Army Records Information Management System

ARL/SLAD

Army Research Laboratory-Survivability Lethality Analysis Directorate

AROC

Army Requirements Oversight Council

ARSTAF

Army Staff

ARSTRAT

U.S. Army Strategic Command

ARTPC

Army Research Technology Protection Center

ASA (ALT)

Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASARC

Army Systems Acquisition Review Council

ATD

advanced technology demonstration

ATEC

U.S. Army Test and Evaluation Command

ATO

Army technology objective

ATWG

Army Technology Protection Working Group

CG

commanding general

CI

Counterintelligence

CIP

critical intelligence parameter

CJCSI

Chairman of the Joint Chiefs of Staff instruction

COLISEUM

Community On-Line Intelligence System for End-Users and Managers

CPI

critical program information

DA

Department of the Army

DAB

Defense Acquisition Board

DCS

Deputy Chief of Staff

DD Form

Department of Defense form

Dev RFP

development request for proposal

DIA

Defense Intelligence Agency

DIAI

Defense Intelligence Agency instruction

DIAP

Defense Intelligence Analysis Program

DITL

Defense Intelligence Threat Library

DOD

Department of Defense

DODD

Department of Defense directive

DODI

Department of Defense instruction

DOT&E

director of operational test and evaluation

DOTMLPF

doctrine, organization, training, materiel, leadership and education, personnel, and facilities

DT

developmental test

DUSA

Deputy Under Secretary of the Army

DUSA (TE)

Deputy Under Secretary of the Army (Test and Evaluation)

FIO

foreign intelligence officer

GMI

general military intelligence

HQDA
Headquarters, Department of the Army

IMD
intelligence mission data

INSCOM
U.S. Army Intelligence and Security Command

IOC
initial operational capability

IPT
integrated product team

IT
information technology

JCIDS
Joint Capability Integration and Development System

JCOFA
joint country force assessment

JP
Joint publication

LCMC
Life Cycle Management Command

LMDP
life cycle mission data plan

M&S
modeling and simulation

MDA
milestone decision authority

MDCITA
Multidiscipline counterintelligence threat assessment

MDI
multidisciplined intelligence

MDR
Milestone decision review

MS
milestone

MSFD
multiservice force deployment

NGIC
National Ground Intelligence Center

OE
operational environment

OSD
Office of the Secretary of Defense

OT
operational test

PEO
program executive officer

PEO-STRI
Program Executive Office for Simulation, Training, and Instrumentation

PM
program/project manager

PPP
program protection plan

PR
production requirement

RDA
research, development, and acquisition

RDEC
Research, Development and Engineering Center

RDECOM
U.S. Army Research, Development and Engineering Command

RRS-A
Records Retention Schedule-Army

S&TI
science and technical intelligence

SAG
study advisory group

SAP
special access program

SIPRNET
secret internet protocol router network

SMDC
U.S. Army Space and Missile Defense Command

SSA
Support for Strategic Analysis

SSG
special study group

STF
special task force

T&E
test and evaluation

TA
threat analyst

TAWG
Threat Accreditation Working Group

TC
training circular

TCM
Training and Doctrine Command capability manager

TEMP
test and evaluation master plan

TISO
threat integration staff officer

TM

threat manager

TMO

targets management office

TRADOC

U.S. Army Training and Doctrine Command

TSG

threat steering group

TSMO

Threat Simulator Management Office

TTSP

threat test support package

VOLT

Validated Online Life-cycle Threat

VV&A

Verification, validation, and accreditation

VWG

validation working group

WIPT

working integrated product team

Section II**Terms****Accreditation**

Process of determining the extent to which a validated threat entity supports the requirements of the specific test or evaluation.

Acquisition category

Categories established to facilitate decentralized decision making and execution, and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority and applicable procedures. See DODI 5000.2 for specific definition for each acquisition category.

Approve

Within the context of this regulation, the term "approve" signifies that the changes required by the validating authority for a threat document have been incorporated by the originator and that the document is now approved for use (see "validate").

Army Research and Technology Protection Center

Integration and synchronization of security, intelligence, counterintelligence, foreign disclosure, and security countermeasures support to research and technology protection activities Armywide.

Army Systems Acquisition Review Council

Top-level DA corporate body for systems acquisition that provides advice and assistance to the Secretary of the Army and the Army Acquisition Executive.

Automated Information System

Subset of an information system which represents the use of general-purpose computer equipment. It does not include embedded computer resources designed into materiel systems by the materiel developer. The system normally consists of a combination of information, hardware (computer), components (monitor, keyboard, modem, printer, display, and so on), software, and telecommunications resources that collect, record, process, store, communicate, retrieve, and display information, such as personnel systems, financial systems, and inventory control systems.

Battle lab

Means to develop capabilities for a force projection Army that begins where battle appears to be changing. Tied to evolving battlefield dynamic concepts and warfighting doctrine in FM 3-0, battle labs use the battlefield as a reference. By encouraging experimentation via simulations or prototypes, battle labs determine requirements in the areas of doctrine, training,

leader development, organizational structure, materiel, and Soldier support. Since resources realities will curtail most new starts, materiel requirements will be primarily in the form of technology insertions. By focusing on horizontal integration of technology across the force, battle labs will further conserve resources.

Capabilities development document

A document that captures the information necessary to develop a proposed program normally using an evolutionary acquisition strategy. It outlines an affordable increment of militarily useful, logistically supportable and technically mature capability.

Capabilities production document

A document that addresses the production elements specific to a single increment of an acquisition program.

Combat developer

Command or agency that formulates doctrine, concepts, organization, materiel requirements, and objectives. Represents user community in materiel acquisition process.

Confidence level

Degree of probability that a given item of intelligence is accurate based on the quality of supporting intelligence information.

Constructive

Mathematical models used as a tool to support collective training (battalion commanders and staffs through Army Theater—Corps Battle Simulation, Combat Service Support Training Simulation System, Battalion Brigade Simulation and in individual training). May be used with or without human interaction. Sometimes referred to as war game models.

Critical intelligence parameter

Formerly known as critical intelligence categories, CIPs are categories of threat information dealing with platforms, weapons, systems, doctrine, or operational employment that, if developed, procured, or implemented by potential adversaries, could significantly influence the effective operation of the developing/deployed system. CIPs may include weapon system type and sub-type, mission and employment considerations, and weapon-related technology. They should include the technical characteristics or performance thresholds of weapon systems or technologies of particular concern to the U.S. program. The status of threat programs, technologies, and research efforts relative to the CIPs will be included, along with the potential for breaching CIP thresholds. The level of detail portrayed in the CIP should be sufficient to stand alone, without reference to other parts of the document. CIPs are used as a basis for developing production requirements in support of the acquisition program.

Critical program information

U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment (see DODI 5200.39).

Defense Acquisition Board

Senior DOD acquisition review board, chaired by Under Secretary of Defense (Acquisition).

Defense Intelligence Threat Library (threat modules)

The DITL is composed of threat modules that provide the bedrock analytical foundation for intelligence threat support to the defense acquisition process. Threat modules serve as the analytical foundation for VOLT reports and maintain projections of technology and adversary capability trends over the next 20 years.

Force development

Integration of allocated and projected Army resources into time-phased program to develop force properly organized, equipped, trained, and supported to carry out Army missions and functions worldwide. Includes force planning, programming, analysis, structuring, and combat and training developments.

Information system

Organized assembly of resources and procedures designed to provide information needed to execute or accomplish a specific task or function. It applies to those systems that evolve, are acquired, or are developed that employ IT. Information system equipment consists of components (for example, hardware, software, firmware, products, or other items) used to create, record, produce, store, retrieve, transmit, disseminate, present, or display data or information.

Initial capabilities document

Replaces the mission needs statement. Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis

of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects and time. The initial capabilities document summarizes the results of the DOTMLPF analysis and describes why nonmaterial changes alone have been judged inadequate in fully providing the capability.

Initial operational capability

First attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics, and which is manned or operated by an adequately trained, equipped, and supported military unit or force.

Instrumentation

The use of electronic or electromagnetic systems to sense and record events performed by real weapons systems, communications systems and personnel. Instrumentation includes detection, measurement, recording, telemetry, and data processing.

Integrated program summary

DOD component documents prepared and submitted to MDR authority in support of milestones. Succinctly highlights status of a program and its readiness to proceed into the next phase of the acquisition cycle.

Intelligence community

The intelligence community includes the service production centers (Army, Navy, Air Force, and Marine Corps), Central Intelligence Agency, DIA, Department of Homeland Security, Drug Enforcement Administration, Energy Department, Federal Bureau of Investigation, National Geospatial–Intelligence Agency, National Reconnaissance Office, National Security Agency, State Department, Treasury Department, and United States Coast Guard.

Joint program

Defense acquisition system, subsystem, component, or technology that involves formal management or funding by more than one DOD Component during any phase of the system’s life cycle.

Materiel developer

Command or agency responsible for research, development, and production of system in response to approved requirements.

Materiel system

Item, system, or all systems of materiel; includes all required system support elements.

Milestone

Major decision points that separate the phases of an acquisition program.

Model and simulation

A model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. A simulation is the operation or exercise of the model overtime. Also, a technique for testing, analysis, or training in which real-world systems are used, or where real-world and conceptual systems are reproduced by a model.

Multidiscipline counterintelligence threat assessment

Multidisciplined threat product that focuses on the foreign intelligence collection threat to the CPI of a specific U.S. Army technology program that will be used in a risk assessment for the allocation of resources to protect the CPI and the program during the acquisition cycle.

Multidiscipline intelligence

All-source intelligence, derived from all intelligence disciplines (including those falling under the classic counterintelligence discipline), that could present a threat to a system or systems development process, technology-based effort, or nondevelopmental item/commercial off-the-shelf procurement.

Production requirement

A PR states an intelligence production need for a general or specific subject, or to support a program, system, or weapon. PRs should be initiated by a DOD component whenever there is a perceived information gap. PRs should be supported by appropriate collection requirements.

Program protection plan

Identifies CPI and the most effective means to protect them following a risk management approach. Required at MS B. Updated on a regular basis, but at a minimum when a major milestone is pending or when new CPI are identified, new threat information is obtained, an annex to the PPP is developed/modified, or a compromise of CPI is identified.

Senior intelligence officer

An office or designated individual responsible for obtaining intelligence required by the command.

Simulation

To feign, to obtain the essence of, without the reality of warfare. In the distributed interactive simulation domains, everything short of actual combat is a simulation. Three categories are live, virtual, and constructive.

Special Access Program

Highly sensitive, classified acquisition program that complies with policies and procedures specified in DOD Instruction 5000.2 for acquisition category of programs with equivalent dollar value. Specific deviations to these policies and procedures must have concurrence of milestone decision authority, which may waive milestone documentation requirements. VOLTs and other threat-related documents prepared for highly sensitive classified programs are handled administratively in the same manner as other programs, unless special security arrangements are necessary. Special access clearances for these programs will be kept to a minimum.

Target array

An aggregation of target components that represents one or more essential aspects of the threat for an exercise, test, or simulation. Targets may range from mockups that resemble the actual threat visually from a distance or they may emit certain signatures that mimic the threat (for example, infrared, electromagnetic, or acoustic emissions, and so on). A target array is composed of expendable resources that may be used once and destroyed in the exercise or simulation.

Technologically feasible threat

The technologically feasible threat, though not constrained by intelligence projections, is consistent with an adversary's technological base, economic situation, and industrial production capabilities. The technologically feasible threat provides decision makers with a basis for judgment about the impact on a specific U.S. weapon system, if the threat were to evolve in a direction other than that considered most likely by the U.S. intelligence community.

Test and evaluation master plan

Overall planning document used to depict structure and objectives of test program. Provides framework within which to generate detailed test and evaluation plans and to determine schedule and resource implications associated with test and evaluation program.

Test and evaluation working integrated process team

Acquisition program working group chaired by PM and convened at PM's discretion, responsible for establishing and defining test conditions and applicable scenarios (year, region, targets, and arrays) in support of program testing. Representation typically consists of representatives from U.S. System PM, DCS, G-2, Threat Support Activities; Operational Test and Evaluation Command; Combined Arms Center Threats Directorate; and AMSAA. Principal threat integrators for T&E WIPT are the supporting AMC FIO for Developmental Tests and the TRADOC TM for Operational Tests. PM Instrumentation, Targets and Threat Simulators and NGIC are represented on T&E WIPT when discussions and test planning warrant their participation.

Threat

The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate U.S. mission accomplishment or reduce force, system, or equipment effectiveness. It does not include natural/environmental factors affecting the ability of the system to function or mission accomplishment; mechanical/component failure affecting mission accomplishment; or program issues related to budgeting, restructuring, or cancellation of the program.

Threat analyst

Army civilian intelligence specialists (series 0132) (or support contractors as necessary) designated as the HQDA threat integrator interchangeable with a TISO and assigned along Battlefield Operating System lines based upon their training and experience.

Threat array

An aggregation of threat components that represents the essential aspects of the threat for an exercise, test, or simulation. For example, an integrated air defense node component of simulated (hardware and software simulations/ simulators) radar vehicles, C3 vehicles, surface-to-air missile systems and affiliated support vehicles could be a threat array for a practical exercise, test, or simulation.

Threat assessment

Evaluation of enemy's or potential enemy's current or projected capability to limit, neutralize, or destroy the effectiveness of a mission, organization, or item of equipment. Involves application of threat analysis to specific mission, organization, or item of equipment within context of a military operation.

Threat data

Threat data includes technical information on threat systems as well as information on the formations and capabilities of potential adversaries. Threat data includes raw and processed information. The intelligence community must validate threat data for formal program usage.

Threat integration staff officer

An Army officer designated as the HQDA threat integrator for designated mission areas, programs, and/or materiel systems. Usually assigned along Battlefield Operating System lines, based upon their Branch and operational experience. Complements the ASA (ALT) staff officer; DCS, G-3/5/7 requirements staff officer; DCS, G-8 synchronization staff officer, and the PEO/PM or a representative. Encourages close coordination for threat support by the intelligence community with Army commands, PEOs, and ARSTAF RDA and T&E agencies to ensure the timely integration of threat into technology programs and the materiel development and acquisition process. Supplements existing management activities but does not relieve ARSTAF agencies, PEO/PMs and Army commanders of established responsibilities. DCS, G-2 is the approving authority for either establishing or ending TISO monitoring of systems. Generally, a TISO will be assigned to all programs designated as ACAT I or II, or that appear on the OSD or Congressional program oversight lists. Other systems and programs will be assigned TISO monitoring on an "as required" basis with DCS, G-2 approval.

Threat representation

Models, simulators, stimulators, simulations, data, targets, actual threat systems, emulators, surrogates, foreign materiel, or systems that replicate foreign military weapon systems or civilian devices used in an adversarial military role. Validation and accreditation is required for threat representations that support formal program analysis, assessment, or test and evaluation. Procedures for VV&A are established in DA Pam 5-11 (for M&S) and DA Pam 73-1 (for T&E).

Threat simulator

A threat simulator is a DOD-developed system that exhibits one or more operational characteristics/physical signatures of an actual threat system for use in testing and evaluation and in training. Threat simulators provide physical representations of threat systems for use in developmental testing, operational testing and training. Threat simulators used in testing that supports an MDR must be validated and accredited.

Threat steering group

Executive level group formed to manage intelligence support requirements to support the combat and materiel development process throughout entire life cycle of systems or processes.

Threat support activity

Provides threat support to a combat, materiel, or systems developer (such as TMs in TRADOC; FIOs in AMC and SMDC; and DCS, G-2 for HQDA).

Threat test support package

A test specific document that provides a comprehensive description of threat to U.S. systems being tested and targets the system will engage.

Validated On-line Life-cycle Threat

The authoritative threat assessment tailored for and normally focused on one specific program and authorized for use in the Defense Acquisition Management process.

Validation

The process used to identify, document, and analyze the critical technical and performance differences between a threat entity and the associated threat system. Validation is the process used to determine whether a threat entity provides a sufficiently realistic representation of the corresponding threat system for use in T&E.

Validation (regional structures)

The process of certifying that a structure is constructed in an appropriate manner to ensure consistent, accurate data can be determined from the T&E event for a wide variety of munitions. This is critical to ensure that weapons and munitions' effectiveness (lethality) can be compared across the board to a set of quantifiable standards. A thorough knowledge of structures and weapons effects is essential to ensure the correct system is employed. This cannot be done without validation of regional structures.

Validation (requirements)

The process of certifying that a customer's requirements are consistent with and necessary for the accomplishment of the customer's mission.

Validation (threat documentation)

Within the context of this regulation, the term "validation" signifies formal or official certification of a VOLT or other product for threat support to acquisition. Validation certifies the assessment or product has been properly prepared and coordinated based upon appropriate primary threat documentation and best available data. VOLTs for all ACAT ID programs must be validated by DIA. VOLTs for ACAT IC, ACAT II, and OSD oversight programs must be validated by DCS, G-2 (DAMI-FIT). VOLTs for non-oversight ACAT III programs must be validated by TRADOC G-2 or AMC G-2 depending on the agency responsible for revision.

Validation and accreditation plan for threat simulators and targets

Plan that defines and prescribes concepts, processes, policies, and procedures employed in validation and accreditation of threat simulators, targets, and target arrays.

Validation office

A small office or a self-contained intelligence organization that has been established for each service, each unified command and the National Military Intelligence Production Center.

Validation working group

Group formed to determine whether threat simulator or target provides sufficiently realistic representation of corresponding threat system and justifies the start or continuation of its development, acceptance, or modification. Chartered by DUSA (TE).

UNCLASSIFIED

PIN 004110-000