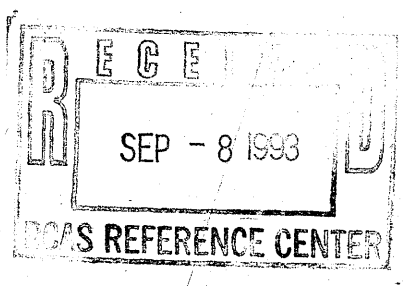
Army Regulation 381-11

Apr 6, 93

Military Intelligence

Threat Support to U.S. Army Force, Combat, and Materiel Development



Headquarters
Department of the Army
Washington, DC
1 March 1993

SUMMARY of CHANGE

AR 381-11
Threat Support to U.S. Army Force, Combat, and
Materiel Development

This revision--

- Delineates threat support policies according to Department of Defense Instruction 5000.2, Defense Acquisition Management Policies and Procedures (para 1-5).
- Identifies threat support responsibilities at Department of the Army and major Army command levels (para 1-4).
- Identifies threat support documentation requirements using the same matrix format found in Department of Defense Instruction 5000.2 (table 1-1).
- Requires annual system threat assessment report updates (paras 2-8b(1)(c), 2-8b(2)(c), and 2-8b(3)(c).
- Expands the scope of the threat support process and documentation requirements through the use of flow charts and diagrams (figs 2-1 through 2-6).
- Requires threat support activities to follow a standard system threat assessment report format (app B).

Headquarters
Department of the Army
Washington, DC
1 March 1993

*Army Regulation 381–11

Effective 1 April 1993

Military Intelligence

Threat Support to U.S. Army Force, Combat, and Materiel Development

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:

MILTON H. HAMILTON
Administrative Assistant to the Secretary of the Army

History. This UPDATE printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation implements Department of Defense Instruction 5000.2 (Defense Acquisition Management Policies and Procedures), Department of Defense Manual 5000.2–M (Defense Acquisition Management Documentation and Reports Manual) and Defense Intelligence Agency Regulation 55–3 (Threat Support for Major Defense Acquisition Programs). It governs threat support to the U.S. Army force, combat, materiel, and training development process. It also provides guidance on the development of threat support programs, use of approved intelligence products, responsibilities of the Office of the Deputy Chief of Staff for Intelligence threat integration staff officers, and the functions of threat coordinating groups.

Applicability. This regulation applies to elements of the Active Army engaged in force, combat, materiel, and training development activities. It does not apply to the Army National Guard or the U.S. Army Reserve nor to other developers, testers, and modelers not specifically identified in this regulation except to ensure that operations security, foreign intelligence, and threat matters for their programs are addressed according to specific program development regulations.

Proponency and exceptions. The proponent of this regulation is the Deputy Chief of Staff for Intelligence (DCSINT). Subject to the reservations set out below, the DCSINT has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The DCSINT may delegate this approval authority, in writing, to a deputy director within the proponent agency who holds the grade of colonel or the civilian equivalent.

Internal control systems. This regulation is not subject to the requirements of AR 11–2. It does not contain internal control provisions.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA (DAMI–FIT), WASH DC 20310–1086.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended changes to Publications and Blank Forms) directly to HQDA (DAMI–FIT), WASH DC 20310–1086.

Distribution. Distribution of this publication is made in accordance with the requirements on DA Form 12–09–E, block number 2181, intended for command levels D for the Active Army, none for the Army National Guard, and none for 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*
Policies • 1–5, *page 3*

Chapter 2
Threat Support, *page 4*

Section I
Threat support programs, page 4
General • 2–1, *page 4*
Intelligence products • 2–2, *page 5*
Threat simulators and targets • 2–3, *page 5*
Threat simulation within Army analyses • 2–4, *page 5*
Threat integration staff officer • 2–5, *page 6*
Threat coordinating groups • 2–6, *page 6*
Threat assessments • 2–7, *page 7*
System Threat Assessment Report • 2–8, *page 7*
System threat assessment • 2–9, *page 8*
Threat test support package • 2–10, *page 8*
Cost and operational effectiveness analysis • 2–11, *page 9*
Special access programs • 2–12, *page 9*

Section II
Army Studies, page 9
Study directives and plans • 2–13, *page 9*
Study advisory group • 2–14, *page 9*
Procedures for HQDA-directed studies • 2–15, *page 9*

Appendixes
A. References, *page 13*
B. System Threat Assessment Report Format, *page 13*
C. TTSP Format Guidance, *page 17*

Table List

Table 1–1: Threat Support Responsibilities Matrix, *page 3*

Figure List

Figure 2–1. Threat support to force, combat, and materiel development, *page 10*
Figure 2–2. Threat support to developmental and operational testing, *page 10*

*This regulation supersedes AR 381–11, 12 March 1986.

Figure 2–3. STAR production & validation process (ACAT I Programs through MS I)., *page 11*
Figure 2–4. STAR production & validation process (ACAT I Programs beyond MS I.), *page 11*
Figure 2–5. Threat test support package (TTSP) validation process, *page 12*
Figure 2–6. Cost and operational effectiveness analysis (COEA) validation process, *page 12*
Figure B–1. Critical intelligence parameter (CIP) examples, *page 16*
Figure B–2. STAR Cover page (format), *page 16*

Glossary

Index

Chapter 1
Introduction

1–1. Purpose

This regulation prescribes policies, responsibilities, and procedures for providing threat support to the Army's force, combat, materiel, and training development processes. It provides guidance on the purpose, content, and focus of threat assessment used in support of force, combat, materiel, and training development activities. This regulation is intended to ensure that threat support helps guide the Army's force modernization efforts.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities

a. The Assistant Secretary of the Army for Research, Development, and Acquisition (ASA(RDA)) will—

(1) Coordinate with Office of the Deputy Chief of Staff for Intelligence (ODCSINT) on research, development, and acquisition requirements for threat support.

(2) Ensure that the integrated program summary (IPS) prepared to support milestone decision reviews for acquisition category (ACAT I) and II systems contains or references Department of the Army (DA)-approved threat assessments.

(3) Provide for the integration of threat support in all study directives and guidance documents for which ASA(RDA) is responsible from earliest concept stages.

(4) Coordinate with ODCSINT to ensure that intelligence assets are programmed to support long-range planning initiatives, and that plans reflect consideration of the threat.

(5) Coordinate with ODCSINT to ensure that approved threat statements and appropriate threat guidance and policies are present in the Materiel Change Management Program.

(6) Participate in DA-level threat coordinating groups (TCGs) for coordination of threat support to the force, combat, and materiel development process, as appropriate.

(7) Ensure that approved intelligence data and threat assessments are integrated into developmental testing (DT).

(8) Through Simulations, Training, and Instrumentation Command (STRICOM), AMC, exercise management responsibility for Army threat simulators and Army target programs in support of development programs other than those provided for by the U.S. Army Space and Strategic Defense Command (SSDC).

(9) Review system threat assessment reports (STARs) for system description.

b. The Deputy Chief of Staff for Intelligence (DCSINT) will—

(1) Establish threat support policy and guidance.

(2) Approve threat documentation designated for Army Systems Acquisition Review Council (ASARC) or Defense Acquisition Board (DAB) decisions, studies, and testing in support of the DA decision process. (See table 1-1 for threat support responsibilities.)

(3) Review and monitor the threat support process to ensure consistent application of threat in support of ACAT I and II programs, selected Director, Office of the Secretary of Defense Test and Evaluation (OSD T&E) oversight systems, DA-directed studies, and selected combat developer-directed studies.

(4) Provide for representation to special task forces (STFs), special study groups (SSGs), study advisory groups (SAGs), General Officer Steering Committees, and other study efforts requiring threat consideration.

(5) Serve as a member of the ASARC.

(6) Establish and chair DA TCGs for ACAT I and II systems and program objective memorandum (POM)-related study programs. Determine the appropriateness of establishing DA TCGs for other programs or studies. Adjust responsibilities for threat document production, in coordination with MACOMs, to include STAR preparation, as required.

(7) Review and approve all aspects of threat portrayed during development and major revisions of the U.S. Army Training and Doctrine Command (TRADOC) standard low resolution scenarios.

(8) Coordinate threat support and assessments with other Service participants prior to submission to the Defense Intelligence Agency (DIA) for validation for joint programs (JPs) in which the Army is the lead Service. For JPs in which the Army is a participant, but not the lead Service, coordinate threat support with the designated lead Service.

(9) Provide Threat Integration Staff Officer (TISO) representation in appropriate Test Integration Working Groups (TIWGs) and Threat Accreditation Working Groups (TAWGs) under TIWG auspices for ACAT I and II programs and selected OSD T&E oversight systems.

(10) Represent the Army at DOD and DIA briefings and coordinate briefing DIA on threat assessments used by the Army to define the threat in the mission need statement (MNS), operational requirements document (ORD), test and evaluation master plan (TEMP), IPS, cost and operational effectiveness analysis (COEA), and STAR, as required.

(11) Ensure that necessary data bases are developed and maintained to facilitate management of the threat support process.

(12) Coordinate, as necessary, with national intelligence agencies and Army intelligence production centers for threat support.

(13) Prepare Intelligence Reports for ACAT IC (milestone decision reviews (MDRs) II–IV) and II (MDRs I–IV) programs. (See table 1–1.)

(14) Assist developers in development of intelligence production requirements (IPRs). (ODCSINT, DAMI–FIP.)

(15) Monitor responsiveness to IPRs. (ODCSINT, DAMI–FIP.)

(16) Validate and approve Army IPRs and submit production requirements to DIA for levy on other DOD intelligence producers when intelligence data required falls into those organizational charters. (ODCSINT, DAMI–FIP.)

(17) Publish listings of approved intelligence products at least annually. (ODCSINT, DAMI–FIP.)

c. The Deputy Chief of Staff for Operations and Plans (DCSOPS) will—

(1) Coordinate with ODCSINT on requirements for threat support to STFs, SSGs, study directives, analyses, and guidance documents.

(2) Participate in DA-level TCGs for coordination of threat support to the force, combat, and materiel development process, as appropriate.

(3) Coordinate with ODCSINT on appropriate threat guidance and policies for COEAs.

(4) Coordinate with ODCSINT for training support requirements, including threat guidance and foreign materiel for training (FMT).

(5) Review STARs for mission and force description adequacy.

d. The Commanding General (CG), AMC, will—

(1) Serve (through the designated foreign intelligence officer (FIO)) as the program executive officer (PEO) or project manager's (PMs) sole source of intelligence support through the entire life cycle of assigned programs.

(2) Prior to MDR I, coordinate on all TRADOC-prepared STARs.

(3) Assume responsibility for ACAT I and II STAR production from TRADOC, coordinate AMC-produced STARs with TRADOC, and forward the coordinated STARs to ODCSINT for review and approval subsequent to MDR I.

(4) Update STARs annually, or when significant changes in either the threat or U.S. system specifications and characteristics occur subsequent to MDR I. Obtain approval and validation for changes, revisions, or updates according to table 1–1.

(5) Prepare, in coordination with appropriate PEO or PMs, threat statements for IPS, TEMP, request for proposal (RFP) and

in-process reviews for ACAT I and II systems. Obtain ODCSINT approval for these threat statements.

(6) Prepare, in coordination with TRADOC, the system threat assessment (STA) for ACAT III and IV systems subsequent to MDR I, unless specifically waived.

(7) Prepare, in coordination with PEO, PM, or developer, threat statements for IPS, RFP, and TEMPs for all ACAT III and IV systems. Provide information copies to ODCSINT.

(8) Identify and submit command threat support requirements.

(9) Document and submit critical intelligence parameters (CIPs) and related IPRs identified by the PEO, PMs, and other developers.

(10) Participate in TIWGs to ensure integration of approved threat in developmental and operational testing; prepare threat test support packages (TTSPs) for developmental tests to ensure realistic threat portrayals; and coordinate TTSP development with TRADOC.

(11) Participate in validation working groups (VWGs), TAWGs, and DA-level TCGs, as required.

(12) Establish appropriate TCGs for ACAT III and IV systems subsequent to MDR I, in coordination with TRADOC.

(13) Review and approve threat inputs in AMC models, to include functional models.

(14) Incorporate foreign intelligence and threat in development systems under CG, AMC cognizance.

(15) Determine threat documentation requirements for development programs under AMC purview and provide requisite support.

(16) Provide threat support and guidance to technology base programs.

(17) Provide DIA-validated threat and intelligence information to contractors according to AR 381–1, in support of materiel development contracts.

(18) Be responsible, through STRICOM, for engineering, development, acquisition, fielding, and capability accounting for Army targets, threat simulators, and major range instrumentation, other than those provided for by SSDC. Develop simulators or surrogates in lieu of foreign materiel as directed by STRICOM. Participate in VWGs and TAWGs.

(19) Prepare intelligence reports according to table 1–1.

(20) Coordinate with ODCSINT for approval of all threat surrogate system data usage in support of Army modeling efforts.

e. The CG, TRADOC will—

(1) Prepare, review, coordinate with AMC, and forward to ODCSINT for DA approval all threat statements developed for each MNS and ORD for ACAT I and II and selected OSD T&E oversight systems.

(2) Prepare, review, coordinate with AMC, and approve all threat statements developed for each MNS and ORD for ACAT III and IV systems. Provide information copies to ODCSINT (DAMI–FIT).

(3) Prepare, coordinate with AMC, and forward all ACAT I and II STARs to ODCSINT for review and approval within 150 days after an MDR 0.

(4) Update STARs annually, or when significant changes in either the threat or U.S. system specifications and characteristics occur through MDR I. Obtain approval and validation for changes, revisions, or updates according to table 1–1.

(5) Coordinate on all AMC-prepared STARs subsequent to MDR I.

(6) Develop command threat support requirements.

(7) Develop, produce, and coordinate the threat portion of the TRADOC standard low-resolution scenarios and forward to ODCSINT for approval.

(8) Provide for threat representation at each SSG and identify threat support requirements to ODCSINT.

(9) Participate in appropriate TIWGs, TAWGs, and DA-level TCGs.

(10) Establish and chair appropriate TCGs in coordination with AMC, to provide threat support to ACAT III and IV systems through MDR I.

(11) Prepare, in coordination with AMC, the STA for ACAT III and IV systems through MDR I, unless specifically waived.

(12) Provide threat integration representation to TIWGs and TAWGs for ACAT III and IV systems in coordination with AMC.

(13) Prepare TTSPs for operational testing in response to stated tester requirements. Ensure that threat portrayals are sufficiently realistic to satisfy test needs. Approve TRADOC-developed TTSPs for operational testing. Conduct on-site approval or validation of threat portrayals in operational testing, as appropriate. Coordinate TTSP development with AMC. Coordinate threat approval and validation with ODCSINT on ACAT I and II programs. Forward TTSPs for approval according to table 1–1.

(14) Review and approve threat used in TRADOC-sponsored studies, to include COEAs, models, scenarios, data, and systems. Ensure that threat data used is DIA-approved and is properly documented.

(15) Prepare and approve the intelligence report for ACAT III and IV systems through MDR I. See table 1–1.

f. The Commander, Intelligence and Security Command (INSCOM), will acquire foreign materiel for scientific and technical intelligence (S&TI) exploitation program and for use in developing simulators and surrogates, or for use as targets in support of developmental and operational tests.

g. The CG, U.S. Army Operational Test and Evaluation Command (OPTEC), will—

(1) Coordinate test planning with the appropriate threat approval authority (table 1–1) to ensure that a validated threat will be used in planning all OPTEC-managed operational activities.

(2) Participate in TCGs to ensure that threat requirements to support operational testing are identified as early as possible after program initiation.

(3) Review and monitor all OPTEC-managed operational testing activities and coordinate with TRADOC to ensure that the threat represented in testing conforms, to the extent feasible, with the validated threat.

(4) Maintain and operate threat simulators and targets in support of Army testing and training programs in a manner commensurate with threat force doctrine, tactics, and operating procedures.

(5) Participate in VWGs, TAWGs, and DA-level TCGs, as appropriate.

(6) Employ targets, threat simulators, and target arrays used in Army operational testing according to the TTSP.

h. The Commanders, U.S. Army Foreign Science and Technology Center (FSTC) and Intelligence and Threat Analysis Center (ITAC), will—

(1) Produce and disseminate general, scientific, and technical intelligence for current and future or follow-on threat systems and qualify and document threat assessments and data when intelligence is either incomplete or absent.

(2) Produce intelligence documents and S&TI quantitative data (in automated format, when possible) to support force, combat, and materiel development programs, to include special access programs (SAPs).

(3) Participate in TCGs to support the force, combat, and materiel development process.

(4) Assist in the development of threat and its application in selected combat and materiel developers' acquisition programs, studies, developmental and operational tests, combat training center (CTC) opposing forces (OPFOR) portrayal, and combat simulations (with emphasis on models in the Army Model and Simulation Management Program (AMSMP) hierarchy as outlined in AR 5–11) and war games. Assist and focus on model sensitivity, decision logic performance, data input, scenario use, tactics, and doctrine.

(5) Provide threat and simulator data and assessments, as required, in support of the Army Validation and Accreditation Plan for Threat Simulators and Targets. Participate in VWGs and TAWGs.

(6) Provide representatives to working groups and TCGs formed to support DA and MACOM-directed studies and analyses.

(7) Develop and maintain threat data bases as directed by ODCSINT.

(8) Develop threat analysis and forecasting methodologies.

(9) Function as the authority for all threat surrogate system data usage in support of Army analytic modeling efforts in coordination with ODCSINT.

i. The Director, Test and Evaluation Management Agency (TEMA), will—

(1) Establish Army validation and accreditation policy for threat simulators and targets.

(2) Charter VWGs.

j. Director, U.S. Army Concepts Analysis Agency (CAA), will—

(1) Develop, in coordination with ODCSINT and ODCSOPS, threat support requirements for theater-level studies and analyses.

(2) Participate in DA-level TCGs involving force development issues.

(3) Coordinate with ODCSINT to ensure provision of appropriate threat support to DA-sponsored force development studies.

(4) Ensure that threat documentation used in DA-sponsored studies is made available for review and approval by ODCSINT.

k. Program executive officers (PEO), program managers (PM), and developing agencies will—

(1) Use DIA-validated threat in all development programs.

(2) Obtain intelligence and threat support and approval through the supporting AMC FIO.

(3) Identify to the supporting AMC FIO all threat and intelligence requirements, including those for threat statements for system program and decision documentation.

(4) Incorporate validated and approved threat statements in each IPS, RFP, and TEMP for all systems.

(5) Develop, in coordination with the supporting FIO and TRADOC, CIPs for each program.

(6) Participate in TCGs and TAWGs, as appropriate.

(7) Address threat risk management in presentations to the ASARC and DAB.

(8) Chair TIWGs (PM responsibility).

l. Other developers, testers and modelers not specifically identified in this regulation will ensure that OPSEC, multi-discipline counterintelligence (MDCI), foreign intelligence, and threat matters for their programs are addressed according to specific program development regulations. Specific organizations identified in AR 70–1 with development responsibility include: U.S. Army Health Services Command, U.S. Army Information Systems Command (also, AR 25–1), U.S. Army Corps of Engineers, U.S. Army Criminal Investigation Command, U.S. Army Strategic Defense Command, and the U.S. Army Medical Research and Development Command.

1–5. Policies

a. DOD Instruction (DODI) 5000.2 contains guidance on threat support to materiel acquisition; it states that the objective is to ensure that each system developed is mission capable in its intended operational environment during its expected life.

b. DIAR 55–3 contains guidance on threat support to ACAT I programs for systems acquisition, and refers to procedures for ACAT II through IV programs.

c. Policies for threat support to training, force, combat, and materiel development as they pertain to the Army are listed below.

(1) Consideration of threat is a command responsibility. Commanders, PEOs/PMs, other materiel developers, combat developers, to include TRADOC system managers (TSMs), and study directors at all levels will ensure via utilization of appropriate intelligence/threat authority that approved threat is applied and integrated into force, combat, materiel, and training development programs.

(2) Threat, which includes scientific and technical intelligence (characteristics, capabilities, and limitations of foreign equipment) and general intelligence (organization, doctrine, force structure, and tactics of threat forces), will only be derived from data sources and threat data bases validated by DIA. The analysis of approved intelligence data to meet threat requirements is the responsibility of the proponent threat support office.

(3) Combat and materiel development commands will prepare required threat documentation, to include threat assessments, to support specific combat, materiel, and training development activities for which those commands are responsible.

(4) The FSTC and ITAC will provide intelligence support, when approved by ODCSINT, in response to requirements approved by the senior intelligence officer (SIO) (or ODCSINT, as appropriate) of the requesting Major Army Command (MACOM) or agency. The Missile and Space Intelligence Center (MSIC) and Armed Forces Medical Intelligence Center (AFMIC) will provide intelligence support in accordance with DIA intelligence support policies. They will provide intelligence information for all force, combat and materiel development-related activities including the Planning, Programming, and Budgeting System (PPBS); scenario development; ORD; COEA; developmental tests; and operational tests. ODCSINT will validate this information.

(5) The threat support activity (such as the Threat Manager's (TM) office for TRADOC; the Foreign Intelligence Directorate for Army Materiel Command (AMC); and SSDC Intelligence Officer) of each command and activity involved in the force, combat, and materiel development process will review and approve threat assessments written in support of command missions before forwarding them to the next higher level of command. (NOTE: When the term AMC is used hereafter, both AMC and SSDC are included, unless otherwise stated.)

Table 1–1
Threat Support Responsibilities Matrix

Document	Type of review	Milestone 0	I	II	III	IV	Threat prepared by	Threat approved/ validated by
ACQUISITION CATEGORY ID REQUIREMENTS								
MNS	ASARC/DAB	X					CBT DEV—Threat Manger	DA DCSINT/DIA
ORD	ASARC/DAB		X	X	X	X	CBT DEV—Threat Manager	DA DCSINT/DIA
IPS	ASARC/DAB		X	X	X	X	MAT DEV	DA DCSINT/DIA
COEA [1]	ASARC/DAB		X	X	X	X	CBT DEV	DA DCSINT/DIA
STAR	ASARC/DAB		X	X	X	X	CBT DEV—Threat Manager [2] MAT DEV—Foreign Intel Off [3]	DA DCSINT/DIA
TEMP	ASARC/DAB		X	X	X	X	MAT DEV—Foreign Intel Off	DA DCSINT/DIA
TTSP	ASARC/DAB			X	X	X	CBT DEV [4] MAT DEV [4]	DA DCSINT/DIA

Table 1–1
Threat Support Responsibilities Matrix—Continued

Document	Type of review	Milestone O	I	II	III	IV	Threat prepared by	Threat approved/ validated by
Intelligence Report	DAB	X	X	X	X	X	DIA	Director, DIA
				ACQUISITION CATEGORY IC REQUIREMENTS				
MNS	ASARC/DAB	X					CBT DEV—Threat Manager	DA DCSINT/DIA
ORD	ASARC/DAB		X	X	X	X	CBT DEV—Threat Manager	DA DCSINT/DIA [2] DA DCSINT [3]
IPS	ASARC/DAB		X	X	X	X	MAT DEV	DA DCSINT/DIA [2] DA DCSINT [3]
COEA [1]	ASARC/DAB [2] ASARC [3]		X	X	X	X	CBT DEV	DA DCSINT/DIA [2] DA DCSINT [3]
STAR	ASARC/DAB [2] ASARC [3]		X	X	X	X	CBT DEV—Threat Manager [2] MAT DEV—Foreign Intel Off [3]	DA DCSINT/DIA [2] DA DCSINT [3]
TEMP	ASARC/DAB [2] ASARC [3]		X	X	X	X	MAT DEV—Foreign Intel Off	DA DCSINT/DIA [2] DA DCSINT [3]
TTSP	ASARC/DAB [2] ASARC [3]			X	X	X	CBT DEV [4] MAT DEV [4]	DA DCSINT/DIA
Intelligence Report	DAB [2] ASARC [3]	X	X	X	X	X	DIA DA ODCSINT	Director, DIA [2] DA DCSINT [3]
				ACQUISITION CATEGORY II REQUIREMENTS				
MNS	ASARC	X					CBT DEV—Threat Manager	DA DCSINT
ORD	ASARC		X	X	X	X	CBT DEV—Threat Manager	DA DCSINT
IPS	ASARC		X	X	X	X	MAT DEV	DA DCSINT
COEA [1]	ASARC		X	X	X	X	CBT DEV	DA DCSINT
STAR	ASARC		X	X	X	X	CBT DEV—Threat Manager [2] MAT DEV—Foreign Intel Off [3]	DA DCSINT
TEMP	ASARC		X	X	X	X	MAT DEV—Foreign Intel Off	DA DCSINT
TTSP	ASARC			X	X	X	CBT DEV— [4] MAT DEV [4]	DA DCSINT/
Intelligence Report	ASARC	X	X	X	X	X	DA ODCSINT	DA DCSINT
				ACQUISITION CATEGORY III/IV REQUIREMENTS				
MNS	IPR	X					CBT DEV—Threat Manager	TRADOC
ORD	IPR		X	X	X	X	CBT DEV—Threat Manager	TRADOC
IPS	IPR		X	X	X	X	MAT DEV	AMC
COEA [1]	IPR		X	X	X	X	CBT DEV	TRADOC
STA	IPR		X	X	X	X	CBT DEV—Threat Manager [2] MAT DEV—Foreign Intel Off [3]	TRADOC AMC [3]
TEMP	IPR		X	X	X	X	MAT DEV—Foreign Intel Off	TRADOC
TTSP	IPR			X	X	X	CBT DEV [4] MAT DEV [4]	TRADOC [2] AMC [3]
Intelligence Report	IPR	X	X	X	X	X	TRADOC [2] AMC [3]	TRADOC [2] AMC [3]

Notes:

[1] Approval/validation occurs early in COEA process—vice concurrences to final, published COEA document.

[2] Through MDR I.

[3] Beyond MDR I.

[4] CBT DEV (operational testing), MAT DEV (developmental testing).

Chapter 2
Threat Support

Section I
Threat support programs

2–1. General

a. The purpose of threat support programs is to ensure that force, concepts, doctrine, training, organization, and materiel systems that most effectively and efficiently respond to the evolving threat environment are developed. Threat support must be timely, consistent, and continuous to achieve this purpose.

(1) Timeliness ensures that threat considerations are provided to combat and materiel developers throughout the combat and materiel development cycle in order to properly influence the requirement for and development of force, concepts, doctrine, training, organization, and materiel systems.

(2) Consistency requires that multiple users work from a standard, approved intelligence baseline.

(3) Continuous threat support means that the impact of the threat is considered throughout the life cycle of a materiel system, from identification of a deficiency, through and including post-development product improvements. It ensures that organizations and doctrinal developments are supported throughout their conceptual phases and after implementation.

b. A threat support program consists of the following:

(1) Validated Department of Defense (DOD), national intelligence community, and Army intelligence products (documents, data bases, models, concepts, and scenarios).

(2) A procedure designed to respond to intelligence requirements that are not fulfilled by published intelligence products.

(3) Procedures used to apply threat data in a study or simulation or integrate threat into the planning and execution of a developmental or operational test.

c. Threat support programs will be initiated early in the combat development process. Early support ensures that the impact of the threat is considered and applied during the process, which may lead to the identification of a requirement for a specific materiel system or a change in organization, doctrine, or training. (Figs 2–1 and 2–2 depict threat support throughout a program's life and testing cycles.)

d. Threat support programs also will be initiated to support the development of all force, combat, and materiel development programs and studies.

e. At the start of a study or project, the proponent will identify threat support requirements. The threat support activity at each command level is responsible for coordinating and providing threat support to combat and materiel developers; and for the application of the threat in support of programs and studies conducted within the command.

f. The relationship between a U.S. system or program and the specific threat is dynamic and reflects changes in tactics, doctrine, and technological advancements. The threat support activity of proponent commands will maintain a life cycle threat audit trail for each program.

g. The basis or start point for developing the threat in support of a specific program, system, or study is threat data sources, to include the threat data base, validated by DIA. The ODCSINT TISO will coordinate and assist in ensuring threat support for the development process.

h. Specific guidance for the preparation of threat assessments is contained in paragraph 2–7.

2–2. Intelligence products

Intelligence products are publications, automated data bases, and electronic media that address foreign force capabilities in the near term (0–5 years), mid term (5–10 years) and far term (10–20 years). DIA-validated data sources will be used in developing threat assessments for satisfying system-specific threat support requirements. To ensure consistency throughout the Army intelligence and development communities, ODCSINT will publish a bibliography of approved intelligence products at least annually. The bibliography is not intended to be all inclusive; in the absence of DIA-validated source documentation, users are not restricted from examination of other sources that may answer threat support requirements for specific programs or systems. However, if other sources are used, their use will be documented with justification in the program or system-specific threat bibliography and approved through appropriate intelligence channels. These baseline products are essential for sustaining the provision of consistent threat throughout the study and acquisition process, and represent the start point for assessments prior to initiating specific requests for support.

2–3. Threat simulators and targets

a. Threat simulators and targets to be used in testing to represent specific threat systems are subject to processes and procedures of established U.S. Army validation and accreditation policies.

b. Validation is the process used to determine whether a simulator or target provides a sufficiently realistic representation of a corresponding threat system; validation justifies the start or continuation of development, acceptance, or modification of a simulator or target to restore or improve its capabilities to conform with current DIA-approved intelligence products. Validation is accomplished by TEMA-chartered VWGs comprised of representatives of user, intelligence, and simulator and target developer organizations.

c. Accreditation is the process used to determine the suitability of threat simulators, targets, and target arrays for a specific test application. Accreditation of ACAT I through IV programs is accomplished via the TAWG process. The TAWG accredits use; develops simulator, target, and target array employment guidance; and identifies simulator, target, and target array limitations. TAWG membership consists of representatives of the test and evaluation, intelligence, simulator and target developer, and project manager organizations.

2–4. Threat simulation within Army analyses

Army analyses make extensive use of computerized combat simulations. These analyses are used to evaluate capabilities and determine user and resource requirements in the context of complete force interactions and varying battlefield requirements, and, as such, use simulations to capture the principal representations of the threat. To ensure the validity of Army analyses, computerized combat simulations must represent threat force combat, combat support, and combat service support in a consistent manner. The agency conducting an analysis must know the appropriate models to use as well as their strengths, weaknesses, and limitations. The validity of threat force activity is a function of data inputs, model sensitivity, tactical decision rules, and scenarios used in the various models employed to conduct the analysis. To achieve threat consistency, commonality and accuracy within models, apply the following procedures:

a. Combat simulation use. MACOMs and supporting intelligence officers will establish procedures ensuring that data used in simulations are accurate and current, and the threat representations in the supporting models depict events correctly. TCGs and existing data bases will be used to satisfy the requirement for current and accurate data inputs. Problem areas and events that cannot be portrayed accurately will be fully documented for decision through the chain of command. Deviations from validated scenarios and threat data will be forwarded to ODCSINT for approval through the chain of command. Problems and deviations will be identified at each MDR meeting or in-process review meeting for consideration by study members. Documentation will include, as a minimum, assumptions, decision rules, uses, limitations, data required, and data currently stored.

b. Intelligence data. Products identified in paragraph 2–2 will be used for threat analyses and subsequent assessments. Deviations from the intelligence contained within these references may be used for interactive analyses by Army analytic activities; however, such excursions will be documented in the assumption portion of all analyses. Study directors and decisionmakers at all levels will be informed of such deviations and their potential impact.

c. Scenario development. Army analytic agencies require basic guidelines regarding precursory events, timelines, and threat employment concepts, in addition to data on threat force structure and weapon systems characteristics. To achieve accuracy, commonality, and consistency of the threat in scenarios, the following guidelines apply to the development of threat force scenarios:

(1) The annual DOD Defense Planning Guidance (DPG) provides the Services with a plan for development of necessary military capabilities to maintain the Nation's security. It will be used to begin development of scenarios intended to support force and materiel development processes. The DPG contains a planning scenario intended to—

(a) Provide a general illustrative sequence of events on which to base force development planning for the future 10-year timeframe and to assess risk to programmed forces.

(b) Provide a common set of US friendly force assumptions for use by the Services in computing readiness, sustainability, mobility, and modernization of resources.

(2) ODCSINT will review the DPG assumptions for impact on threat and provide scenario development guidance at the beginning of each year.

(a) TRADOC. TRADOC standard scenarios will be used in studies and analyses to identify Army force modernization needs encompassing doctrine, organization, training, leadership, and materiel. Threat scenarios developed by TRADOC and approved by ODCSINT through timely in-process reviews will serve as the base for Army combat and materiel development studies, unless otherwise directed by DA. TRADOC will use threat data based on DIA-approved sources to develop standard scenarios. In the absence of approved data, data derived from nonapproved sources will be highlighted and submitted for approval through intelligence channels. TRADOC standard scenarios will be based on ODCSINT-developed operational concepts. Army schools, centers, and activities involved in force and materiel development will use these approved scenarios for analyses. If threat excursions are employed, they will be highlighted clearly in study reports.

(b) CAA. ODCSINT guidance to CAA on global force employment scenarios will be based on specific study and model requirements. Scenarios developed will provide a common threat basis for annual planning and programming studies conducted for the Army Staff (ARSTAF). ODCSINT will provide data to CAA and will review results of analyses as appropriate, to ensure that intelligence data on threat doctrine and force employment are logical and consistent.

d. Combat simulation development. Combat simulations being developed will be fully documented and reviewed. MACOMs, contract monitors, and intelligence offices supporting these efforts will establish procedures for reviewing threat data and decision rules for accuracy, currency, and correct portrayal of threat activities and events. Existing data bases and intelligence resources will be used to satisfy this requirement. AR 381–19 outlines procedures for tasking intelligence resources in the event available intelligence products are not sufficient. On request, FSTC and ITAC will assist MACOMs in the development and application of threat portrayed in MACOM models.

2–5. Threat integration staff officer

a. A TISO is designated to function as the HQDA threat integrator for designated mission areas, programs and materiel systems. The TISO represents ODCSINT on all aspects of threat support throughout the life cycle or study process. The TISO system complements the ODCSOPS system integrator, ASA(RDA) staff officer, and the PEO representative, and is designed to foster close coordination among the intelligence community and MACOMs, PEOs, and ARSTAF agencies to ensure the timely integration of threat into the materiel development and acquisition process. The TISO system supplements existing management procedures but does not relieve ARSTAF agencies, PEO/PMs and MACOMs of established responsibilities.

b. The TISO performs the following functions:

(1) Represents the DCSINT and serves as the primary DA Staff point of contact for threat integration.

(2) Coordinates implementation of Army policy relating to threat support.

(3) Establishes and manages TCGs for ACAT I and II systems, POM-related studies, and selected DA studies and analyses.

(4) Provides timely DA threat guidance to those threat support activities and commands responsible for combat and materiel development.

(5) Coordinates DA approval for all threat assessments, written or oral, to support ACAT I and II systems and selected studies and analyses.

(6) Coordinates DIA validation of threat assessments written to support systems requiring DAB decision review.

(7) Directs the threat support process to ensure timely and consistent application of intelligence to ACAT I and II systems and selected studies and analyses.

(8) Adjusts functions for threat document production, to include STAR preparation, as required.

(9) Reviews and approves CIPs that impact on the effectiveness, survivability, or security of the U.S. system, as well as reviews and approves the IPRs that support CIPs.

(10) Coordinates appropriate ODCSINT participation in STFs and SSGs for MACOM-managed studies.

(11) Coordinates with DOD, DIA, and other Service intelligence agencies on all aspects of threat support to Army-specific or joint Service acquisition programs.

(12) Reviews threat statements and assessments contained in ARSTAF requirements, decision, and program documents in coordination with ODCSOPS and ASA(RDA).

(13) Represents ODCSINT on all ACAT I, II, and selected OSD T&E oversight system TIWGs to ensure timely threat support. Support the TIWG chairman through his respective TRADOC TM and AMC FIO in order to assist in generating and articulating requirements for threat support.

(14) Approves and monitors use of threat data, when appropriate, during developmental and operational test and evaluation phases of the materiel development cycle for ACAT I and II systems, to ensure maximum benefit from knowledge of the threat environment.

(15) Establishes liaison and maintains close coordination with Army staff agencies, PEO/PMs, MACOMs, testing agencies, and other agencies to ensure that threat support is timely, consistent, and continuous throughout the life cycle process.

(16) Recommends, as appropriate, the establishment of MACOM-chaired TCGs.

(17) Represents DA at MACOM-level TCGs, if requested and appropriate.

(18) Attends formal and informal program reviews in the course of the materiel life cycle, and determines the impact of threat considerations on the progress of systems development.

(19) For ACAT I and II systems, ensures a smooth transition for STAR responsibility to AMC after MDR I approval.

c. ODCSINT is the approving authority for either establishing or ending TISO monitoring of systems. Generally, all programs designated as ACAT I or II systems will be assigned TISOs. Other systems and programs will be assigned TISO monitoring responsibility on an "'as required"' basis with ODCSINT approval.

2–6. Threat coordinating groups

a. TCGs are integrating bodies composed of the Army's combat and materiel development activities, test and evaluation organizations, and the intelligence community to coordinate the provision of timely, consistent, and approved threat support throughout the life cycle or study process. The TCG coordinates the identification, validation, and fulfillment of threat requirements supporting each system or program.

b. The purpose of the TCG is to ensure that all appropriate organizations are informed of pertinent threat issues and means for resolution, and that they are mutually supportive of the overall effort. Preparation of the threat assessment associated with the project or study remains the developer's responsibility. The TCG chairman will coordinate the approval of threat assessments that are based on intelligence data provided in response to user requirements.

c. The two types of TCGs, system specific and mission area are discussed below.

(1) System specific TCGs coordinate threat support requirements for specific programs. For each ACAT I and II system, ODCSINT normally will establish and chair a TCG. Other programs of particular DA interest also may require a DA-level TCG. MACOMs will establish TCGs for ACAT III and IV programs as required.

(2) Mission area TCGs coordinate threat support requirements common to all systems within given mission areas. Mission area TCGs can be conducted either at DA or MACOM level.

d. For new programs, system-specific TCGs will be formed immediately following an MDR 0 decision to continue program development.

e. Membership of each DA-managed TCG will consist of representatives from the ARSTAF, combat and materiel development commands, test and evaluation organizations, and the Army intelligence community. As appropriate, representatives from DIA and other Services will be invited to take part in TCGs.

f. Functions of system specific and mission-area TCGs are to—

(1) Assist combat and materiel developers in articulating their intelligence requirements and facilitating the resolution of these requirements.

(2) Develop, for the user, a comprehensive baseline of intelligence products from appropriate approved intelligence documents. Ensure that the user considers all-source intelligence data.

(3) Coordinate and review combat and materiel developers' CIPs and ensure the development of IPRs in response to identified CIPs.

(4) Review intelligence data and threat portrayed in the concept formulation process and provide recommendations to appropriate agencies.

(5) Coordinate review of models, scenarios, and analyses for correct application and interpretation of threat.

(6) Coordinate and review threat support for developmental and operational testing, to include use of scenarios, simulators, surrogates, and targets.

(7) Coordinate the review of the STAR, TTSP, and threat portions of program management documents, such as MNS, ORD, IPS, COEAs and TEMP.

(8) Provide for transition of threat support from the generic mission area to appropriate TCGs established to support ACAT I and II systems.

(9) Identify threat and threat support issues and determine responsibility for resolution.

2–7. Threat assessments

a. The proponent responsible for developing a specific program document will also write the required threat assessment for that document. See table 1–1. The threat assessment will provide a summary of current and projected threat, targets, and missions of the proposed systems emphasizing the interactive effects of the system and threat.

b. When drafting threat assessments, the intelligence office supporting the developer will use DIA-validated threat data sources. If DIA-validated sources are not available, other source data will be highlighted and submitted for approval through intelligence channels for use in threat assessments.

c. For assistance in preparing a threat assessment to support an ACAT I or II system, threat support requirements will be forwarded through command channels to ODCSINT. The TISO, with the assistance and participation of the appropriate TCG, will assist in identifying relevant existing intelligence documents or by tasking new intelligence production according to AR 381–19.

d. The appropriate MACOM headquarters will be responsible for coordinating the preparation of threat assessments to support ACAT III and IV systems.

e. Threat assessments will be written at the lowest possible classification consistent with user needs, but no higher than SECRET. More highly classified supplements will be developed if necessary for program decisions. If a threat assessment must be released to the North Atlantic Treaty Organization (NATO), a specific country, or group of countries, it will be prepared in coordination with DIA. ODCSINT will coordinate this effort.

f. Approval authorities for threat assessments are indicated in table 1–1. Threat assessments for ACAT I and II systems will be forwarded through command channels to ODCSINT for review and approval.

g. A complete draft document (such as a complete TEMP or ORD) will be forwarded for review and approval.

h. ODCSINT will forward threat assessments written for materiel systems requiring DAB review to DIA for validation. In the case of threat assessments prepared for Army-lead JSAPs, ODCSINT will coordinate assessments with other Services involved before submitting them to DIA.

i. Threat assessments submitted for DA approval will be footnoted, by paragraph, to indicate data sources. Footnoting is required to expedite the approval process.

j. AR 381–19, AR 71–9, and this regulation provide guidance for validation of IPRs and preparation of threat assessments to be included in program management documents.

2–8. System Threat Assessment Report

a. Concept. The STAR summarizes the approved threat provided to combat and materiel developers for a specific ACAT I or II systems. It provides an assessment of the capabilities of potential adversaries, as addressed in the MNS, and their ability to neutralize or degrade a specific US systems or system concepts. It is the primary threat reference to be used in preparation of threat portions of the ORD, IPS, COEA, TEMP, and TTSP. (See table 1–1 for STAR preparation responsibilities and approval authorities.) In the rare event ACAT I, ACAT II, or OSD T&E oversight programs will not be affected by threat, the combat developer may submit requests for waivers. Waivers for ACAT I or DAB oversight programs will be submitted to the Under Secretary of Defense for Acquisition via the Army Acquisition Executive (AAE). Waivers for ACAT II programs will be submitted to the AAE. All waiver requests will be processed through intelligence channels.

b. Timing.

(1) Requirements for ACAT ID programs (subject to DAB review at milestones I through IV) and ACAT IC programs through milestone I (subject to DAB review at milestone 1) are as follows:

(a) Responsibilities. Through MDR I, the combat developer maintains responsibility for STAR preparation; thereafter, it becomes the responsibility of the materiel developer. In all instances, the developer preparing the STAR is responsible for coordinating initial STARs, updates, or changes prior to forwarding to ODSCINT according to criteria established in paragraph 2–8 *e* below.

(b) Submissions. The combat developer will prepare and submit 10 copies of the initial STAR to ODCSINT no later than 150 days following MDR 0. ODCSINT will forward the DA-approved STAR to DIA for validation within 60 days of receipt, but no later than 60 days prior to the documentation review meeting.

(c) Updates. As a minimum, STARs will be updated annually by responsible developers and forwarded to ODCSINT (10 copies) no later than 1 year beyond the most recent DIA validation date, and also no later than 120 days prior to the documentation review meeting for the next MDR. Updates will include all intelligence information to be considered by the developer prior to the next milestone.

(d) Out-of-cycle changes. When significant changes in the threat occur, especially threat affecting critical system characteristics, CIPs, and the CIP threat status, STARs will be revised and reissued or changes developed prior to the normal annual update requirement. Changes will be forwarded for ODCSINT approval and DIA validation. (Subsequent updates will be according to para 2–8 *b*(1)*(c)* above.)

(e) Intelligence report preparation. See table 1–1.

(2) Requirements for ACAT IC programs beyond MDR I (subject to Army Systems Acquisition Review Council (ASARC) at MDR II through IV) are as follows:

(a) Responsibilities. The materiel developer assumes responsibility for STAR preparation beyond MDR I. The materiel developer preparing the STAR is responsible for coordinating STAR updates or changes with the combat developer prior to forwarding to ODSCINT according to criteria established in paragraph 2–8 *e* below.

(b) Submissions. Under normal circumstances, the initial STAR will be approved by ODCSINT and validated by DIA as of MDR I. Thereafter, updates will be prepared according to criteria in paragraph 2–8 *b*(2)*(c)* below. ODCSINT will function as the final approving authority for STARs supporting ACAT IC programs subsequent to MDR I.

(c) Updates. As a minimum, STARs will be updated annually by responsible developers and forwarded to ODCSINT (10 copies) no later than 1 year beyond the most recent ODCSINT approval date (or DIA approval date, if it's the first update after MDR I), and no later than 60 days prior to the next scheduled ASARC. Updates will include all intelligence information to be considered by the developer prior to the next milestone. Combat and materiel developers must keep these dates in mind when submitting IPRs that support STAR submissions.

(d) Out-of-cycle changes. When significant changes in the threat occur, especially threat affecting critical system characteristics, CIPs, and the CIP threat status, STARs will be revised and reissued

or a change developed prior to normal annual update requirements. Changes will be forwarded for ODCSINT approval. Subsequent updates will be as stated in paragraph 2–8 *b*(1) *(c)* above.

(e) Intelligence report preparation. See table 1–1.

(f) Validation process. See figures 2–3 and 2–4 for examples of the STAR production and validation process.

(3) Requirements for ACAT II programs (subject to ASARC review at milestones I through IV) are as follows:

(a) Responsibilities. Through MDR I, the combat developer maintains responsibility for STAR preparation; thereafter, it becomes the responsibility of the materiel developer. In all instances, the developer preparing the STAR is responsible for coordinating the initial STAR, updates, or changes prior to forwarding to ODCSINT according to criteria established in paragraph 2–8 *e* below.

(b) Submissions. The combat developer will prepare and submit 10 copies of the initial STAR to ODCSINT not later than 150 days following MDR 0 and no later than 60 days prior to the next scheduled ASARC. ODCSINT will function as the final approval authority for STARs supporting ACAT II programs.

(c) Updates. As a minimum, STARs will be updated annually by responsible developers and forwarded to ODCSINT (10 copies) no later than 1 year beyond the most recent ODCSINT approval date, and also not later than 60 days prior to the next scheduled ASARC for an MDR. Updates will include all intelligence information to be considered by the developer prior to the next milestone.

(d) Out-of-cycle changes. When significant changes in the threat occur, especially threat affecting critical system characteristics, CIPs, and the CIP threat status, STARs will be revised and reissued or changes will be developed prior to normal annual update requirements. Changes will be forwarded for ODCSINT approval. Subsequent updates will be according to paragraph 2–8 *b*(2)*(c)* above.

(e) Intelligence report preparation. See table 1–1.

c. Structure. STAR format guidance is contained in appendix B.

d. Content.

(1) *Threat assessments.* Threat assessments will be based on DIA-validated threat data sources. Other analyses, however, are acceptable as long as the rationale is included and they are reasonable projections of accepted data. Thus, unvalidated data should not necessarily be discarded. Appropriate data can be included in documents that support the acquisition process, as long as it is clearly highlighted and identified as unvalidated data and is accompanied by a request for validation through appropriate channels. Terms of estimative probability should be used to the maximum extent possible. (See para B–4 *e*(2).)

(2) *CIPs.* CIPs represent threat capabilities or thresholds established by the program, changes that critically impact the effectiveness and survivability of proposed systems. CIPs normally will be developed by the PM or materiel developer, assisted by the supporting FIO, and coordinated with the proponent TSM or combat developer. The IPRs incorporating CIPs will be forwarded according to AR 381–19. New intelligence bearing on the CIPs should be brought to the attention of the PM and TSM immediately. CIPs will be used to focus subsequent STAR changes or updates.

(3) *Appendixes.* Appendixes will be developed as necessary to support assessments made in the body of the STAR.

e. Approval and validation. ODCSINT is the DA approving authority for STARs for ACAT I and II systems. CG, AMC; CG, SSDC; and CG, TRADOC are respective materiel and combat developer authorities responsible for approving STARs forwarded to DA, DAMI–FIT. A fully coordinated draft STAR with appropriate approval documentation from the combat or materiel developer, as appropriate, will be forwarded to ODCSINT, DAMI–FIT. The STAR will include a statement signed by the PM or his representative that he has reviewed the document and that the CIPs reflect the program's critical intelligence needs. (For STARs up to MDR I, the statement will be provided by the proponent materiel developer in coordination with the combat developer.) ODCSINT will obtain DIA validation of STARs for ACAT ID programs and ACAT IC through MDR I prior to DAB MDRs.

f. Classification. STAR classification will be limited to SECRET. Higher level annexes may be added as needed.

g. References.

(1) A bibliography will be included in the STAR, which will list all data sources used in preparation of the document. Referenced data sources will be the most recent versions.

(2) The STAR will be annotated by paragraph and keyed to the bibliography to show the sources of data. Annotation is required to expedite the approval process; it also will assist in STAR updates and changes.

2–9. System threat assessment

STAs serve the same purpose for ACAT III and IV programs as the STAR for ACAT I and II programs, and will be prepared using the STAR format. (See table 1–1 for STA preparation and approval responsibilities.) The threat support activity will forward an information copy of the STA to ODCSINT. In the event an ACAT III or IV system will not be affected by the threat, the combat developer may submit a request for waiver to the system or program approval authority and, if approved, forward an information copy of the waiver to ODCSINT. Requests for waiver will be processed through intelligence channels.

2–10. Threat test support package

a. Basis. The TTSP is based on the STAR but focuses on the particular purpose of the test (such as a developmental or operational test). It must provide sufficient detailed intelligence information to enable the tester to accurately portray the threat projected to exist at a post-IOC date. Determination of the threat year and scenario selection will be made by the TIWG on recommendation of the system proponent and evaluation organization.

b. Timing. The TTSP will be prepared or updated as required to meet the testing milestones as set by the TIWG. Normally, the draft TTSP (Sections I–III) will be prepared no later than 540 days prior to test day (T–540) for review by appropriate approval authorities. (See table 1–1). Section IV, Test Specific Appendixes (app C), should be completed by T–420. TTSPs are updated as required to accommodate evolving test planning.

c. Structure. TTSP format guidance is at appendix C.

d. Preparation.

(1) TTSPs will be prepared for developmental and operational testing of ACAT I–IV systems when an operationally realistic threat is required. Specific testing requirements will be determined by the appropriate TIWG. Determination of the requirement for an operationally realistic threat portrayal will be made by the TIWG on the recommendation of the evaluation organization based on the TEMP requirements.

(2) TRADOC will prepare the initial TTSP and all subsequent iterations that support operational testing.

(3) AMC will assist in the preparation of initial TTSP and prepare all subsequent iterations that support developmental testing. A TTSP is not required for a developmental test that does not require replication of threat.

(4) Conflicts related to planned threat portrayals that deviate from the approved threat that cannot be resolved at MACOM level will be referred to DA ODCSINT for resolution.

e. Approval.

(1) ODCSINT approves all TTSPs developed for ACAT I, II and OSD T&E oversight systems. ODCSINT will forward a copy to DIA for review and comment for ACAT ID and ACAT IC (through MDR I). (See fig 2–5 for an example of the TTSP validation process.)

(2) TRADOC approves all TTSPs developed for operational testing of ACAT III and IV systems that are not on the OSD T&E oversight list.

(3) AMC approves all TTSPs developed for developmental testing of ACAT III and IV systems that are not on the OSD T&E oversight list.

f. Classification. TTSP classification will be limited to SECRET or below. Higher level supplements may be added as needed.

2–11. Cost and operational effectiveness analysis

a. Threat analysis. The threat analysis portion of the COEA references the STAR and determines those elements against which a given system might be used and threat forces that could be used against that system. Determination of the threat year and scenario selection will be made by DCSOPS and ASA(RDA). Scenarios used in the COEA should include a set based on situations that conform to scenarios in the DPG. Underlying assumptions concerning the threat should not conflict with DPG assumptions. (See table 1–1 for preparation responsibilities of the threat-related sections of the COEA.)

b. Timing. Threat-related sections of the COEA will be prepared and updated as required to meet the milestone decision review process.

c. Structure. The threat-related section's structure and format are dependent on the scope of the COEA. Formats will be determined at the initial TCG.

d. Content. Threat assessment will be based on the STAR and other DIA-validated threat data sources. The threat should be provided in sufficient detail to identify, with a reasonable degree of assurance, the conditions that might exist when employing the new US 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, electronic warfare, precision munition countermeasures employed, and so forth).

e. Approval and validation. ODCSINT is the DA approving authority for the threat-related sections of COEAs (see table 1–1). ODCSINT will obtain DIA validation of the threat-related sections as required. See figure 2–6 for an example of the COEA validation process.

f. Classification. Threat-related sections of the COEA will be limited to SECRET or below. Higher-level supplements may be added as needed.

2–12. Special access programs

Threat support, in addition to that required by this regulation, for SAPs and sensitive activities will be under provisions of AR 380–381. ODCSINT is responsible for recommending to the SAP Oversight Committee (SAPOC) whether a program or activity warrants protection as a SAP. This recommendation will be based on the program security status, the state of similar foreign technology (to include possible countermeasures), and the threat posed by foreign intelligence services. Program security will be reviewed by INSCOM. Multidiscipline counterintelligence (MDCI) threat data will be furnished to ODCSINT (DAMI–CI) and the Working SAPOC by the ITAC. Generally, SAP threat support will be managed in a manner similar to normal acquisition programs. The ability to get the necessary threat producer to "'read on'" to the program will determine what deviations are required from the standard procedure. DAMI–FIT will validate the foreign technology assessment as furnished by the appropriate program threat support activity (PM, FIO, TM, or other) as determined by the mission area TISO. The TISO will coordinate all threat support through the DAMI–FIT Scientific Advisor and ensure that a copy of the validated threat assessment is furnished to the SAP program manager in DAMI-CIC prior to the working SAPOC. The TISO will attend all working meetings and the working SAPOC. If not able to attend, a replacement will be appointed and coordinated with the scientific advisor. The TISO, in coordination with the SAP program manager and appropriate threat support activity, will direct the review and distribution of SAP STARs and STAs. Maximum use of technical support from FSTC and approved threat documentation such as STARs for existing programs will be made. ACAT I and II SAPs require a STAR. ACAT III and IV SAPs require a STA; an information copy of each STA will be provided to the TISO.

Section II
Army Studies

2–13. Study directives and plans

a. Study directives and plans prepared by HQDA according to AR 5–5, which require threat support, will be coordinated, in draft, with ODCSINT to ensure that appropriate threat support tasking has been included.

b. Each study directive or plan will include, as a minimum, a threat guidance subparagraph, which will give location, general situation, and intensity of combat applicable to the study.

2–14. Study advisory group

For each major study, the study sponsor will form a SAG. SAGs advise study sponsors on the conduct of the study and will provide assistance, coordination, and support to the study performing organization. All studies requiring threat support will have a threat representative on the SAG. ODCSINT will provide a representative to the SAG for DA-directed studies or those requiring DA-approved threat support.

2–15. Procedures for HQDA-directed studies

a. When directed by ODCSINT, the ITAC (with support from FSTC) will provide threat analysis and production support to DA-directed studies. The SAG chairman will ensure that threat requirements are identified and submitted in writing to ODCSINT. Threat support required outside the Army will be coordinated with ODCSINT.

b. The SAG chairman will provide a copy of the minutes of each SAG meeting to ODCSINT.

THREAT SUPPORT TO FORCE, COMBAT, AND MATERIEL DEVELOPMENT

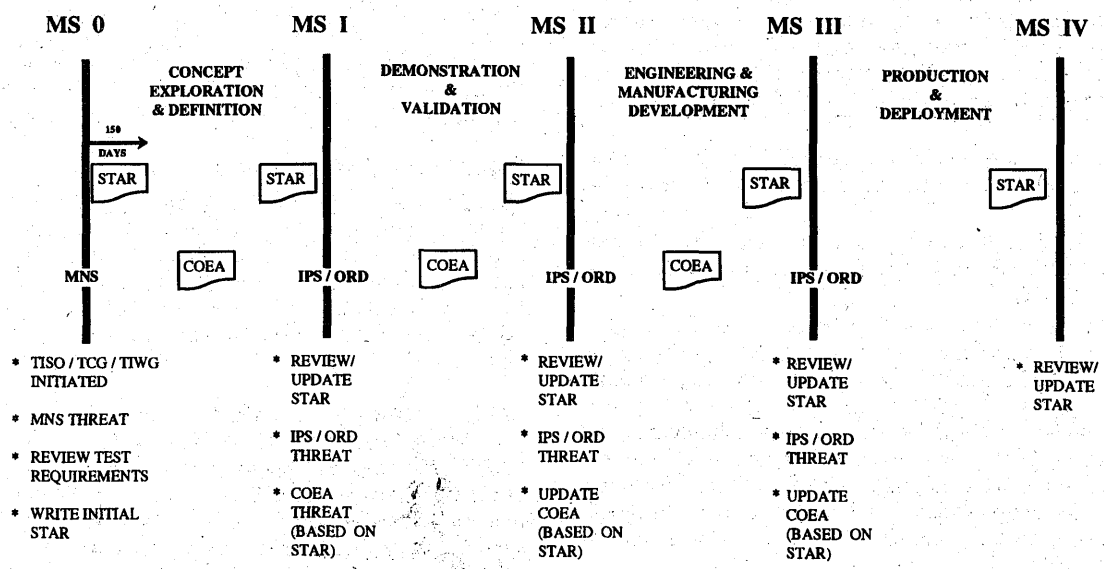


Figure 2–1. Threat support to force, combat, and materiel development

THREAT SUPPORT TO DEVELOPMENTAL AND OPERATIONAL TESTING

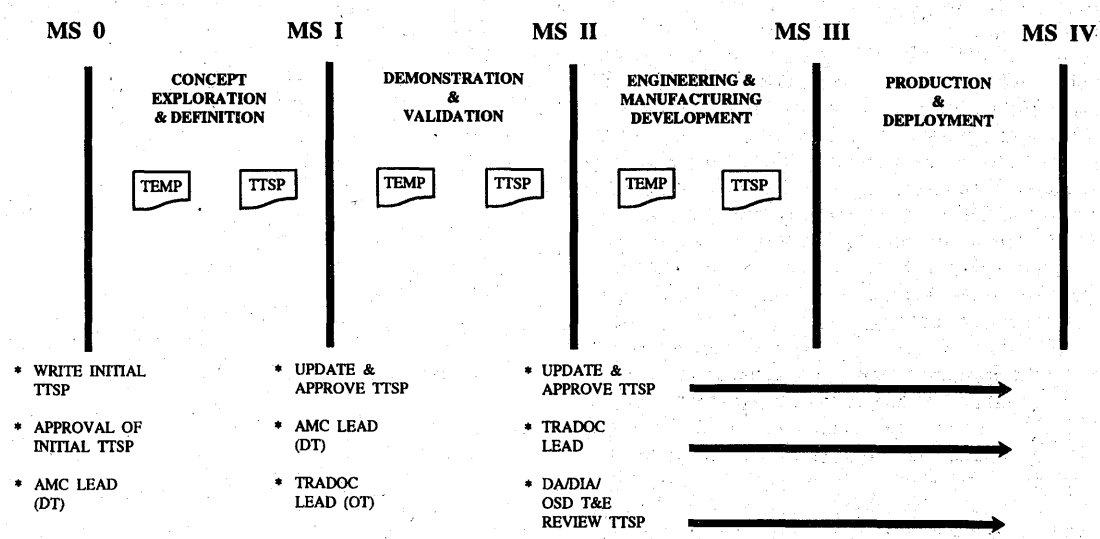


Figure 2–2. Threat support to developmental and operational testing

STAR PRODUCTION & VALIDATION PROCESS (ACAT I PROGRAMS THROUGH MS I)

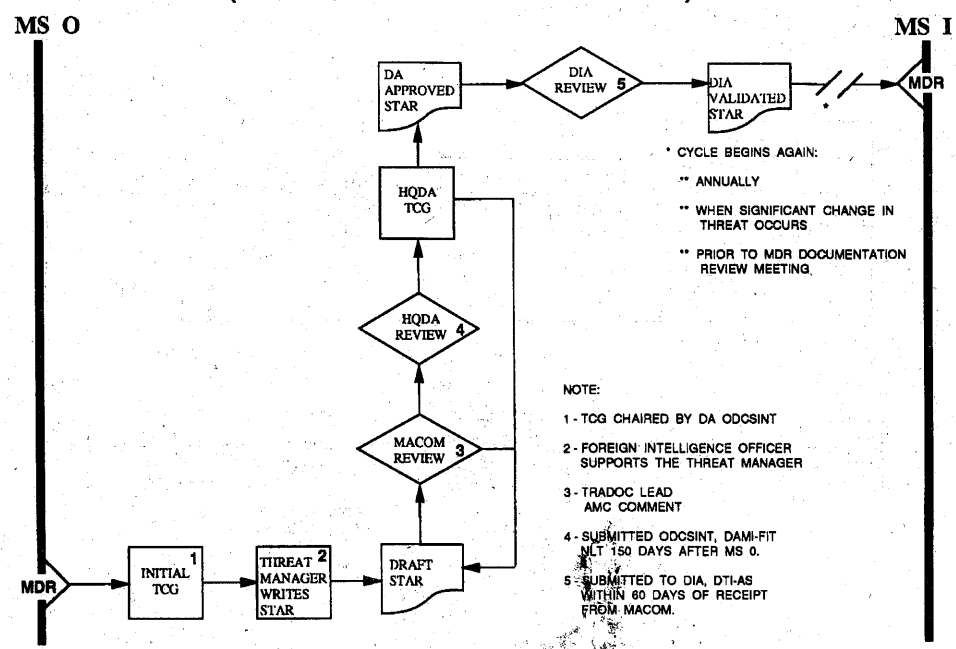


Figure 2–3. STAR production & validation process (ACAT I programs through MS I)

STAR PRODUCTION & VALIDATION PROCESS (ACAT I PROGRAMS BEYOND MS I)

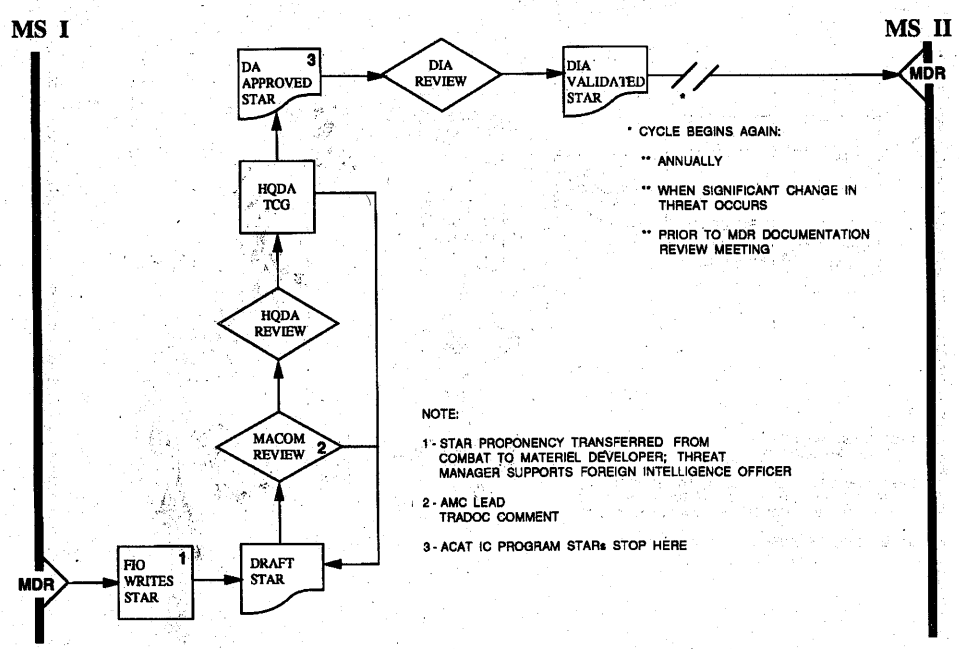


Figure 2–4. STAR production & validation process (ACAT I programs beyond MS I)

THREAT TEST SUPPORT PACKAGE (TTSP) VALIDATION PROCESS

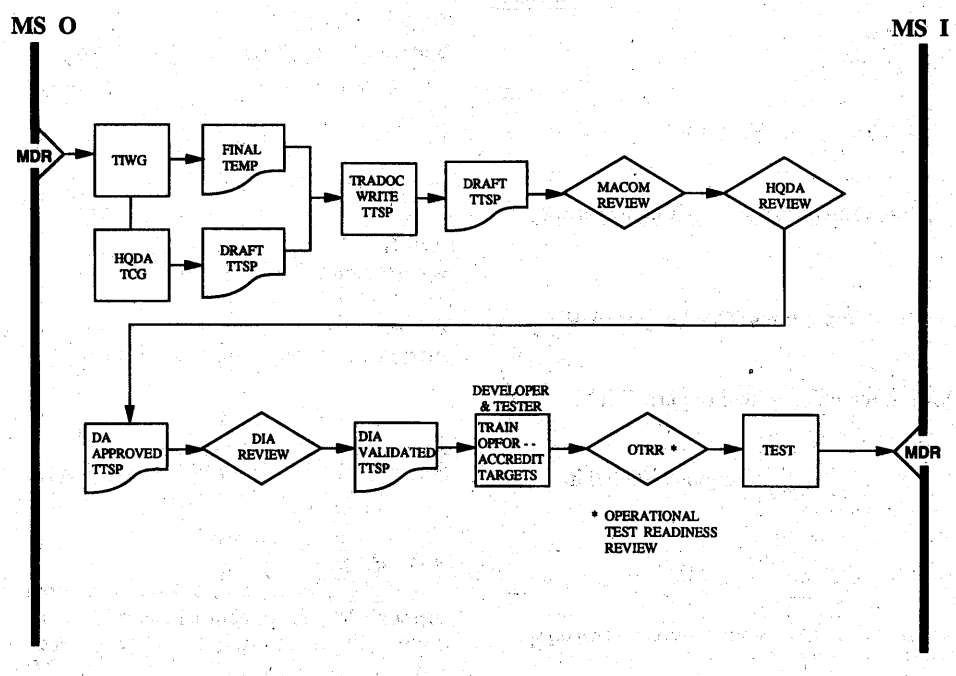


Figure 2–5. Threat test support package (TTSP) validation process

COST AND OPERATIONAL EFFECTIVENESS ANALYSIS (COEA) VALIDATION PROCESS

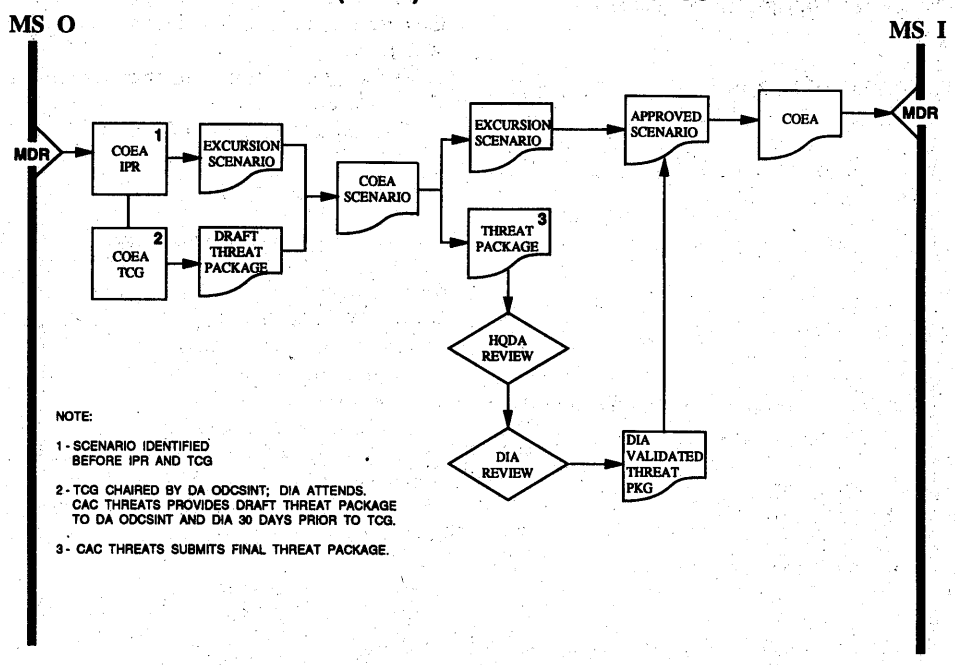


Figure 2–6. Cost and operational effectiveness analysis (COEA) validation process

Appendix A
References

Section I
Required Publications

AR 5–5
Army Studies and Analyses. (Cited in para 2-13.)

AR 5–11
Army Model Simulation Management Program (Cited in para 1-4h(4).)

AR 70–1
Systems Acquisition Policy and Procedures (Cited in para 1–4.)

AR 71–9
Materiel Objectives and Requirements. (Cited in para 2-7j.)

AR 381–19
Intelligence Dissemination and Production Support. (Cited in paras 2-4d, 2-7c, 2-7j, 2-8d(2), and b-5a(3)(d).)

Section II
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this publication.

AR 1–1
Planning, Programming, and Budgeting, and Execution

AR 15–14
Systems Acquisition Review Council Procedures

AR 25–1
The Army Information Resources Management Program

AR 70–17
System/Program/Project/Product Management

AR 73–1
Test and Evaluation Policy

AR 380–5
Department of the Army Information Security Program

AR 380–381
Special Access Programs.

AR 381–1
Security Controls on the Dissemination of Intelligence Information

AR 381–20
U.S. Army Counterintelligence Activities

AR 525–20
Command and Control Countermeasures (C2CM) Policy

DIA Regulation 55–3
Intelligence Support for Defense Acquisition Programs.

DODI 5000.1
Defense Acquisition

DODI 5000.2
Defense Acquisition Management Policies and Procedures.

DOD 5000.2–M
Defense Acquisition Management Documentation and Reports Manual.

DOD 5200.1–R
Information Security Program Regulation

DODI O–5205.7
Special Access Program (SAP) Policy

Section III
Prescribed Forms

There are no entries in this section.

Section IV
Referenced Forms

DD Form 1497
Intelligence Production Requirement

Appendix B
System Threat Assessment Report Format

B–1. General
This appendix provides a standard format for STARs prepared in support of defense acquisition programs. Administrative procedures will specify details for page numbering and references to source documentation. Contents of the STAR itself are discussed in sections covering preliminary (front matter) pages and the STAR body.

B–2. Administrative procedures
a. Cover Page. See figure B–2.
b. Page Numbering.
(1) Cover page: No numbers should be used.
(2) Preface/Table of Contents/Acronyms and Abbreviations/Executive Summary: Use lower case Roman numerals (i, ii, and so forth).
(3) Chapter 1: Begin numbering with the chapter-page number (1–1, 1–2, and so forth).
(4) Chapters 2 through 6: As with chapter 1, begin numbering with the chapter-page number (for chap 3, for example, 3–1, 3–2, 3–3, and so forth).
(5) Appendixes: Begin numbering with A–1, A–2, and so forth. Use as many appendices as needed. Examples are listed below.
(a) Appendix A—CIPs, CIP threat status, and intelligence production requirements. (Page 1 will be numbered A–1, etc.)
(b) Appendix B—Tables, drawings, and charts.
(c) Appendix C—Bibliography.
(d) Appendix D—Distribution.
(6) References:
(a) Standard rule: Every paragraph in chapters 1 through 6 must be referenced via identifying, in brackets, the bibliographical source(s) listed in appendix C. For example, a bracket entry [6, 7, 15] implies the source of information for the given paragraph was derived from the 6th, 7th, and 15th entries in appendix C (Bibliography).
(b) Possible Exception: Chapter 6 (Likely Reactive Threat), due to the nature of the information therein, may not always have referenced paragraphs. In such instances, the proponent will clearly identify the source of the stated information (for example, analyst comment or conclusion) in brackets following the paragraph—for example, [analyst comment].

B–3. STAR preliminary (front matter) pages
a. Preface: A formatted page outlining the scope of the STAR, offices involved in preparation, responsible program office, information cutoff date, and system and milestone identified. When appropriate, DIA and CIA review statements will be included in the STAR. The criteria outlined below applies.

(1) DIA validation statement (ACAT I or OSD T&E oversight programs only). Documents for DIA review and validation will include the following statement in final copies of the STAR: "The Defense Intelligence Agency has validated this document for use in analysis supporting (program name) milestone X decisions and development activities taking place during Phase X."

(2) CIA review statement (ACAT I or OSD T&E oversight programs only). DIA will forward a copy of each draft STAR to CIA for review and comment, and appropriate CIA comments will be incorporated into the STAR. DIA's validation package sent back to DA, ODCSINT will contain the CIA comments as an enclosure. Approval must be obtained from both CIA and DIA to incorporate any CIA comments in the STAR. The following statement will be placed in the preface of final copies of the STAR: "CIA has reviewed this STAR."

b. Table of contents and list of figures and illustrations.

c. Executive summary: A concise description of the projected future operational threat environment, the system-specific threat, the reactive threat that could affect program decisions, and, when appropriate, results of interactive analysis obtained by the program manager when evaluating the program against the threat. Timeframe of the threat to be addressed will start at initial operational capability (IOC) of the program and extend to at least IOC+10. The executive summary will provide a complete, autonomous threat overview. It will be specific and sharply focused and provide key intelligence judgments applicable to critical intelligence parameters and particular milestone issues. (Note: It will specifically identify significant threat changes that have been noted since the last STAR was validated. These threat changes may be related to events such as a breached CIP threshold or otherwise be significant enough to note.) Key intelligence judgments will be identified in a separate subparagraph within the executive summary.

B–4. STAR body

The body of the STAR will focus on relevant major threat capabilities that could impact on the effectiveness of the new U.S. system. The body will consist of the following chapters:

a. Chapter 1 (Introduction): Brief opening statement, to include a short summary of the MNS for the system.

b. Chapter 2 (US System Description): Summary of program objectives for the system as defined in the ORD, to include: mission; available physical and technical characteristics (including such electronic parameters as frequency bands, radiated power, modulation, and so forth); system operational concepts or method of operation; initial operational capability; and lifespan data (detailed parameters may only become available as the program develops). If development of the system would cause a marked change in the threat to related elements, such as launch platform, associated command, control, and communications (C3), then these elements should be addressed in the system description. (Note: If that marked change is already identified in another document such as a capstone STAR, then a statement that cross-references the other document will suffice.) The minimum acceptable operational performance requirements, expected operational environments, critical system characteristics, and system operational and support concepts contained in the ORD should be summarized. The system description section of the STAR must describe the U.S. system in sufficient detail to ascertain what threats may have capability against the proposed system. The following statement should be placed in the system description section of the STAR: "The elements of (enter program name) program protection including sensitive technologies and unique system features, protection threats and vulnerabilities, and program security concept and proposed countermeasures are contained in the program protection plan (PPP). In developing the PPP, the Program Manager has used the information contained in this STAR where appropriate."

c. Chapter 3 (Operational Threat Environment (OTE)): A generalized overview of the operational, physical, and technological environment in which the system will have to function through at least IOC and IOC+10 and, if applicable, the targets it is designed to engage. The OTE will be broken out by region or country, or both. Ongoing political and military changes affecting the threat should be included. Developments and trends that can be expected to affect mission capability during the system's lifetime should be projected out to the end of the life cycle when possible. Areas covered should include enemy doctrine, strategy, and tactics affecting system missions and operations. Threat content and emphasis will vary from program to program. (Note: The OTE will portray a comprehensive picture of the total aggregate of conditions and influences in which the system will be intended to function. It should include (but not be limited to) countermeasures, initial nuclear weapons effects (electromagnetic pulse, radiation, thermal, and blast), nuclear, biological, chemical (NBC) contamination threats.)

d. Chapter 4 (Targets): If applicable, an analysis of actual capabilities and signatures of projected enemy targets (such as vehicles, ships, aircraft, or silos) the U.S. system is designed to engage. The targets chapter will be broken out by region, or country, or both. Target employment, characteristics, command and control, numbers, and signatures should be included. Types and density of targets might also be covered along with such common parameters as thickness and types of armor to be defeated. Threat characteristics for individual targets, if required, should be placed in appendixes to the basic documents. (Note: The targets section will include the full range of targets to be engaged within the mission areas the system is designed to perform. Some STARs might not require a targets section. An example would be a satellite-based communications system STAR.)

e. Chapter 5 (System-Specific Threat): An assessment of the threat to the mission capabilities of the system throughout its operational lifetime. The system-specific threat section may be broken out by region and country or by technology. Ongoing political and military changes affecting the threat should be included. Time frames for threat snapshots are at IOC of the system and at IOC+10. Threat assessment should integrate doctrine, force level and structure, combat readiness, and means (conventional; electronic; initial nuclear weapons effects; NBC warfare capabilities; advanced weapons such as directed energy weapons used as either threats or countermeasures; or others, as appropriate). Detail and certainty will decrease as projections extend into the far term. Confidence in key judgments should be expressed in estimative terms to the maximum extent possible. Analysis will be responsive to CIPs developed by the PM. CIPs are a series of threat capabilities or thresholds established by the program, changes to which could critically impact the effectiveness and survivability of the proposed system.

(1) System-specific threats will focus on threat capabilities that are directly relevant to the mission and performance of the U.S. system. Descriptions of threat capabilities or projections of threat capabilities will be based on approved DOD intelligence or national intelligence when available. Other analyses are acceptable for the far term, so long as the rationale is included and they are reasonable projections of acceptable data.

(2) Conclusions and judgments will be expressed in terms of estimative probability to the maximum extent possible. The assignment of qualifying adjectives to express probability for example, the probability of an event occurring, or of the existence of capability and intent is an important component of threat assessment. To achieve consistency in the use of qualifying estimative terminology, the following qualifiers, listed below in decreasing order of likelihood, will be used.

(a) Near certain (also: will, shall, is expected, or is anticipated): 90 to 99 percent.

(b) Probable (also: likely, we believe, we estimate, or it is probable that): 65 to 89 percent.

(c) Possible (also: even chance, may, or could): 36 to 64 percent.

(d) Improbable (also: unlikely or probably not): 10 to 35 percent.

(e) Slight chance (also: highly doubtful or near impossible). 0 to 9 percent.

(3) The system-specific threat (IOC) checklist includes the following information:

(a) System description (of opposing weapons).
(b) Magnitude of threat (projected force level).
(c) Threat integration combined evaluation of threat to the U.S. system when hostile employment doctrine, force levels, and systems are considered together.

(4) Follow-on information on the system-specific checklist includes a snapshot threat at IOC plus 10 years. This section also should assess developments that would serve to degrade the system's capability out to the end of its cycle. Appropriate items are:
(a) System description.
(b) Magnitude of threat.
(c) Threat integration.

f. Chapter 6 (Reactive Threat): To the maximum extent possible, changes that might reasonably be expected to occur in enemy doctrine, strategy, tactics, force levels, technology, and weapon systems (to include advanced weapons such as directed energy weapons) as a result of development and deployment of the new system or disclosure of system technical information.

(1) Analysis of each reactive threat should consider, as a minimum, projections of—
(a) Modifications in strategy, doctrine, and tactics.
(b) New Systems or modifications to existing systems description and likely deployment.
(c) Changes in force level.
(d) Threat integration (combined evaluation of components of potential reactive threat to system).

(2) The reactive threat section will contain both the most likely reactive threat and the technologically feasible threat, broken out by region and country, or both as follows:
(a) The most likely reactive threat provides a best estimate of an adversary's developments based on historical trends, evidence of research and development, perceived military and political-economic requirements, and technological capabilities. The likely reactive threat delineates the system an adversary will most probably develop and deploy during a specified period. Threat options should be defined and any potential for those options to be exercised, presented.
(b) Technologically feasible threat section projects alternatives should the adversary's requirements differ from those assessed most likely from intelligence sources. The technologically feasible threat, although not constrained by intelligence projections, must be consistent with an adversary's technology, economic, and production capabilities. The technologically feasible threat section provides decisionmakers with a basis for judgment about the impact on a specific U.S. system if the threat were to evolve in a direction other than that considered most likely by the intelligence community. Potential for projected technologically feasible threats must be discussed.

B–5. Appendixes

Appendixes contain detailed information, generally in tabular form, required by the Service to conduct an interactive analysis or to support statements made in the body of the STAR. Minimum essential appendixes are outlined below.

a. Appendix A: CIPs, CIP Threat Status (CTS), and associated intelligence production requirement control numbers will be combined in appendix A.

(1) *CIPs.*
(a) CIPs are those threat parameters, generally quantifiable (such as a potential adversary's quantity, type, force mix, and characteristics of actual or projected threat systems and technological changes—identified by the combat developer or materiel developer), that would critically impact on the effectiveness, survivability, security, and cost of an acquisition program. CIPs represent "show stoppers" (that is, if breached, would defeat or significantly degrade the ability of the US system to perform its mission). The combat and materiel developer, in coordination with his TM or FIO, must conduct a detailed analysis of the types of enemy technologies or doctrinal changes that—if they presently exist or are later developed—could degrade the successful development of the program. For example, directed energy weapons (either threats or countermeasures to US systems), could radically impact on personnel and equipment on future battlefields. Military doctrine, tactics, strategy, and expected employment of systems should be considered for inclusion in CIPs. CIPs also should contain specific parametric values, such as radar cross-section, armor type and thickness, and acoustic characteristics that highlight US system vulnerabilities in relation to an adversary's capability.
(b) There should be a direct correlation between CIPs and the system's critical system characteristics. CIPs must be developed in sufficient detail to provide the intelligence community a clear idea of exactly what information is needed. They are not general statements of interest; rather, they should address specific thresholds. Normally, a CIP will have a numeric value; rarely should it be answerable with a "yes" or "no" response.
(c) CIPs must be developed for the initial STAR. Updates to the STAR will focus on intelligence relevant to them. Examples are provided in figure B–1.
(d) If no CIPs are identified, a statement to that effect will be included in the CIP appendix.

(2) *CTS.* For each CIP, an assessment of its threat status (CTS) will be provided. The CTS will be a stand-alone synopsis and will include the status of foreign threat programs and technology and research efforts, along with a projection of capabilities and potential for breach of the CIP threshold. In addition, intelligence data required for in-depth analyses—such as is found in scenarios for gaming, lengthy technical descriptions, vulnerability studies, or table of organization and equipment (TOE)—should be consistent with the main body of the STAR and placed in appendices or separately published documents. If these separately published documents are intended to supplement the STAR, they must be validated by DIA.

(3) *Intelligence production requirements.*
(a) Once the CIPs are developed, each will be converted to a separate IPR. If two or more CIPs are closely related, they may be included in one IPR.
(b) The TM/FIO will include a copy of the IPR on DD Form 1497 (Intelligence Production Requirement) as part of appendix A. Either the validated IPR control number or the preliminary MACOM control number will be indicated for each CIP listed in a STAR.
(c) All intelligence echelons, including DIA and DA ODCSINT, must ensure that new intelligence bearing on CIPs is brought to the attention of the PM in a timely manner.
(d) The TM/FIO will process IPRs according to AR 381–19.

b. Appendix B: Tables, Drawings, and Charts.

c. Appendix C: Bibliography. A reference list of current, major sources used in the preparation of the report. These sources should mainly include DIA-validated intelligence data sources. Other sources should be clearly identified as unvalidated data sources. Preface those sources not DIA-validated with an asterisk ("*"), and include a footnote specifying that asterisks imply that sources are not DIA-validated.

d. Appendix D: Distribution. Appropriate DOD component and DA level offices should be included.

1. *(classification)* Evidence of multispectral obscurants being fielded that are capable of degrading or defeating the *(type)* infrared sensor in the *(number)* micron *(mid)* or *(number)* micron (far) infrared bands.

2. *(classification)* Evidence of fielding *(type)* jammers, decoys, or mufflers that could degrade or defeat the *(type)* sensor in the *(no.)* Hz bandwidth.

3. *(classification)* Evidence of fielding IR camouflage, signature suppression devices, decoys, or jammers that could degrade or defeat the *(number)* sensor in the *(no.)* to *(no.)* micron bands.

4. *(classification)* Evidence of fielding a high-power microwave (HPM) weapon operating in the *(no.)* to *(no.)* GHz range.

5. *(classification)* Evidence of armor protection levels that exceed *(no.)* mm of rolled homogeneous armor for top surfaces.

Figure B–1. Critical intelligence parameter (CIP) examples

(SYSTEM NAME)

SYSTEM THREAT ASSESSMENT REPORT (STAR)

APPENDIX __ / ANNEX __

TO > [if applicable]

(CAPSTONE SYSTEM)

PREPARING AGENCY:

INFORMATION CUTOFF DATE:

APPROVED/VALIDATED BY: (DA)/(DIA)
[as appropriate]

DATE APPROVED/VALIDATED: (DA)/(DIA)
[as appropriate]

PUBLICATION DATE (DRAFT OR FINAL):

NOT RELEASABLE TO FOREIGN NATIONALS

WARNING NOTICE: INTELLIGENCE SOURCES AND METHODS INVOLVED

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

CLASSIFIED BY:
DECLASSIFY ON:

Figure B–2. STAR Cover page (format)

Appendix C
TTSP Format Guidance

C–1. TTSP preliminary pages

a. Title page. Shows the title, preparing agency, information cutoff date, U.S. system project office, and MACOM or DA validation date, as appropriate.

b. The table of contents and illustrations follow the title page.

C–2. TTSP body

a. Section I. Background Information:

(1) Description of system, organization, or concept to be tested.
(2) Type of test.
(3) Evaluating agency.
(4) Test organization.
(5) TRADOC proponent school.
(6) Test dates.
(7) Test location.
(8) Simulated location (for example, central Europe)
(9) IOC of system being tested
(10) Threat year.
(11) Title and date of STAR.

b. Section II. Issues and Criteria: Critical operational issues and criteria (COIC) are key issues, with associated scope, criteria, and rationale that must be satisfied at a milestone III decision review. Exit criteria are used in lieu of intermediate COIC for milestone II and limited initial production decisions. They provide broad insight into threat support requirements for each test. Additional operational issues and criteria (AOIC) are developed by the evaluator to complement the COIC or exit criteria, as well as provide for comprehensive evaluation of the total system. Approved COIC or exit criteria and AOIC may not be available when drafting the initial TTSP, which cannot be completed until COIC or exit criteria and AOIC are approved. The TTSP should not be forwarded for validation unless the approved COIC or exit criteria and AOIC are included in Section II.

c. Section III. Threat: This section is required approximately 18 months prior to the actual test (T–540). When initially developed, it will be somewhat generic in nature but adequate for test planning. The threat portrayed will be based on and consistent with the systems' STAR. As the test requirements are better defined, this section will be revised to describe the specific threat required for the test. Should an extensive amount of material be required, systems and tactical considerations are to be summarized with references to more detailed and approved intelligence documents. This section will include the following:

(1) Specific systems and units and organizations that are a threat to, or a target of, the system, organization, or concept being tested; included are technical descriptions of threat systems and TOE for units.

(2) Threat tactics, doctrine, techniques, procedures, and flight profiles (as appropriate).

(3) Threat countermeasures. Primary sources for information include the system STARs and other DIA-approved intelligence documents

d. Section IV. Test-Specific Appendixes: Appendixes cited below are essential elements of the TTSP as completed. All required appendices must be included in the TTSP when forwarded for final approval.

(1) *Appendix A.* Test Concept: The test concept is developed by the tester from chapters 1 & 2 of the Test Evaluation Plan (TEP), which is prepared by the evaluator. It will describe, in detail, test scope and criteria. Test concept will be used to define the required threat for a specific test. Approved issues are found in the TEP.

(2) *Appendix B.* Scenario: Test scenario describes how the test operations should be conducted. Selection of the scenario is the responsibility of the test proponent. The test organization, in coordination with the TRADOC threat support office, is responsible for integrating the approved threat into the scenario. Normally, test scenarios are based on TRADOC-approved low- or high-resolution scenarios or other recent and related combat developer actions. All aspects of the scenario must be reviewed from the threat perspective to ensure adequate portrayal in support of the stated test issues and criteria. Areas to consider include scheme of maneuver, TOE organization and types of equipment, tactics and supporting fires or forces.

(3) *Appendix C.* Description of trials, test runs, and vignettes: This appendix describes how the threat operations will be conducted. The TTSP must include a description of threat forces and operations that will be used to portray the scenario during the test. Templates showing threat force locations, routes of movement, and listings of threat force organizations and equipment to be used in the test are required. Inclusion of this information allows reviewing agencies to determine whether or not the threat will be portrayed accurately to support the COIC or exit criteria and AOIC.

(4) *Appendix D.* Firer and target matrix: Test organization will participate in the development of instrumentation and possibly modeling data requests (Ph and Pk numbers) developed and submitted by the proponent school or, in some cases, the test agency. Data requests normally will be in the form of a firer or target matrix submitted for approval. When required, the firer or target matrix is prepared by the proponent threat office and the test organization.

(5) *Appendix E.* Targets, threat simulators, or surrogates: Most field testing requires the use of U.S. Army, NATO, or contractor equipment to be used, in lieu of actual threat systems. Assessments are to be limited to features that are applicable to the specific test. For example, if test threat systems are to be immobile during a test, then it is not appropriate to point out that surrogate systems are not as fast as the actual threat system is attempting to portray. Validation and accreditation reports pertinent to the targets and simulators are listed in the outline test plan and contain technical information needed to assess the impact of shortcomings of threat equipment as potential test limitations. Include a list of all equipment required for the test.

(6) *Appendix F.* Limitations: Test proponent and test agency are required to make known overall limitations of the test, such as tactics, equipment, or considerations that should have been in the test but are excluded for whatever reason. The preparer is required to assess and describe the effects of these stated limitations, plus any limitations they perceive, on the ability of the test to portray a valid threat.

(7) *Appendix G.* Threat force training plan: A threat force training plan is mandatory for force-on-force tests or tests involving any threat replication requiring threat player personnel. The proponent will develop a threat force training plan to train designated player units in threat tactics and situations to be portrayed in the test. The threat force training plan will include a program of instruction (POI). Lesson plans are not required for inclusion into the TTSP, but may be necessary to use in training the actual unit. The POI should be based on what the test threat force needs to know for the specific test.

Glossary

Section I
Abbreviations

AAE
Army Acquisition Executive

ACAT
acquisition category

AFMIC
Armed Forces Medical Intelligence Center

AMC
U.S. Army Materiel Command

AMSAA
Army Materiel Systems Analysis Activity

AMSMP
Army Model and Simulation Management Program

AOIC
additional operational issues and criteria

ARSTAF
Army Staff

ASARC
Army Systems Acquisition Review Council

ASA(RDA)
Assistant Secretary of the Army (Research, Development, and Acquisition)

CAA
Concepts Analysis Agency

CAC
Combined Arms Command

CBTDEV
combat developer

CIA
Central Intelligence Agency

CIP
critical intelligence parameter

COEA
cost and operational effectiveness analysis

COIC
Critical Operational Issues and Criteria

CTC
Combat Training Center

CTS
CIP threat status

DA
Department of the Army

DAB
Defense Acquisition Board

DAE
Defense Acquisition Executive

DIA
Defense Intelligence Agency

DIAR
DIA Regulation

DOD
Department of Defense

DODI
DOD Instruction

DPG
Defense Planning Guidance

DT
developmental test

FDTE
force development testing and experimentation

FIO
Foreign Intelligence Officer

FSTC
US Army Foreign Science and Technology Center

HPM
high-power microwave

INSCOM
U.S. Army Intelligence and Security Command

IOC
initial operational capability

IPR
intelligence production requirement

IPS
Integrated Program Summary

IR
infrared

ITAC
U.S. Army Intelligence and Threat Analysis Center

JP
Joint Program

JSAP
Joint Service Acquisition Program

LRRDAP
long-range research, development and acquisition plan

MACOM
major Army command

MATDEV
materiel developer

MDCI
multidiscipline counterintelligence

MDAP
major defense acquisition program

MDR
milestone decision review

MNS
mission need statement

MSIC
Missile and Space Intelligence Center

NATO
North Atlantic Treaty Organization

NBC
nuclear, biological, chemical

NDI
non-developmental item

ODCSINT
Office of the Deputy Chief of Staff for Intelligence

ODCSOPS
Office of the Deputy Chief of Staff for Operations and Plans

OPFOR
opposing forces

OPSEC
operations security

OPTEC
Operational Test and Evaluation Command

ORD
operational requirements document

OSD
Office of the Secretary of Defense

OT
operational test

OTE
operational threat environment

OTSA
OPTEC Threat Support Activity

PEO
Program Executive Officer

PM
program, project, or product manager

POI
program of instruction

POM
program objective memorandum

PPP
program protection plan

RDA
research, development, and acquisition

RDTE
research, development, test and evaluation

RFP
request for proposal

SAG
study advisory group

SAP
Special Access Program

SAPOC
Special Access Program Oversight Committee

SIO
senior intelligence officer

SST
system specific threat

SECDEF
Secretary of Defense

SSDC
US Army Space and Strategic Defense Command

SSG
special study group

S&TI
scientific and technical intelligence

STA
system threat assessment

STAR
system threat assessment report

STRICOM
US Army Simulations, Training, and Instrumentation Command

STF
special task force

TAWG
threat accreditation working group

TCG
threat coordinating group

T&E
test and evaluation

TEMA
Test and Evaluation Management Agency

TEMP
Test and Evaluation Master Plan

TEP
test evaluation plan

TISO
Threat Integration Staff Officer

TIWG
test integration working group

TM
Threat Manager

TOE
table of organization and equipment

TRADOC
US Army Training and Doctrine Command

TSM
TRADOC System Manager

TTSP
threat test support package

USD(A)
Under Secretary of Defense (Acquisition)

VWG
validation working group

Section II
Terms

Acquisition categories (ACATs)
Categories established to facilitate decentralized decisionmaking and execution and compliance with statutorily imposed requirements. Categories determine level of review, decision authority, and applicable procedures.

Approve
Within the context of this regulation, the term "approve" signifies the formal or official acceptance or sanction of a threat assessment or product at the intermediate level of authority. For example, an ACAT II program STAR would require approval by the appropriate MACOM and validation by DA ODCSINT. (See validate.)

Army Systems Acquisition Review Council (ASARC)
Top-level DA corporate body for systems acquisition that provides advice and assistance to the Secretary of the Army and the Army Acquisition Executive.

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

Coordinate
Process of seeking concurrence from one or more organizations or agencies on adequacy of specific draft assessment, estimate, or report. Intended to increase product's factual accuracy, clarify its judgments, and resolve disagreements on threat issues.

Cost and operational effectiveness analysis (COEA)
Analysis of estimated costs and operational effectiveness of alternative materiel systems to meet mission need and associated program for acquiring each alternative.

Critical intelligence parameters (CIPs)
Threat capability or threshold established by program manager, changes to which could critically impact on effectiveness and survivability of proposed system. CIPs serve to alert supporting intelligence organizations regarding specific priority intelligence requirements, in order for them to focus intelligence production and collection efforts.

Critical intelligence parameters threat status (CTS)
Status of threat programs, technologies, and research efforts relative to CIP. Will include projection of threat capabilities and potential for breaching CIP thresholds.

Defense Acquisition Board (DAB)
Senior DOD acquisition review board, chaired by USD(A).

Force development
Integration of allocated and projected Army resources into a 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.

Initial operational capability (IOC)
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.

Integrated program summary (IPS)
DOD Component document prepared and submitted to MDR authority in support of MDRs I-IV. Succinctly highlights status of a program and its readiness to proceed into the next phase of the acquisition cycle.

Intelligence
Product resulting from the collection, processing, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas. Intelligence information evaluated in developmental process is referred to as "threat."

Intelligence community document
Finished intelligence product published under sponsorship of the Director for Central Intelligence and coordinated by various members of the intelligence community, to include DCSINT. Examples are national intelligence estimates and Weapons and Space Systems Intelligence Committee documents. CIA-produced documents are not intelligence community documents.

Intelligence production requirement (IPR)
Stated need for production of intelligence on general or specific subject, program system, or weapon.

Intelligence report
Report provided by appropriate intelligence agency or command to milestone decision authority prior to each MDR. For MDR 0, for example, report will confirm validity of the threat contained in the MNS; for MDRs I-IV, report will confirm validation of STA(R) used in support of acquisition program and will address threat issues, risks, or unresolved threat concerns affecting program.

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.

Major defense acquisition program (ACAT I)
Acquisition program not a SAP and that is—
a. Designated by USD(A) as a MDAP.
b. Estimated by USD(A) to require the following:
(1) Eventual total expenditure for RDTE of more than $200 million FY80/approximately $300 million FY90 constant dollars.
(2) Eventual total expenditure for procurement of more than $1 billion FY80/approximately $1.8 billion FY90 constant dollars.

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.

Mission need statement (MNS)
Statement of operational capability required to perform an assigned mission or to correct deficiency in existing capability to perform mission. Identifies USD(A) mission area and describes mission area need. Supports milestone O decisions, and contains threat to be countered. Threat will be derived from DIA-produced or -validated documents.

Nonmajor defense acquisition program (ACAT II-IV)
Program other than MDAP or SAP. (Threat support procedures for ACAT II-IV programs are listed in table 1-1 of this regulation.)

Operational requirements document (ORD)
Document containing performance (operational effectiveness and suitability) and related operational parameters for proposed concept or system. Submitted to milestone decision authority in support of milestone I through IV reviews. Summarizes threat to be countered and projected threat environment. Threat will be derived from DIA-validated STAR for all ACAT I programs through milestone I and for ACAT ID programs for milestone II through IV. STAR will be referenced in ORD.

Production
Conversion of information or intelligence information into finished intelligence through integration, analysis, evaluation, and interpretation of all available data and preparation of intelligence products in support of known or anticipated user requirements.

Reactive threat
Changes that might reasonably be expected to occur in hostile doctrine, strategy, tactics, force levels, and weapon systems as a result of development and deployment of the US system.

Simulator
Generic term used to describe family of equipment used to represent threat weapon systems in development testing, operational testing, and training. Threat simulator has one or more characteristics which, when detected by human senses or man-made sensors, provide appearance of actual threat weapon system with prescribed degree of fidelity.

Special access program (SAP)
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. STARs 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.

System threat assessment (STA)
Describes threat to be countered and projected threat environment. Threat information will reference DIA-validated threat data sources. Prepared in STAR format, supports ACAT III and IV systems.

System threat assessment report (STAR)
Threat assessment tailored to and focused on a particular ACAT I or II system. Contains integrated assessment of projected enemy capabilities (doctrine, tactics, hardware, organization, and forces) to limit, neutralize, or destroy system. Will serve as basic threat document supporting system development and will reference DIA-validated threat data sources. A dynamic document that will be continually updated and refined as a program develops. Required for MDRs I-IV. Will be approved and validated in support of ASARC/DAB review.

Technologically feasible threat
Potential threat that may be assessed as unlikely but for which capability exists and which would impact on U.S. system under development.

Test and evaluation master plan (TEMP)
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.

Threat
Ability of an enemy or potential enemy to limit, neutralize, or destroy effectiveness of current or projected mission, organization, or item of equipment. Statement of that threat is prepared in sufficient detail to support Army planning and development of concepts, doctrine, training, and materiel.
Statement of a capability prepared in necessary detail, in context of its relationship to specific program or project, to provide support for Army planning and development of operational concepts, doctrine, and materiel.

Threat Accreditation Working Group (TAWG)
Group formed to accredit specific test application of threat simulators, targets, surrogates, and target arrays.

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 assessments consider product of threat analysis vis-a-vis a US force and include perceived military judgments of evaluated threat force.

Threat coordinating group (TCG)
Group formed to manage threat support to combat and materiel development process throughout entire life cycle of systems process.

Test integration working group (TIWG)
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 US System PM, ODCSINT (HQDA), Threat Support Activities, Operational Test And Evaluation Command (OPTEC), Combined Arms Center (CAC) Threats Directorate, and Army Materiel Systems Analysis Activity (AMSAA). Principal threat integrator for TIWG is supporting AMC FIO. PM ITTS, FSTC, and

ITAC are represented on TIWG when discussions and test planning warrant their participation.

Threat support activity
Provides threat support to either a combat or materiel developer (such as Threat Managers (TMs) in TRADOC; Foreign Intelligence Officers (FIOs) in AMC; and Assistant Chief of Staff for Intelligence (ACSI) for SSDC).

Threat test support package (TTSP)
Document or group of documents that provide comprehensive description of threat to US system being tested and targets the system will engage.

Validate
Within the context of this regulation, the term "validate" signifies formal or official acceptance or sanction of a threat assessment or product at the highest level of authority. Validation certifies the assessment or product as the official version or edition. For example, a STAR for an ACAT ID program would require approval by DA ODCSINT and validation by DIA. (See approve.)

Validation working group (VWG)
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 TEMA.

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.

Section III
Special Abbreviations and Terms

There are no special terms.

Index

Accreditation
1-4h(5), 2-3a, 2-3c, Appendix C C-2d(5)

AMC Foreign Intelligence Officer (FIO)
1-4d(1), 1-4k(2), 2-5b(13), 2-12, Appendix B B-5a(1)(a)

Bibliography
2-2, 2-8g, Appendix B B-2b(5)(c), B-2b(6)(a), B-5c

Central Intelligence Agency (CIA)
Appendix B B-3a, B-3a(2)

CIP Threat Status (CTS)
2-8b(1)(d), 2-8b(2)(d), 2-8b(3)(d), Appendix B B-5a, B-5a(2)

Combat simulations
1-4h, 2-4

Cost and Operational Effectiveness Analysis (COEA)
1-4c(4), 1-4a(10), 1-4b(3), 1-4f(14), table 1-1, 2-6f(7), 2-8a, 2-11, figure 2-1, figure 2-2, figure 2-6

Critical Intelligence Parameters (CIP)
1-4d(9), 1-4k(5), 2-5b(9), 2-6f(3), 2-8b(1)(d), 2-8b(3)(d), 2-8d(2), Appendix B B-3c, B-4e, B-5a, B-5a(1), B-5a(3)

Defense Planning Guidance (DPG)
2-c(1), 2-4c(2), 2-11a

Defense Intelligence Agency (DIA)
1-5b, 1-5c(2), 1-5c(4), 1-4b(8), 1-4b(10), 1-4b(16), table 1-1, 2-1g, 2-5b(6), 2-5b(11), 2-6e, 2-7e, 2-7h, 2-8b(1)(b), 2-8b(1)(c), 2-8b(1)(d), 2-8b(2)(b), 2-8b(2)(c), 2-8e, 2-10e, 2-11e, figure 2-2, figure 2-3, figure 2-4, figure 2-5, figure 2-6, Appendix B B-3a, B-5a(3), B-5a(3)(c), figure B-1

Developmental test
1-5c(4), 1-4a(7), 1-4d(10), 1-4f, 1-4h(4), table 1-1, 2-1b(3), 2-5b(14), 2-6f(6), 2-10a, 2-10d(1), 2-10d(3), 2-10e(3), figure 2-2

Integrated Program Summary (IPS)
1-4a(2), 1-4b(10), 1-4d, 1-4d(7), 1-4k(4), table 1-1, 2-6f(7), 2-8a, figure 2-1

Intelligence Production Requirements (IPR)
1-4b(14), 1-4b(15), 1-4b(16), 1-4d(9), 2-5b(9), 2-6f(3), 2-8d(2), Appendix B B-2b(5)(a), B-5a, B-5a(3)

Intelligence products
1-4b(17), 2-1b(2), 2-2, 2-3b, 2-4d, 2-6f(2)

Intelligence Report
1-4b(13), 1-4d(19), 1-4e(15), 2-8b(1)(e), 2-8b(2)(e), 2-8b(3)(e)

Low resolution scenarios
1-4b(7), 1-4e(7), table 1-1, Appendix C C-2d(2)

Mission area
2-5a, 2-6c, 2-6c(2), 2-12, Appendix B B-4d

Mission Need Statement (MNS)
1-4b(10), 1-4e(1), 1-4e(2), table 1-1, 2-6f(7), 2-8a, figure 2-1, Appendix B B-4a

Operational Requirements Document (ORD)
1-5c(4), 1-4b(10), 1-4e(1), 1-4e(2), table 1-1, 2-6f(7), 2-7g, 2-8a, figure 2-1, Appendix B B-4b

Operational testing
1-5c(4), 1-4d(10), 1-4e(13), 1-4f, 1-4g(2), 1-4g(6), 1-4h(4), table 1-1, 2-1b(3), 2-5b(14), 2-6f(6), 2-10a, 2-10d(1), 2-10d(2), figure 2-2, figure 2-5

Program Protection Plan (PPP)
Appendix B B-4b

Special Access Program (SAP)
1-4h(2), 2-12

Study advisory group (SAG)
1-4b(4), 2-14, 2-15

System Threat Assessment Report (STAR)
1-4a(9), 1-4b(6), 1-4b(10), 1-4c(5), 1-4d(2), 1-4d(3), 1-4d(4), 1-4e(3), 1-4e(4), 1-4e(5), table 1-1, 2-5b(8), 2-5b(19), 2-6f(7), 2-8, 2-9, 2-10a, 2-11a, 2-11d, 2-12, figure 2-1, figure 2-3, figure 2-4, Appendix B, Appendix C C-2a(11), C-2c, C-2c(3)

System Threat Assessment (STA)
1-4d(6), 1-4e(11), table 1-1, 2-9, 2-12

Simulations, Training, and Instrumentation Command (STRICOM)
1-4a(8), 1-4d(18)

Surrogate
1-4d(18), 1-4e(20), 1-4f, 1-4h(9), 2-6f(6), Appendix C C-2d(5)

Threat Accreditation Working Group (TAWG)
1-4b(9), 1-4d(11), 1-4e(9), 1-4e(12), 1-4g(5), 1-4h(5), 1-4k(6), 2-3c

Test and Evaluation Master Plan (TEMP)
1-4b(10), 1-4d(5), 1-4d(7), 1-4k(4), table 1-1, 2-6f(7), 2-7g, 2-10d(1), figure 2-2, figure 2-5

Test Integration Working Group (TIWG)
1-4b(9), 1-4d(10), 1-4e(9), 1-4e(12), 1-4k(8), 2-5b(13), 2-10a, 2-10b, 2-10d, figure 2-5

Threat assessments
1-1, 1-5c(3), 1-5c(5), 1-4a(2), 1-4b(10), 1-4h(1), 1-4h(5), 2-1h, 2-2, 2-5b(5), 2-5b(6), 2-5b(12), 2-6b, 2-7, 2-8d(1), 2-12, Appendix B B-4e

Threat Coordinating Group (TCG)
1-4a(6), 1-4b(6), 1-4c(2), 1-4d(11), 1-4d(12), 1-4e(9), 1-4e(10), 1-4g(2), 1-4g(5), 1-4h(3), 1-4h(6), 1-4j(2), 1-4k(6), 2-5b(3), 2-5b(16), 2-5b(17), 2-6, 2-7c, 2-11c, figure 2-3, figure 2-4, figure 2-5, figure 2-6

Threat Integration Staff Officer (TISO)
1-4b(9), 2-1g, 2-5, 2-7c, 2-12

Threat Test Support Package (TTSP)
1-4d(10), 1-4e(13), 1-4g(6), table 1-1, 2-8a, 2-10, figure 2-2, figure 2-5, Appendix C

TRADOC Threat Manager (TM)
1-5c(5), table 1-1, 2-5b(13), 2-12, figure 2-3, figure 2-4, Appendix B B-5a(1)(a), B-5a(3)(b)

Validation Working Group (VWG)
1-4d(11), 1-4g(5), 1-4h(5), 1-4i(2), 2-3b

Waiver
2-8a, 2-9

*U.S. G.P.O.:1993-342-064:40283

PIN 004110–000