

Threat Support Improvement

for DoD Acquisition Programs

Christopher Boggs ■ Maj. Jonathan Gilbert, USAF
Paul Reinhart ■ Maj. Dustin Thomas, USAF
Brian Vanyo

Department of Defense Instruction (DoDI) 5000.02 requires the intelligence community to provide a technology-based assessment, known as the System Threat Assessment Report (STAR), delivered at Milestones B and C. The STAR is intended to reduce technology surprise for weapon systems in development by informing the program office of foreign developments and operational capabilities.

Changes to DoDI 5000.02 are expected to force a dramatic increase in STAR production, due to new requirements for an additional STAR at Milestone A and for system-specific STARs for all Major Defense Acquisition Programs, Major Automated Information System programs, and programs under oversight of the Director of Operational Test and Evaluation in the Office of the Secretary of Defense. The DoD intelligence community must adapt to meet the increased demand for STAR production, but without additional resources.

Boggs is a former Army Signal Corps Officer. Currently with the Defense Intelligence Agency (DIA), he supports Major Defense Acquisition Programs and Major Automated Information Systems with adversary Cyberspace Operations and Information Operations threat assessments.

Gilbert is an Air Force acquisition officer with previous assignments in intelligence, test, and research labs. He currently provides DIA intelligence support to Department of Defense (DoD) acquisition programs. **Reinhart** is a former naval aviator and is now a DIA aviation-related technology specialist, supporting Major Defense Acquisition Programs with analysis and oversight of related assessments. **Thomas**, an Air Force engineer with previous assignments in operational test and research labs, currently provides intelligence support to DoD acquisition programs. **Vanyo** is a former naval flight officer and now is an aviation-related DIA technology specialist, supporting Major Defense Acquisition Programs with analysis and oversight of related assessments.

Report Documentation Page

*Form Approved
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE APR 2014	2. REPORT TYPE	3. DATES COVERED 00-00-2014 to 00-00-2014			
4. TITLE AND SUBTITLE Threat Support Improvement for DoD Acquisition Programs		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S)		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Acquisition University, Defense AT&L, 9820 Belvoir Road, Fort Belvoir, VA, 22060-5565		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)			
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	Same as Report (SAR)	5	



Modifications to current threat-support production methodology will create an efficient means to enable both large-scale STAR production and to standardize content for all STARs, ensuring currency of the information, uniformity of assessments and improved decisional value for the requirements generation, acquisition and test communities.

Today's System Threat Assessment Report

Today's STAR is a labor-intensive document to produce, often with outdated content and sometimes offering limited decisional value to program managers, the test community and the milestone decision authority. Most of these inherent issues with STAR production and content are not evident to DoD customers who may be using these assessments to inform program decisions.

Most STARs are produced by a relatively small number of authors at Service intelligence units. Complicating production is the lack of uniformity in how the Services implement their STAR programs. In some cases the Services decentralize production to the local systems

command intelligence support units; others produce it at the Service intelligence centers without much interaction with the systems command intelligence support units. STARs are also reviewed or "validated" by different organizations, based on the program acquisition category (ACAT) level. Respective Service intelligence directorates validate threat documentation for ACAT IC programs and below.

The Defense Intelligence Agency's Defense Technology and Long-Range Analysis Office (DIA/TLA) is the validation authority for ACAT ID and ACAT IAM program threat assessments. Over the last 6 years, TLA has noticed a number of production process inefficiencies and content standardization issues in most intelligence assessments supporting DoD acquisition programs.

Delivery Schedule: Current STARs are not produced in time to influence design decisions. They offer inconsistent decisional value, and they are not tailored to support key activities in the acquisition process. DoDI 5000.02 currently requires a program STAR at

Milestones B and C, but these events occur after the validation by the Joint Capabilities Integration Development System (JCIDS)/Joint Requirements Oversight Council of threat-sensitive Key Performance Parameters (KPPs) or Key System Attributes (KSAs), and take place after most system design decisions.

Topic Redundancies: Topic redundancies are costing thousands of work hours across the intelligence community through inefficient and labor-intensive production processes,

key trends by using a source that does not happen to capture current thinking of relevant subject matter experts in the intelligence community.

Improving the Value of Threat Assessments for OSD

We believe we can improve the value of threat support provided for acquisition programs and can correct many current deficiencies noted above through two key steps: development of an authoritative, DIA-validated, DoD threat library



Certain topics appear in multiple STARs, and therefore are being reviewed dozens of times per year by the DIA, the test community, systems commands and the Service intelligence centers.

with little value added for the additional reviews. Certain topics appear in multiple STARs, and therefore are being reviewed dozens of times per year by the DIA, the test community, systems commands and the Service intelligence centers. For example, "Ground-Based Early Warning Radar Threats" is a topic in the 2012 or 2013 editions of STARs for the F-22, F-35, Global Hawk, KC-46A, B61 Tail Kit Assembly, Naval Rotary Wing Aircraft and Naval Fixed Wing Aircraft. Each of these documents required a separate review and update process by the handful of ground-based radar experts at a cost of lost analysis and production, which could have contributed to other important work, such as threat modeling.

Ineffective Reviews: The current review process sometimes is ineffective in catching new threat developments, possibly due to the large size of current STARs and the large number of redundant reviews by the same analyst in a given year. Reviewing personnel tend to be less thorough when asked to review the same products, or very similar products, several times. The effect becomes apparent when major threat developments are not reflected in a STAR despite numerous reviews.

Authoritative Sources: STAR authors today have no single authoritative source for a DoD position on any given technology topic; hence the same "Ground-Based Early Warning Radar Threats" topic often is covered in multiple Capstone Threat Assessments and STARs. Consequently, two different programs may receive substantially different assessments on the same topic, with both assessments considered equally valid during a given 2-year period. STAR authors lacking a particular subject matter expertise might inadvertently miss

of technology-related threat assessment modules; and basing STAR production around life-cycle/design-related events instead of milestones.

DoD Threat Library: Today's Capstone Threat Assessments are used as de facto sources for most STAR content, but with all the standardization issues detailed above. Replacement of the Capstone volumes with a centrally managed DoD library of technology topic assessments would provide customers and STAR authors with an identifiable, current and authoritative source for each topic relevant to acquisition programs.

Key advantages of a centrally controlled DoD threat library:

- Centralized threat content ensures a single, identifiable source is provided for the intelligence community and all OSD/Service customers on a given topic, which eliminates the potential for contradictory information presented to decision makers on the same topic.
- A central DoD threat library should enable faster production of threat assessments, by maintaining a set of reference assessments in a validated state.
- Central control of all STAR topics provides a means to identify infrequently updated assessments and to regularly update all technology topics relevant for programs.
- An online threat library, based on the Secret Internet Protocol Router Network, would provide the required data for future searchable tools, useful to generate a set of relevant threats for considering planned capabilities or for developing program requirements (e.g., providing the requirements

community with a tool for considering threats during requirements development efforts).

The Service intelligence centers and related STAR producers also would benefit from efficiencies gained through eliminating redundant production of the same assessment topics in multiple, simultaneous, yet separately produced, assessments.

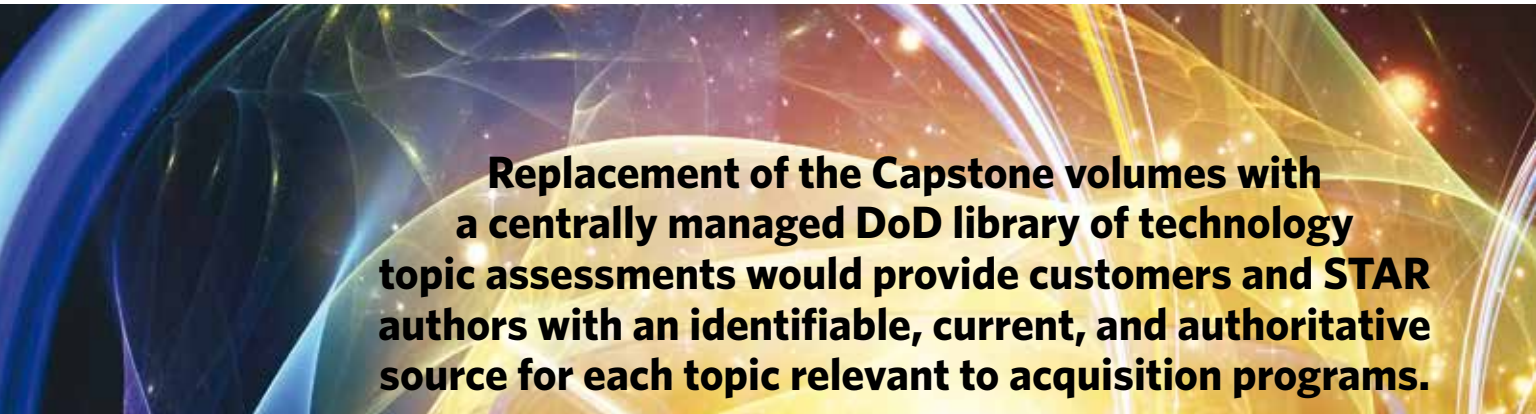
There are several reasons to standardize the content of all threat assessments provided to the acquisitions community, regardless of whether this is accomplished within a centrally controlled DoD threat library.

- Today's threat assessments often exceed 400 pages, and the varying level of detail across each topic often buries key points in unnecessary detail.
- The decisional value of threat assessments to the acquisition, requirements and test communities should be significantly improved. Assessments should state all threats in terms of "most likely" or "most stressing," which should clearly draw a line for program officials deliberating on performance thresholds (minimum acceptable capability) versus performance objectives (desired capability). All "most stressing" example systems should also include the estimated inventory of those systems.

Program Event-Based Threat Assessment Production: We propose four threat assessments that will be delivered during a program's life cycle, each carefully tailored for specific customer sets performing specific functions during a program timeline.

planned program capabilities listed in the Initial Capability Document (ICD). ITEAs will include relevant threat key judgments to drive potential material solutions and inform the development of threat sensitive KPPs and KSAs.

- **Milestone A STAR (MS A STAR):** Delivered at Milestone A, at roughly 20 to 50 pages long. The primary MS A STAR customer is the capability developer, and the STAR would inform the "downward V" of the technology development phase as depicted on the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System diagram (a.k.a., the "horse blanket"). This STAR will build on the ITEA and add detail by drawing on information from the AoA report, such as the identification of enabling and critical technologies, as well as great specificity in likely program attributes. The Milestone A STAR also will contain critical intelligence parameters (CIPs) used to shape the tradespace identified in KPPs and KSAs.
- **System Requirements Review STAR (SRR STAR):** Delivered by the system requirements review, at fewer than 200 pages. The SRR STAR main customers are the program manager, preliminary design review team, and the test community. The SRR STAR would build upon the Milestone A STAR, and will become more system specific by using information from the draft Capability Development Document (CDD), including the DoD architectural framework views (i.e., OV-1, SV-6), KPPs, and KSAs. Projected enemy force numbers drawn from intelligence community projections will be included to highlight "most likely" threats.
- **Test Readiness Review STAR (TRR STAR):** Delivered 90 days before the TRR, and shorter than 200 pages. The TRR STAR main customers are the program manager, full-rate



Replacement of the Capstone volumes with a centrally managed DoD library of technology topic assessments would provide customers and STAR authors with an identifiable, current, and authoritative source for each topic relevant to acquisition programs.

- **Initial Threat Assessment Report (ITEA):** Delivered 30 days into the analysis of alternatives (AoA), and roughly 20 pages long. The ITEA would be written for the systems commands and capability developers, and it would be used to inform the AoA decision, leveraging the DoD threat library and its DoD-validated key judgments. The advantage of the ITEA is to reduce the possibility of a program told one thing during requirements generation, then held to a different intelligence community judgment during later operational testing. ITEAs should focus on threats to

production decision team and the test community. This will build on the SRR STAR and will be more tailored to the program by including a complete system description. This STAR will inform the full-rate production decision and TRR.

A Streamlined Production Process for Threat Assessments

The DoD has assigned specific responsibility (and topic authority) to the Service intelligence centers and DIA for most technology assessment topics. Threat assessments would

heavily leverage a DoD threat library as a primary source for threat information, with references to additional databases and sources of further detail.

- DIA or another appropriate DoD-level organization would task the Defense Intelligence Enterprise for production of all DoD library topics, annually or biennially. All DoD threat library topics would be directly produced by the topic-responsible Service intelligence center, which would eliminate the risk that relevant subject matter experts might be skipped during STAR production and thereby miss the chance to make urgent changes for a given STAR topic.
- All DoD threat library content would be reviewed by the entire DoD intelligence community per current practice for Capstone Threat Assessments and STARs, but each topic would only be reviewed once by relevant subject matter experts every 1 or 2 years. Subjects requiring interim updates could be easily produced due to the small size of each topic assessment, with update notification sent to all regular STAR producers.
- Program STAR production would start with a review of all DoD threat library topics to identify topics relevant to the program and any new topics that should be produced.
- STAR authors would assemble all relevant topics from the DoD threat library, and would introduce each topic with a “relevance to program” statement, with assistance from the supporting systems command intelligence organization.
- Program offices would continue to provide system descriptions and acquisition documents (ICD, CDD, etc.).
- Systems command intelligence organizations would continue to develop critical intelligence parameters for the JCIDS sponsor and program office, with assistance from the Service intelligence center and DIA.

- DIA validation would consist of verification that the current set of DoD threat library assessments has been reflected in the STAR. Any late-breaking Service center assessments that would alter DoD analytic judgments would be included, which would also drive interim updates to the DoD threat library.
- ACAT ID STAR coordination will be reduced to the primary stakeholders, including the applicable Service intelligence centers, DIA, and the program office, thereby greatly reducing the number of work hours community wide. ACAT IC programs (and below) could use the same production process without DIA involvement to further standardize threat-assessment production.
- JCIDS sponsors or program offices retain their ability to request interim STAR updates, and program managers would retain the local intelligence support office for additional threat information.

We believe this proposal will dramatically improve the value of STAR content to the DoD customer set while enhancing both efficiency and responsiveness of the intelligence community in support of defense acquisition programs in general. We also believe this concept probably is the only conceivable means for the intelligence community to meet the increased demand for acquisition-related intelligence in an age of decreased resources. &

The views expressed in this paper are those of the authors and do not reflect official policy or positions of the Defense Intelligence Agency, the Department of Defense or the U.S. government.

*The authors can be contacted at **christopher.boggs@dodiis.mil, jonathan.gilbert@dodiis.mil, paul.reinhart@dodiis.mil, dustin.thomas@dodiis.mil** and **brian.vanyo@dodiis.mil**.*

Expand Your Network

- Available 24/7
- More than 40 different acquisition-related Communities of Practice and Special Interest Areas
- Access to policies, guidance, tools, and references
- Automatic notification of new content (by subscription only)
- Ability to tap into the wisdom of the community
- Interact, share resources, ideas, and experiences with fellow practitioners across DoD and industry

Acquisition Community Connection (ACC)

Where the Defense Acquisition Workforce Meets to Share Knowledge

<https://acc.dau.mil>