



ACQUISITION INNOVATION
RESEARCH CENTER

Test and Evaluation Methods for Middle-Tier Acquisition (MTA) – Base Year

EXECUTIVE SUMMARY

SEPTEMBER 2023

PRINCIPAL INVESTIGATOR:

Dr. Laura Freeman, *Virginia Tech National Security Institute*

CO-PRINCIPAL INVESTIGATOR:

Mr. Geoff Kerr, *Virginia Tech National Security Institute*

SPONSORS:

Dr. Sandra Hobson, Deputy Director, Strategic Initiatives, Policy, and Emerging Technologies, Office of the Director, Operational Test and Evaluation (DOT&E)

Dr. Kristen Alexander, Chief Learning and Artificial Intelligence Officer, DOT&E

Dr. Jeremy Werner, Chief Scientist, DOT&E

Dr. Tyler Englestad, Emerging Technologies Advisor, DOT&E

Mr. Paul Lowe, Executive Officer for DOT&E Strategic Initiatives, Policy and Emerging Technologies, DOT&E



DISTRIBUTION STATEMENT A.
Approved for public release:
distribution unlimited.

In support of Pillar 1, the AIRC research team focused on maturing evaluation methodologies for Joint Warfighting Concepts with the development of a fundamental Joint Test Concept (JTC). The team established a broad Community of Interest (COI) to explore numerous aspects and challenges around the test and evaluation of Joint Warfighting Concepts. The team conducted a three-phased research approach, each of which concluded in a workshop that first shaped and bound the focus of the research team, developed initial JTC priorities, and concluded with a tabletop simulation of joint operation assessment.

In support of Pillar 2, the research team explored current threats to DoD data and how these threats can be mitigated. The team responded with a Data Security paper that expands upon the findings. In addition to the data security aspects of accelerating Weapons that Work, the research team developed Bayesian-based approaches to leverage contractor testing, development testing, live fire testing, modeling and simulation results, and operational test to ensure more rapid test and evaluation of weapon systems to expedite fielding of warfighting capabilities. In the future efforts, the research team will be working on a Model Based Test and Evaluation Plan (MB TEMP) and supporting the advancement of the Integrated Decision Support Key (IDSK) beyond the initial efforts described in the Digital Engineering for T&E section of this report.

In support of Pillar 4, the research team investigated improved methods for test and evaluation of Artificial Intelligence (AI) /Machine Learning (ML) -enabled DoD systems. The team has developed recommendations on how to ensure AI/ML systems have proper training data while continuing to evaluate and inform system performance while in use. The team further explored methods to evaluate AI/ML systems when the T&E community has limited or no detailed understanding of the underlying AI/ML algorithms within a system. Also, in support of Pillar 4, the multi-university team helped further the application of digital engineering practices in support of Test and Evaluation. With a realistic look at tooling challenges and current cultural challenges, the team made practical recommendations on the use of Model Based Systems Engineering (MBSE) methods for test planning and execution, in addition to digital linkage from mission requirements through operational assessment. Lastly, Pillar 4 efforts also included maturing a framework to automate security Penetration Testing. After conducting cyber security research, the team developed early test software methods that enable cyber physical system penetration testing to be automated in concert with a continuous innovation, continuous deployment product development environment. In the next year, the team intends to test these capabilities with case study DoD products.

Finally, in support of DOT&E emerging priorities, the research team supported numerous tasks that included providing policy reviews and recommendations, offering workforce planning concepts, developing exemplar IDSK, and delivering technical support to T&E meetings, workshops, and conferences. The research impact has been wide reaching. The AIRC team hosted 5 different workshops (2 under WRT-1070), delivered 14 presentations/webinars/briefings (10 under WRT-1070), authored 11 reports/publications (8 under WRT-1070), and developed 3 test related tools/applications (2 under WRT-1070).

Based on the foundational work performed in this initial year, the AIRC research team looks forward to building on the year 1 recommendations and tooling by performing case study evaluations on actual DoD programs of record and on conceptual programs. The team also intends to introduce workforce development efforts in the follow-on year in support of DOT&E's fifth pillar, Foster an Agile and Enduring T&E Enterprise Workforce.

DISCLAIMER

Copyright © 2023 Stevens Institute of Technology and Virginia Tech National Security Institute (VTNSI). All rights reserved.

The Acquisition Innovation Research Center is a multi-university partnership led and managed by the Stevens Institute of Technology and sponsored by the U.S. Department of Defense (DoD) through the Systems Engineering Research Center (SERC)—a DoD University-Affiliated Research Center (UARC).

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) and the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) under Contract HQ0034-19-D-0003, TO#0396.

The views, findings, conclusions, and recommendations expressed in this material are solely those of the authors and do not necessarily reflect the views or positions of the United States Government (including the Department of Defense (DoD) and any government personnel), the Stevens Institute of Technology, or Virginia Tech National Security Institute.

No Warranty.

This Material is furnished on an “as-is” basis. The Stevens Institute of Technology and Virginia Tech National Security Institute make no warranties of any kind—either expressed or implied—as to any matter, including (but not limited to) warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material.

The Stevens Institute of Technology and Virginia Tech National Security Institute do not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

