DHS SCIENCE AND TECHNOLOGY

Test and Evaluation

The Key to Successful Acquisition Outcomes

Homeland Security
Science and Technology

Steve Hutchison
Director
Office of Test and Evaluation

32nd Annual National T&E Conference

Strategic T&E Collaboration: Government & Industry Partnering to Achieve Decisive Operational Advantage

autonomous learning systems

Third Offset Strategy?

human-machine collaboration

human-machine combat teaming

assisted human operations

network-enabled autonomous weapons and high-speed weapons

32nd Annual National T&E Conference

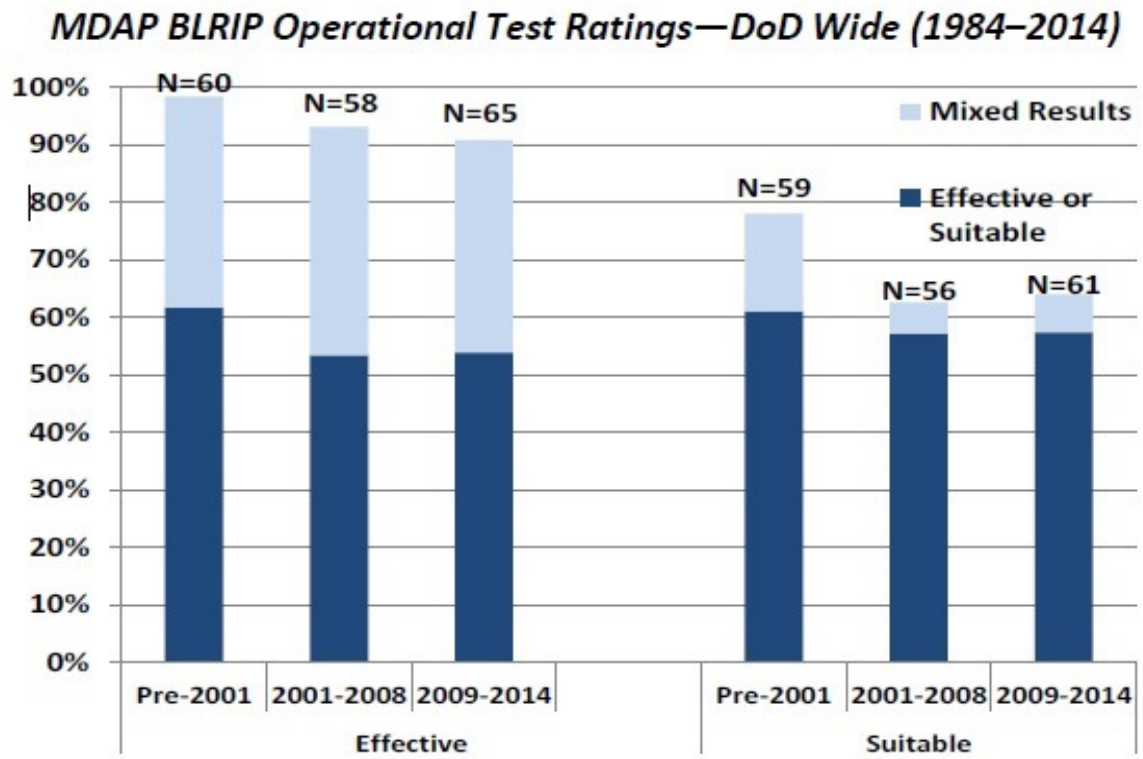
Strategic T&E Collaboration: Government & Industry Partnering to Achieve Decisive Operational Advantage

'Third Offset' Strategy Calls for Fresh Thinking
Artie Mabbett and John Kovach

"…technology development is not our biggest challenge in meeting our adversaries' military posture; fielding innovative technologies more rapidly and efficiently is the challenge we face today."

Performance of the Defense Acquisition System

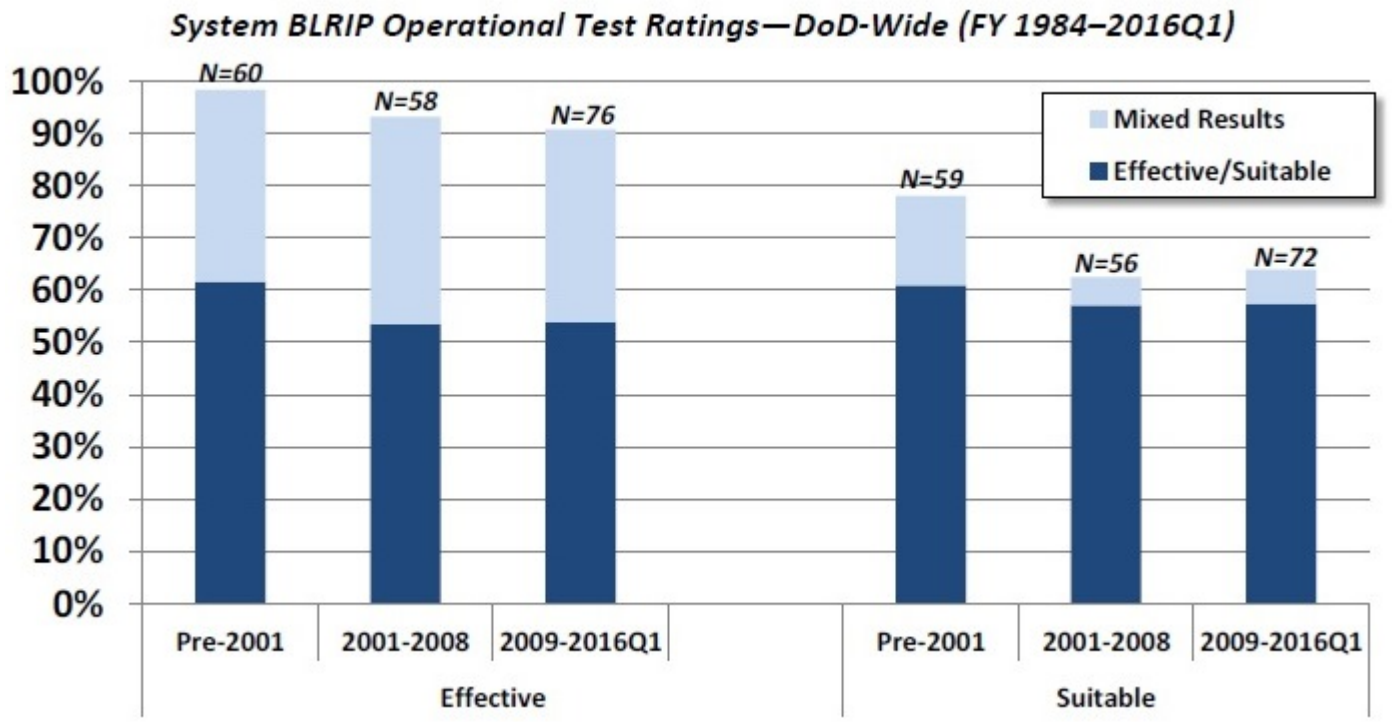
2015 Report



http://www.acq.osd.mil/fo/docs/Performance-of-Defense-Acquisition-System-2015.pdf

Performance of the Defense Acquisition System

2016 Report

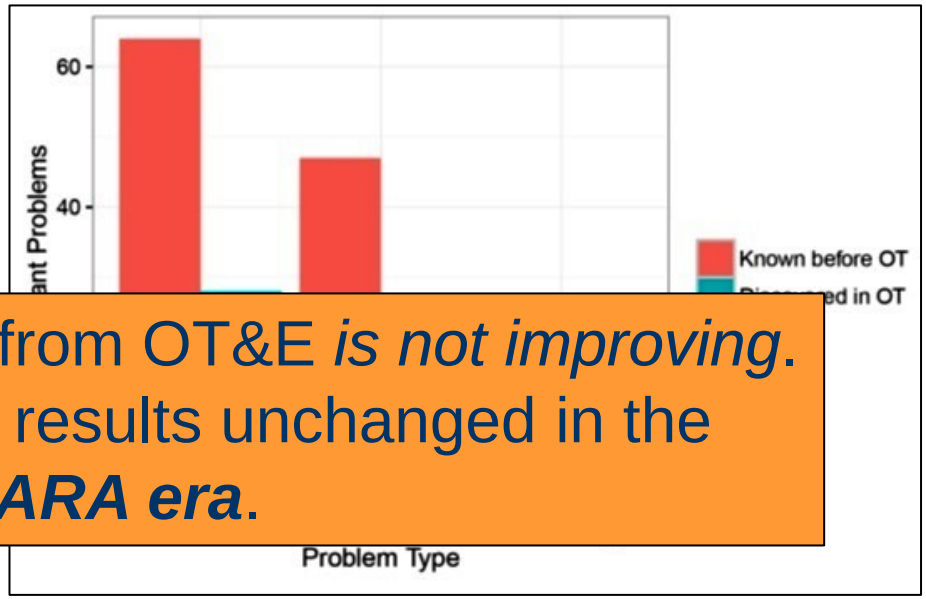


http://www.acq.osd.mil/fo/docs/Performance-of-Defense-Acquisition-System-2016.pdf

Problem Discovery Affecting OT&E

DOT&E FY2016 Annual Report

- 74 programs had a total of 83 operational tests
- 30% (25/83) of the operational
- effectiveness, suitability, or survivability.
- 36 percent (30/83) discovered significant problems that were ***unknown prior to operational testing***.



Rate of favorable outcomes from OT&E *is not improving*.
Note for T&E community: results unchanged in the ***post-WSARA era***.

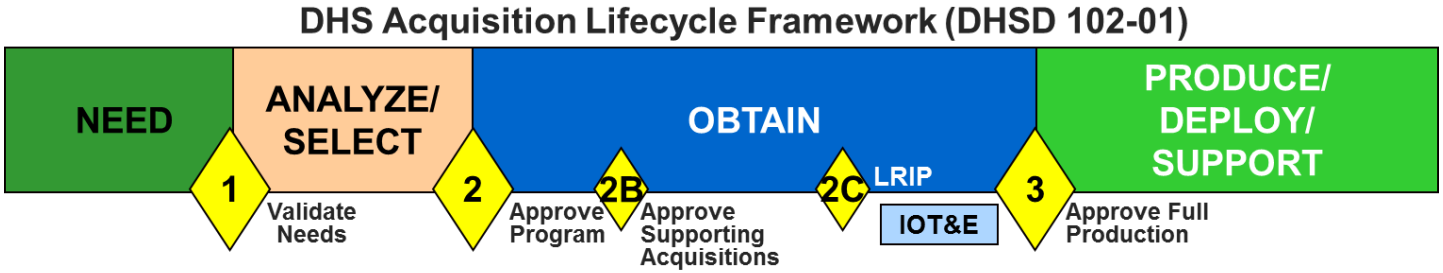
http://www.dote.osd.mil/pub/reports/FY2016

T&E Role in Improving Acquisition Outcomes

- Our job as testers is to *help programs succeed*.*
- *Independent* T&E must be a *lifecycle* activity.
  - Initial production decision should not be made based solely on vendor data.
- Challenge the *status quo*; don't bring "old-T&E" to a new program.
  - DT&E matters
    - DT&E is not "technical testing"
    - Users must be involved in DT&E
  - OTAs *can* do DT&E
  - The purpose of DT&E is *not* "to determine readiness for OT&E"
    - determine readiness to begin production
  - Cybersecurity is *not* some other tester's responsibility
  - Effectiveness and Suitability do not adequately evaluate today's systems
- Fix this in the schoolhouse; practice it in program engagement.

**Test and Evaluation Myths and Misconceptions*, Defense AT&L, Jan-Feb 2015

Leading Change in DHS



Department of Homeland Security
DHS Delegation Number: 10003
Revision Number: 00
Issue Date: 05/06/2009

DELEGATION TO THE DIRECTOR OF OPERATIONAL TEST AND EVALUATION

"The delegated authority herein does not extend to developmental test and evaluation."

Department of Homeland Security
DHS Delegation Number: 10003
Revision Number: 01
Issue Date: 6/17/2016

DELEGATION TO THE DIRECTOR OF TEST AND EVALUATION

"The delegated authority extends to developmental testing and evaluation to appropriately inform Acquisition Decision Events 2 C/3 as negotiated and documented during development of the Test and Evaluation Master Plan."

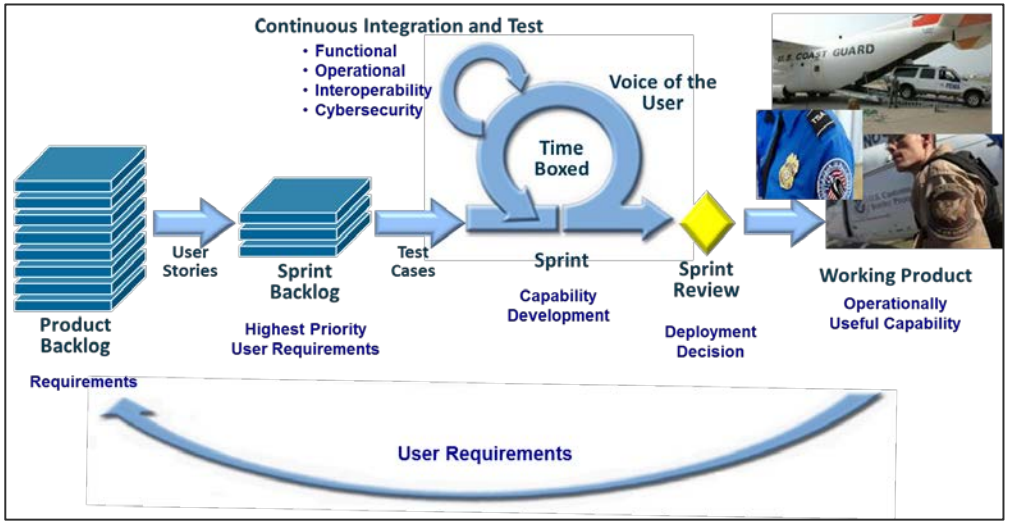
Leading Change in DHS

USCG Polar Ice Breaker

International Engagement: Canada National Research Council Ice Lab

Leading Change in DHS

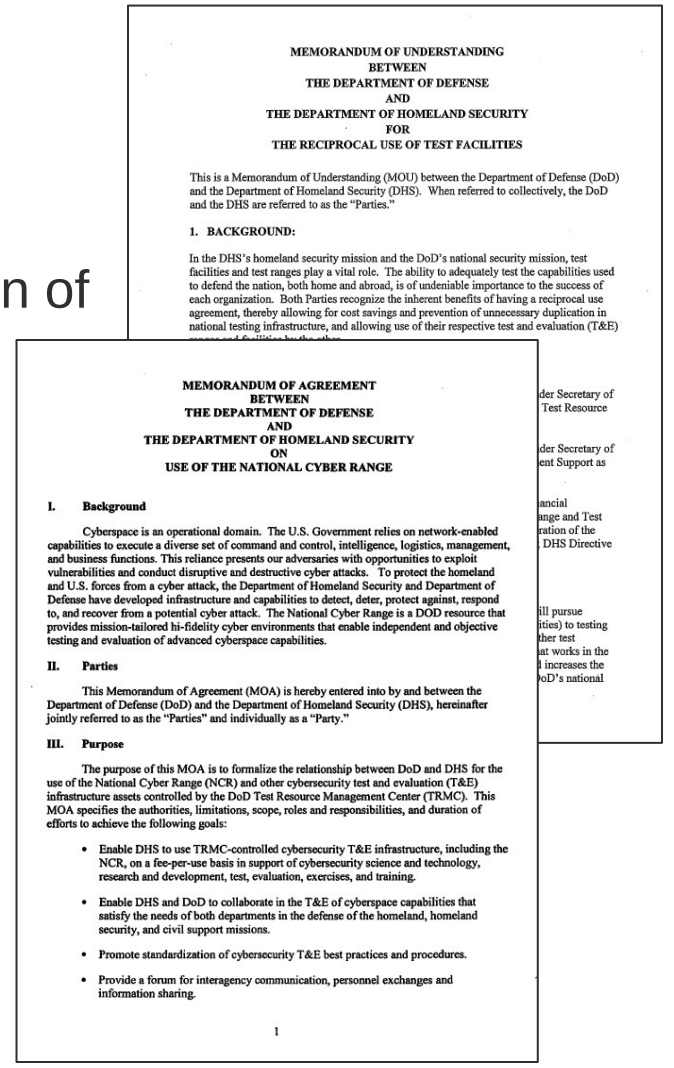
- DHS Agile Pilot Programs
  - Student Exchange Visitor Information System (ICE)
  - National Flood Insurance Program IT Phoenix (FEMA)
  - Technology Infrastructure Modernization (TSA)
  - Grants Management Modernization (FEMA)
  - Verification Modernization (USCIS)
- *Agile training is required*
- Agile T&E WIPT
  - TEMP for Agile programs
  - Integrated Test Plans



Leading Change in DHS

Other T&E Initiatives:

- TEMP Instruction
- T&E Management Guide
- Procedures for Operational Test and Evaluation of Cybersecurity
- Reliability
- Threat Assessments for Acquisition Programs
- T&E Career Field Certification *IT Track*
- Operational Test Director Course
- JIATF-S partnership
- MOU on Reciprocal Use of Test Facilities
- MOA on Use of the National Cyber Range



MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DEPARTMENT OF DEFENSE
AND
THE DEPARTMENT OF HOMELAND SECURITY
FOR
THE RECIPROCAL USE OF TEST FACILITIES

This is a Memorandum of Understanding (MOU) between the Department of Defense (DoD) and the Department of Homeland Security (DHS). When referred to collectively, the DoD and the DHS are referred to as the "Parties."

1. BACKGROUND:

In the DHS's homeland security mission and the DoD's national security mission, test facilities and test ranges play a vital role. The ability to adequately test the capabilities used to defend the nation, both home and abroad, is of undeniable importance to the success of each organization. Both Parties recognize the inherent benefits of having a reciprocal use agreement, thereby allowing for cost savings and prevention of unnecessary duplication in national testing infrastructure, and allowing use of their respective test and evaluation (T&E)

MEMORANDUM OF AGREEMENT
BETWEEN
THE DEPARTMENT OF DEFENSE
AND
THE DEPARTMENT OF HOMELAND SECURITY
ON
USE OF THE NATIONAL CYBER RANGE

I. Background

Cyberspace is an operational domain. The U.S. Government relies on network-enabled capabilities to execute a diverse set of command and control, intelligence, logistics, management, and business functions. This reliance presents our adversaries with opportunities to exploit vulnerabilities and conduct disruptive and destructive cyber attacks. To protect the homeland and U.S. forces from a cyber attack, the Department of Homeland Security and Department of Defense have developed infrastructure and capabilities to detect, deter, protect against, respond to, and recover from a potential cyber attack. The National Cyber Range is a DOD resource that provides mission-tailored hi-fidelity cyber environments that enable independent and objective testing and evaluation of advanced cyberspace capabilities.

II. Parties

This Memorandum of Agreement (MOA) is hereby entered into by and between the Department of Defense (DoD) and the Department of Homeland Security (DHS), hereinafter jointly referred to as the "Parties" and individually as a "Party."

III. Purpose

The purpose of this MOA is to formalize the relationship between DoD and DHS for the use of the National Cyber Range (NCR) and other cybersecurity test and evaluation (T&E) infrastructure assets controlled by the DoD Test Resource Management Center (TRMC). This MOA specifies the authorities, limitations, scope, roles and responsibilities, and duration of efforts to achieve the following goals:

- Enable DHS to use TRMC-controlled cybersecurity T&E infrastructure, including the NCR, on a fee-per-use basis in support of cybersecurity science and technology, research and development, test, evaluation, exercises, and training.
- Enable DHS and DoD to collaborate in the T&E of cyberspace capabilities that satisfy the needs of both departments in the defense of the homeland, homeland security, and civil support missions.
- Promote standardization of cybersecurity T&E best practices and procedures.
- Provide a forum for interagency communication, personnel exchanges and information sharing.

1

Summary

We can improve the rate of favorable outcomes.
Partnering with the programs is key to success.

Homeland Security Operators are counting on us to get it right.