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

28 March 2017

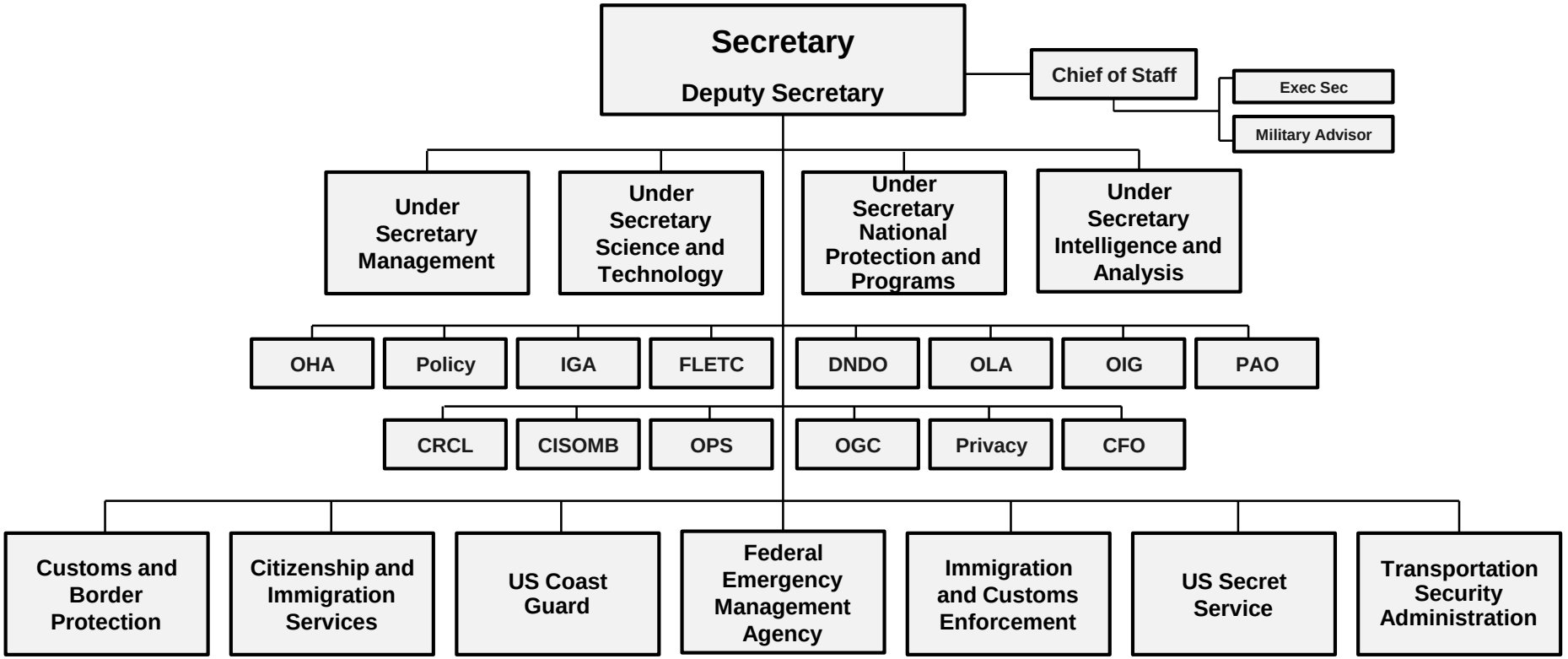
Department of Homeland Security

John F. Kelly
Secretary of Homeland Security

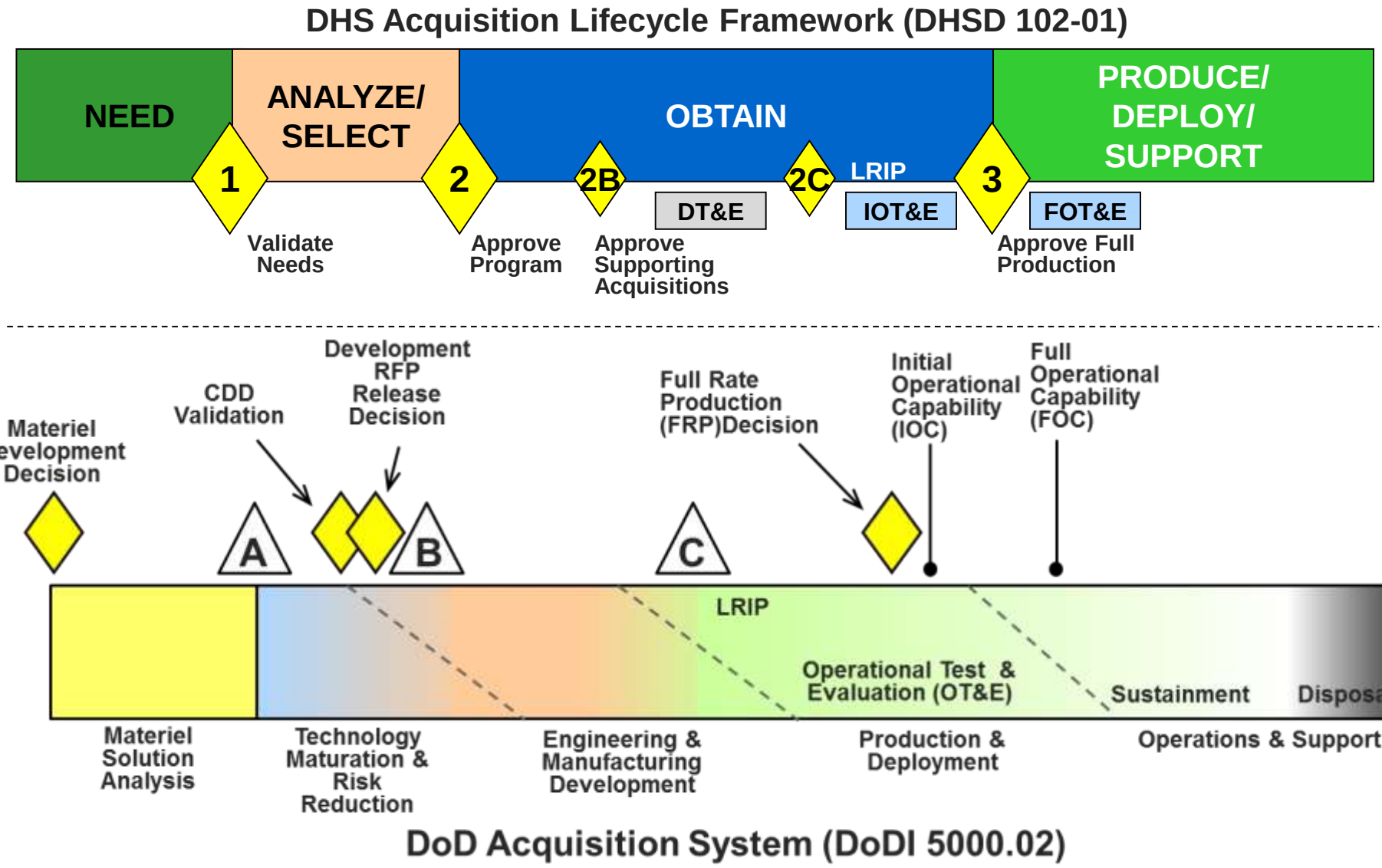
With honor and integrity, we will safeguard the American people, our homeland, and our values.

- Prevent Terrorism and Enhance Security
- Secure and Manage Our Borders
- Enforce and Administer Our Immigration Laws
- Safeguard and Secure Cyberspace
- Strengthen National Preparedness and Resilience

Organization

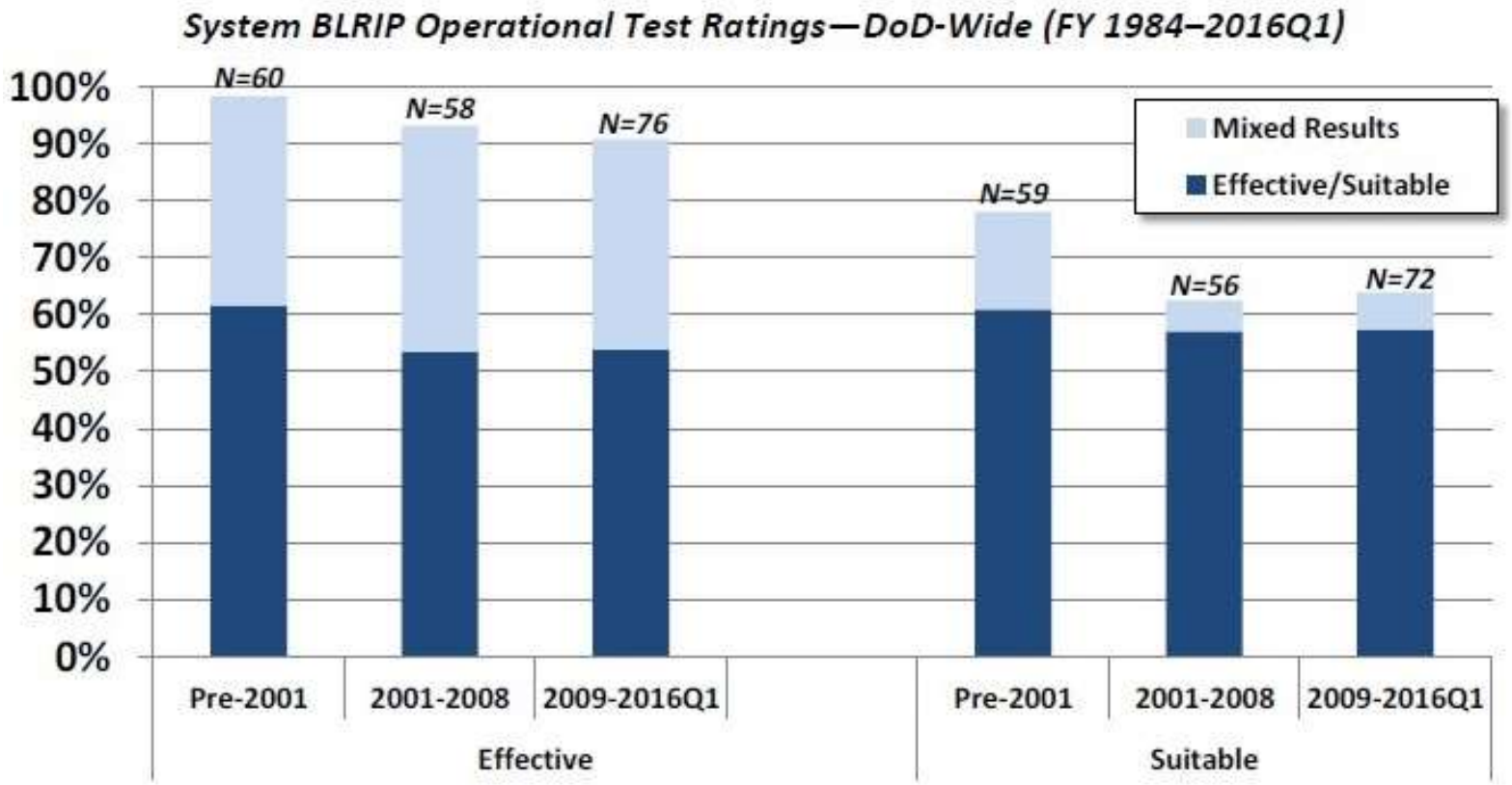


Acquisition: DHS vs DoD



Performance of the Defense Acquisition System

2016 Report

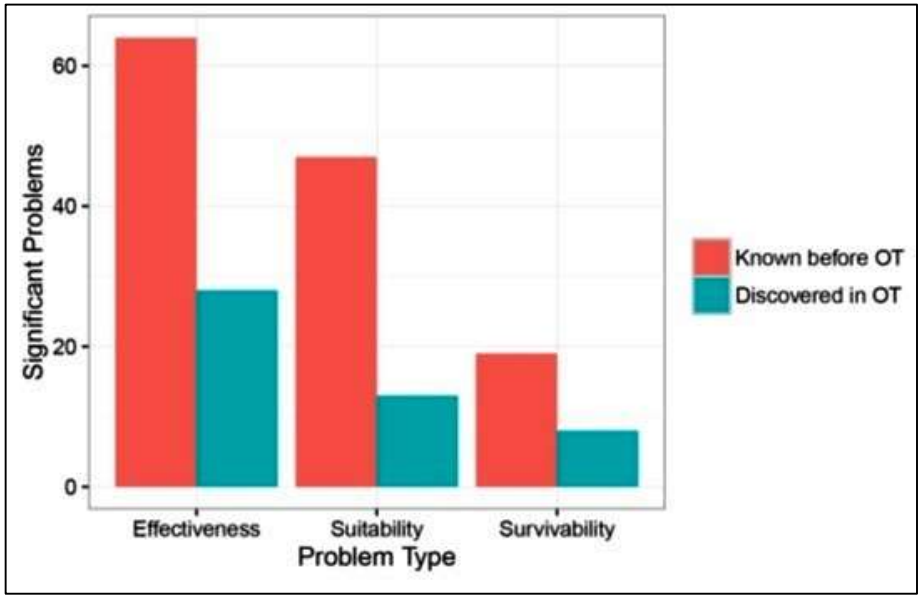


http://www.acq.osd.mil/fo/docs/Performance-of-Defense-Acquisition-System-2016.pdf

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 tests had no significant problems
- 70% (58/83) revealed problems significant enough to adversely affect determination of system effectiveness, suitability, or survivability.

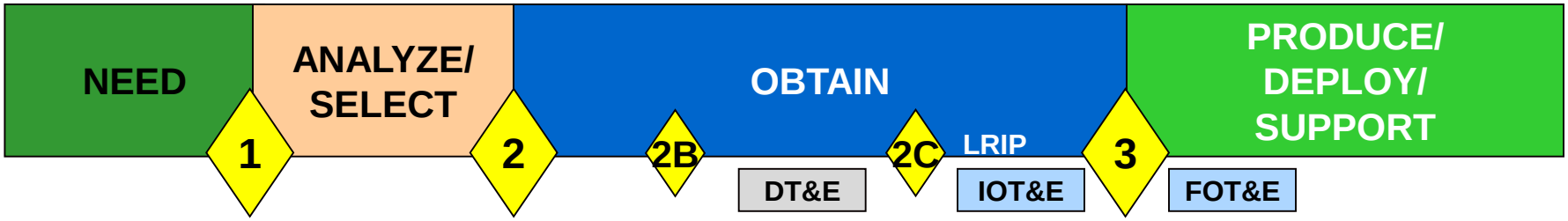


- 36 percent (30/83) discovered significant problems that were ***unknown prior to operational testing***.

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

DHS Acquisition

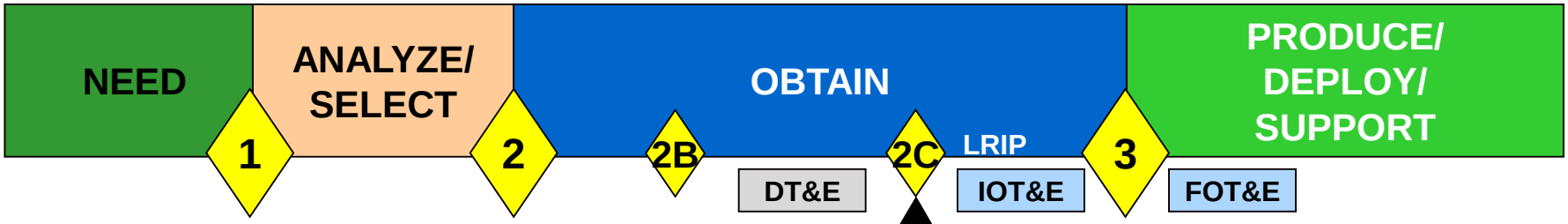
DHS Acquisition Lifecycle Framework (DHSD 102-01)



- 4 Phase; 3 Acquisition Decision Events (ADEs)
- 3 Program Levels
  - Level 1: > $1B
  - Level 2: $300M - $1B
  - Level 3: <$300M
- Master Acquisition Oversight List
  - 113 programs; 72 Major (Level 1 or 2)
  - Approximately 2/3 Information Technology

Shift Left!

DHS Acquisition Lifecycle Framework (DHSD 102-01)



Where we can make a difference

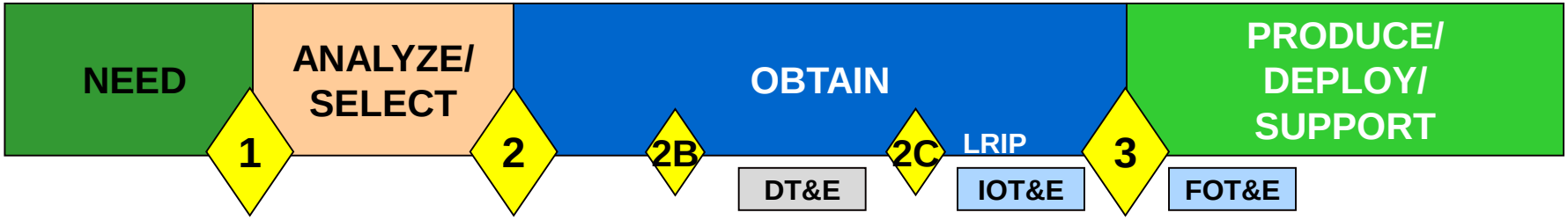
- **Requirements engineering**
- **Systems engineering**
- **Developmental T&E**
- **Standards integration**

Start of Production: Determinant of Program Success

Where we have been focused

Cybersecurity Test and Evaluation

DHS Acquisition Lifecycle Framework (DHSD 102-01)



Cybersecurity Requirements	*Attack Surface*	*Kill Chain*	T&E
• ORD, MNS, etc • System Characterization • Threat	• Local • Adjacent • Network	• Deny • Disrupt • Modification • Exfiltration	• Adversarial

A DHS Red Team Pilot

- Program initiative to remediate an OT finding. Program's cooperation was key to successful pilot
- Developed plan for robust "red team" test
  - Leveraged DOT&E contract with JHU APL
- Rules of Engagement documented and signed.
- Red team:
  - open source intel collection
  - live ops in production and user acceptance test environments
- Results (described on next slide) provided to PMO for remediation.
  - DOT&E report addendum: program is operationally cybersecure.
- Low cost; high ROI
  - Report recommendations served to remediate vulnerabilities
  - Resulted in new CVE filing (common vulnerabilities and exposures)

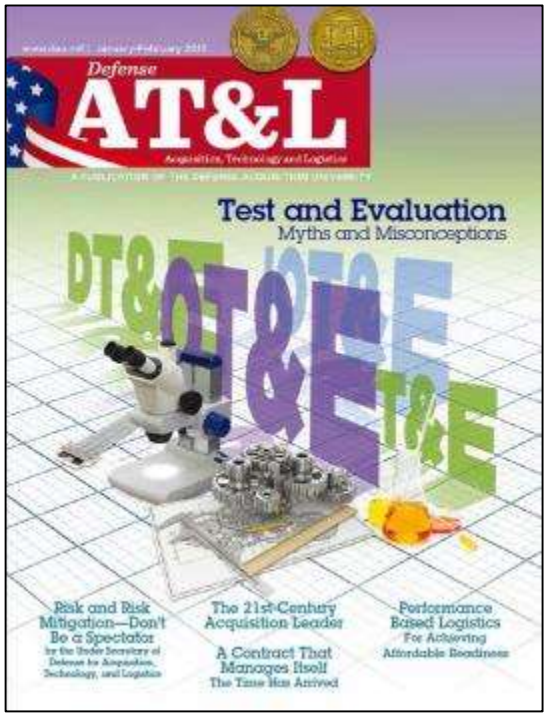
Every major program should conduct adversarial testing

Red Team Pilot Results

- Open Source intel gathering found:
  - key program personnel and regular users
  - physical location of the infrastructure
  - IP range of production & user acceptance test (UAT) environments
  - partner organizations
  - 3rd party components
  - non-“.gov” systems to provide information about program
- Live Ops:
  - access to core capability thru hosted applications
  - captured traffic used for admin account hijacking, transaction spoofing, privilege escalation
  - cross site scripting, application bypass/evasion
  - non-solution access points can retain credentials after use

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.

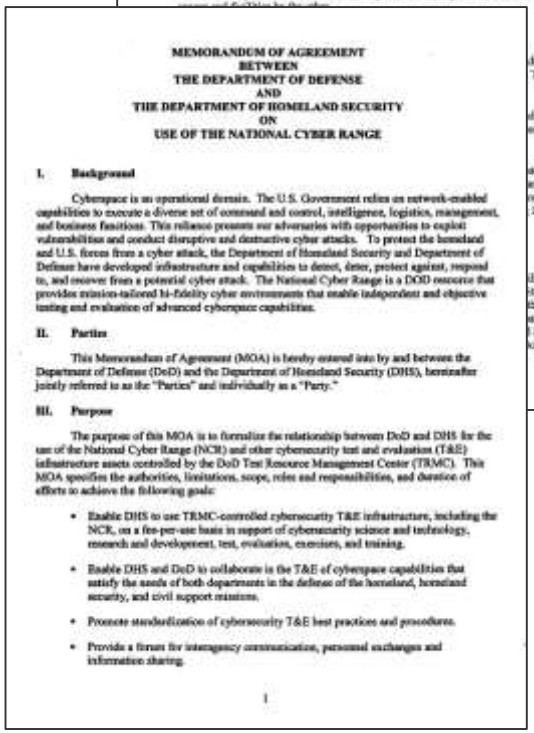


AT&L Magazine
Jan-Feb 2015

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 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

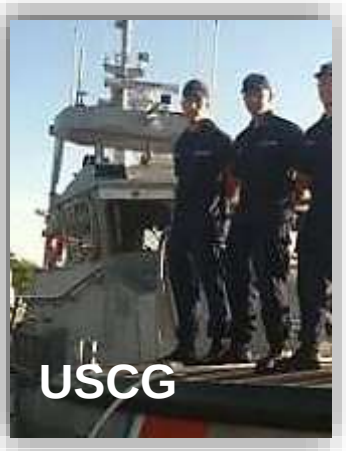
The purpose of this MOA is to formalize the relationship between DoD and DHS for the use of the National Cyber Range (NCR) and other cybersecurity test and evaluation (T&E) infrastructure assets controlled by the DoD Test Resource Management Center (TRMC). This MOA specifies the authorities, limitations,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