DHS SCIENCE AND TECHNOLOGY

Cybersecurity Test and Evaluation

Closing the Gap between Authority to Operate and Operating Securely

18 July 2017

Homeland Security
Science and Technology

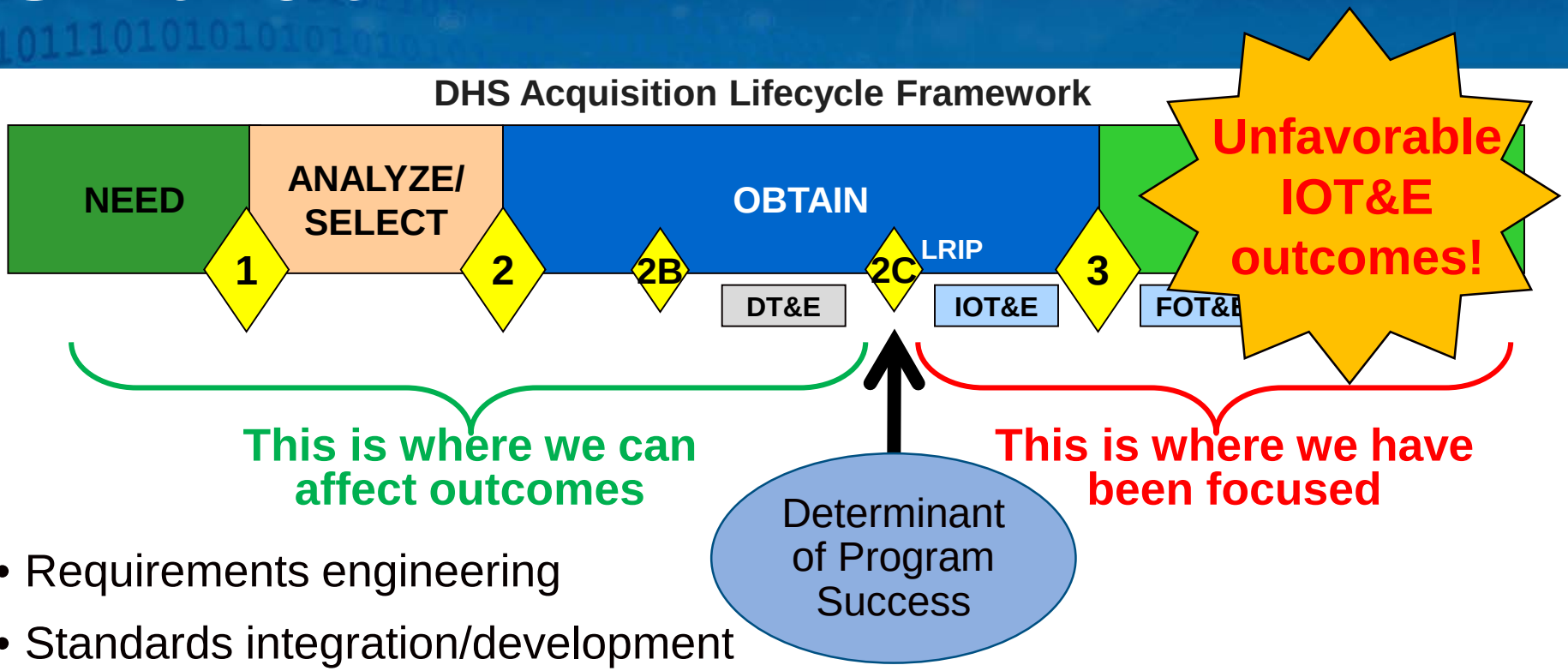
Steve Hutchison
Director
Office of Test and Evaluation

The Gap

Our adversaries are not limited to exploiting vulnerabilities within the set of *Security Controls* defined by the Risk Management Framework.

Operational Cybersecurity testing is about testing our systems the way the adversary is testing our systems!

Shift Left!



- Requirements engineering
- Standards integration/development
- Early identification *and remediation* of technical risks and key failure modes
  - Performance: at scale and under load
  - Reliability: throughout the operational envelope
  - Interoperability: exchange data in support of the mission
  - Cybersecurity: operational resilience in contested cyber domain

Program Managers must *set the conditions* for a favorable outcome

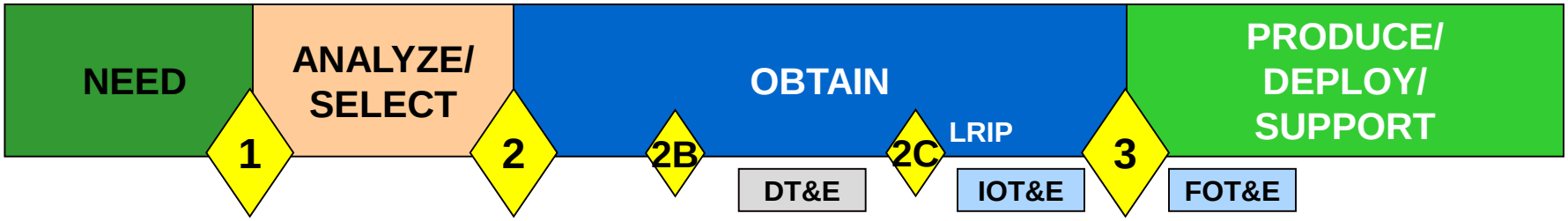
Procedures for Operational Test and Evaluation of Cybersecurity

- Purpose:
  - Inform decision-making process
  - Improve *operational resilience* of network-enabled capabilities
- Applicability
  - All acquisition programs subject to DOT&E oversight.
- Policy:
  - include cybersecurity in Test and Evaluation Master Plans
    - Mission context
    - Threat
    - Integrated Evaluation Framework
    - Resources
  - Operational Test Agents (OTAs) will include cybersecurity in OT&E concepts, plans, and reports
  - OT&E will include realistic threat portrayal to determine mission effects
- DOT&E will include cybersecurity in LOAs
  - Effectiveness, Suitability, Cybersecurity


Homeland Security

Cybersecurity in the Integrated Evaluation Framework

DHS Acquisition Lifecycle Framework (DHS Directive 102-01)



Cybersecurity *Decision Support Questions*

1 Are cybersecurity requirements measurable, testable, achievable?

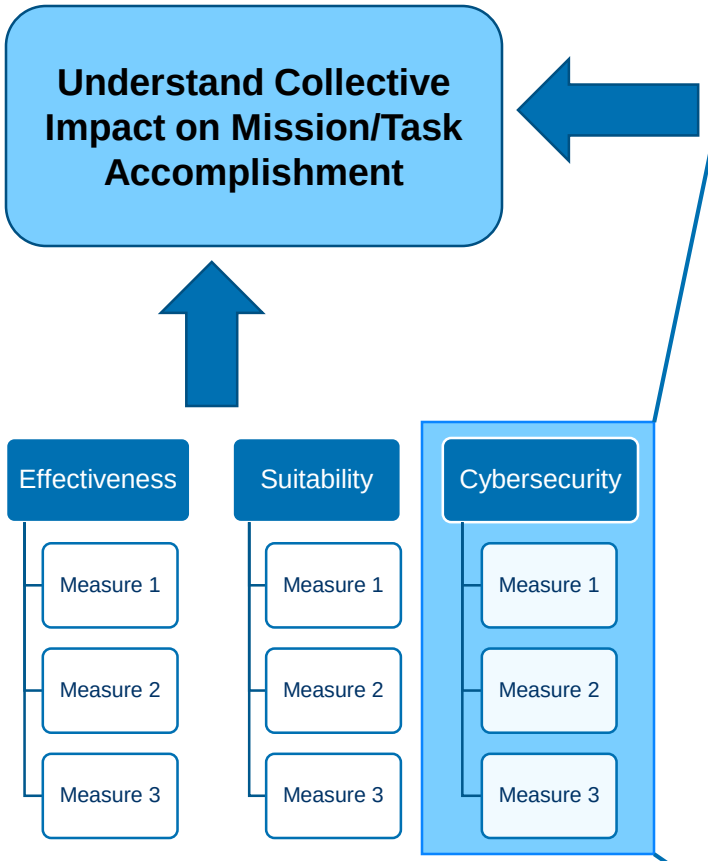
2 Does the system software feature appropriate design-for-security elements?

2B Is there a sound plan to collect adequate cybersecurity data to inform production and deployment decisions?

2C Is the system sufficiently cyber secure to enter initial production?

3 Is the system operationally resilient in the cyber domain?

Sample Cybersecurity Evaluation Structure



Cybersecurity

Is this capability resilient to cyber attack?

Denial of Service

- Probability of Occurrence
- Duration
- Repeatability
- Attack Resources

Degradation of Service

- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Degree of Degradation
- Attack Resources
- Defend Resources

Data Manipulation

- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Degree of Manipulation
- Attack Resources
- Defend Resources

Data Exfiltration

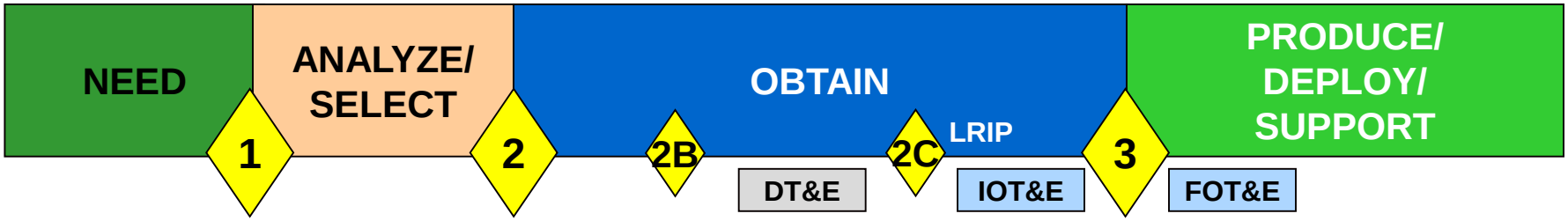
- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Significance of Exfiltration
- Attack Resources
- Defend Resources

External Pivoting

- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Attack Resources
- Defend Resources

Cybersecurity Test and Evaluation

DHS Acquisition Lifecycle Framework (DHS Directive 102-01)



- What are the Cybersecurity requirements?
  - ORD, System Characterization (Confidentiality, Integrity, Availability)
  - Threat Assessment
- What is the Attack Surface?
  - Local
  - Adjacent
  - Network
- Can the cyber adversary affect the mission (Kill Chain)?
  - Deny, Disrupt, Modify
  - Exfiltrate, Pivot

Test and Evaluation
- Threat-realistic (adversarial)
- Rules of Engagement (ROE)
- Determine mission impacts
- Remediate vulnerabilities

Is the system operationally resilient in the cyber domain?

The Red Team Pilot

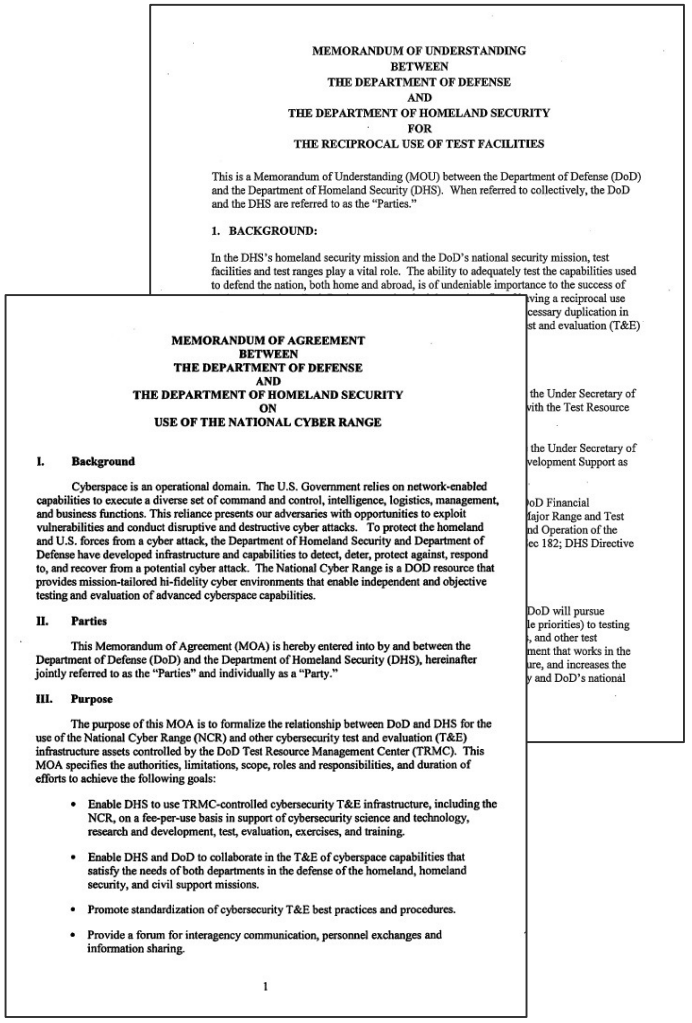
- Program initiative conduct robust “red team” test
  - Leveraged DOT&E contract with JHU APL
  - Rules of Engagement documented and signed
- Red team operations:
  - open source intel collection
    - key program personnel, regular users, and physical location of the infrastructure
    - IP range of production & user acceptance test (UAT) environments
    - partner organizations, 3rd party components
  - live ops in production and user acceptance test environments
    - accessed core capability thru hosted applications
    - captured traffic for admin account hijacking, transaction spoofing, privilege escalation
    - cross site scripting, application bypass/evasion
    - non-solution access points can retain credentials after use
- Results provided to PMO for remediation.
- Low cost; high ROI
  - Report recommendations served to remediate vulnerabilities
  - Resulted in new CVE filing (common vulnerabilities and exposures)

Every MAOL program should conduct Red Team testing

Other Resources

- MOU on Reciprocal Use of Test Facilities
  - Signed 26 October 2015
  - Expand capability set
  - Reduce costs
  - Reduce duplication

- MOA on Use of the National Cyber Range
  - Signed 21 July 2016
  - DHS use of NCR
  - DoD/DHS collaboration in cyber defense



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

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.

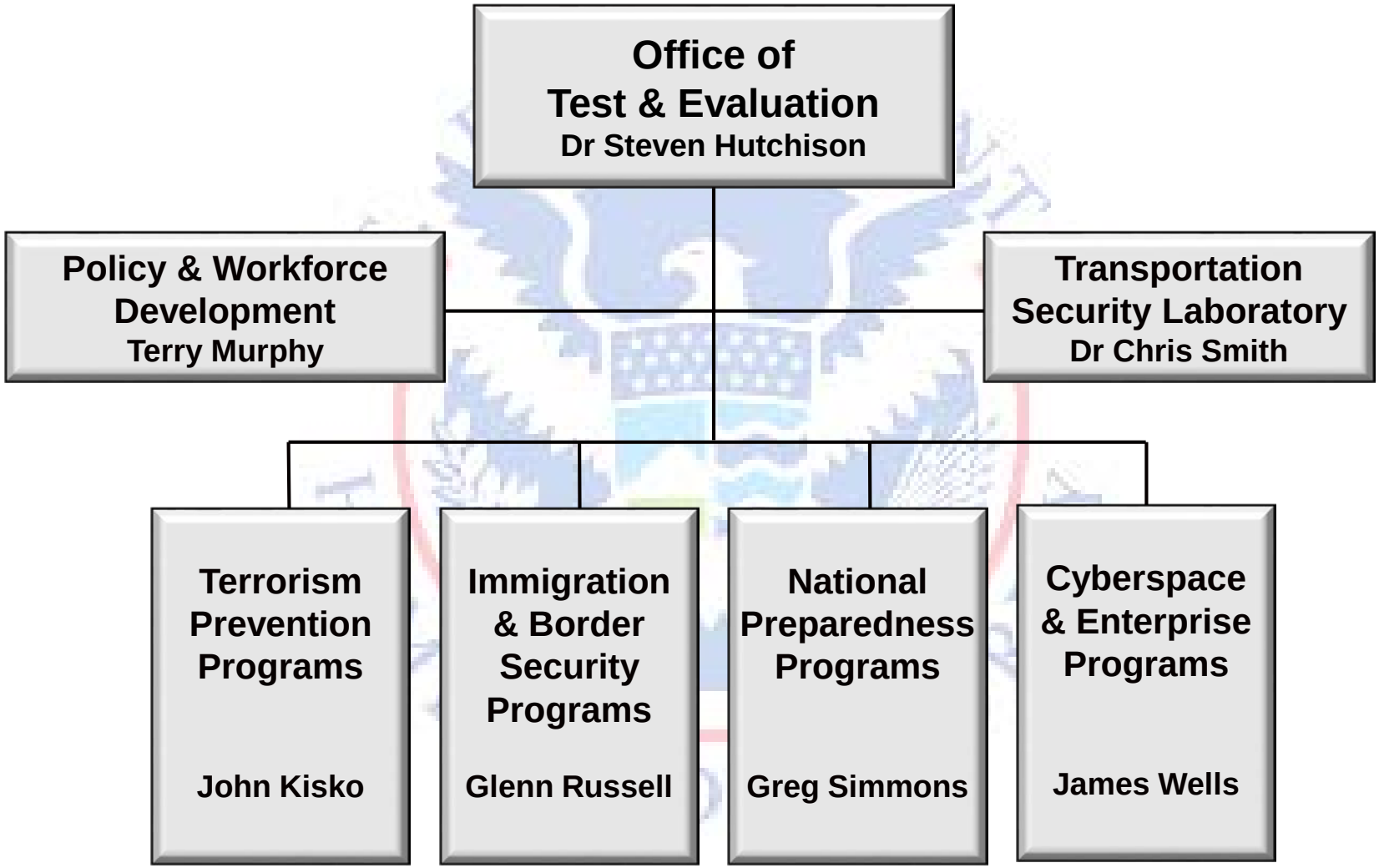
1

Summary

If you want to know your system works, *you have to test it*.
If you want to know *with confidence*, you have to plan, resource, and conduct T&E accordingly.

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

Questions?


Office of
Test & Evaluation
Dr Steven Hutchison
Policy & Workforce Development
Terry Murphy
Transportation Security Laboratory
Dr Chris Smith
Terrorism Prevention Programs
John Kisko
Immigration & Border Security Programs
Glenn Russell
National Preparedness Programs
Greg Simmons
Cyberspace & Enterprise Programs
James Wells