# DoD Joint Cyber T&E Policy and Guidance

## What's New?

Sarah Standard
Cyber/Interoperability Technical Director
OUSD(R&E)
Developmental Test, Evaluation, & Assessments

Washington, DC
6 June 2023

Nilo Thomas
Strategic Initiatives, Policy, and
Emerging Technologies
OSD/Office of the Director, Operational
Test and Evaluation

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-1907, 3 May, 2023

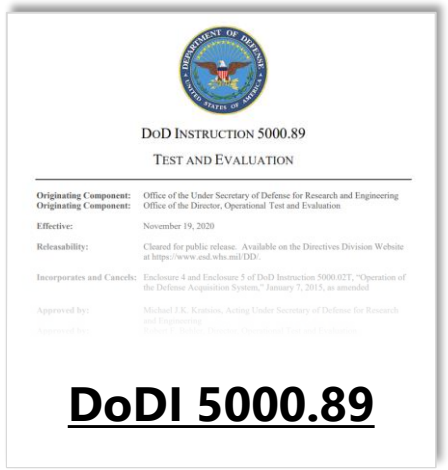
# Agenda

- DoD T&E Policy and Guidance Updates
- Cyber T&E Policy and Guidance

*The opportunity to secure ourselves against defeat lies in our own hands,*
*But the opportunity of defeating the enemy is provided by the enemy himself.*

*-Sun Tzu, The Art of War*

# DoD T&E Policy and Guidance Updates


DoD Instruction 5000.89

Test and Evaluation

Originating Component: Office of the Under Secretary of Defense for Research and Engineering
Originating Component: Office of the Director, Operational Test and Evaluation
Effective: November 19, 2020
Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels: Enclosure 4 and Enclosure 5 of DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015, as amended

**DoDI 5000.89**

Under Revision

## DoD Manuals

Several Special Areas of Focus for T&E

### Future 5000.XX DoD Manuals

- DoDM 5000.XA TEMP / TES
- DoDM 5000.XB M&S VV&A in T&E
- DoDM 5000.XC Cyber T&E
- DoDM 5000.XD T&E in Complex EMS Environment
- DoDM 5000.XF Software T&E

…

High-level procedures on **WHAT** is required

Supporting Guides

Replaced DAG, Chapter 8

## Enterprise T&E Guidebook

### Enterprise T&E Guidebook

- T&E Overview
- T&E for Major Capability Acquisition
- T&E for Middle Tier Acquisition
- T&E for Urgent Capabilities Acquisition
- T&E for Software Acquisition
- T&E for Defense Business Systems

https://www.test-evaluation.osd.mil/T-E-Enterprise-Guidebook/

## Companion Guides

### Enterprise T&E Guidebook Companion Guides

- Cyber
- DevSecOps
- Autonomous Systems
- AI Systems
- IDSK

Includes detailed material for practitioners on **HOW** to implement aspects of the T&E Guidance

**POLICY**

**GUIDANCE**

# Forthcoming DoD Cyber T&E DoD Manual

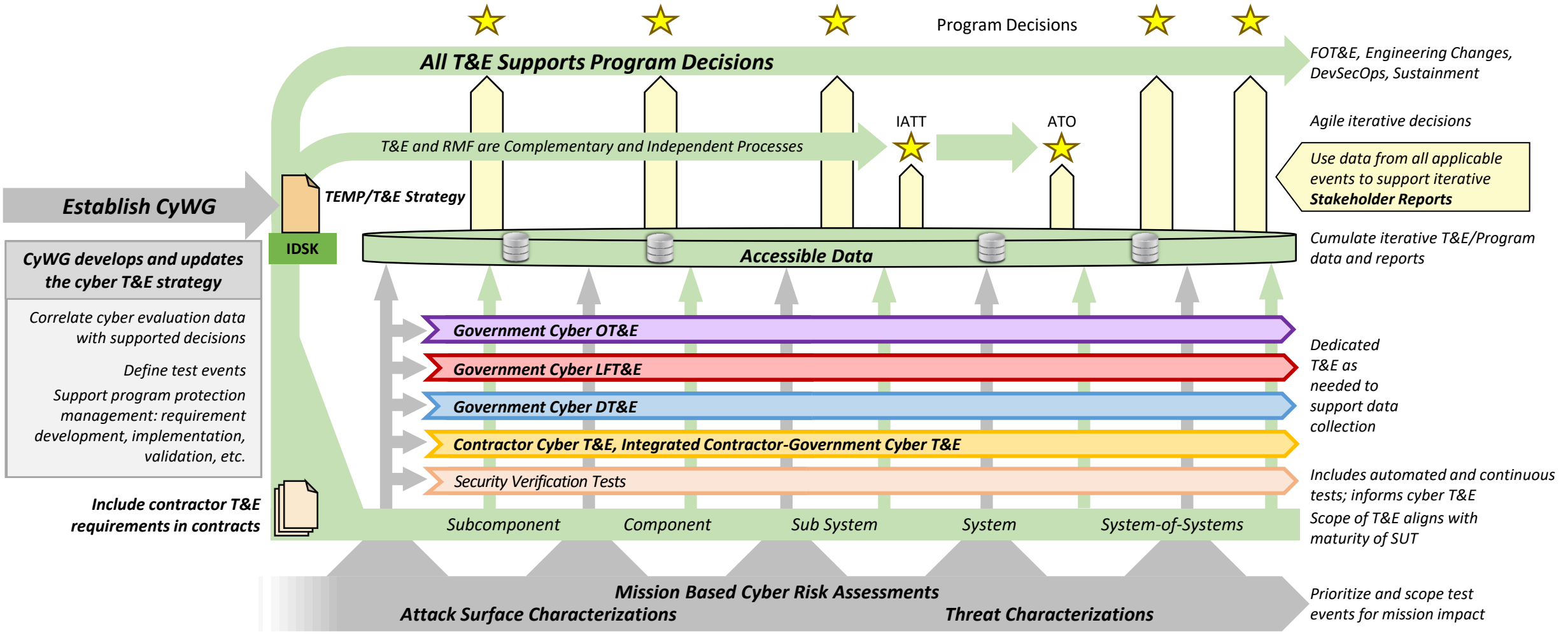
- Approach: Co-developed between DOT&E and DTE&A, supplements DoDI 5000.89, replaces existing single-signature “cybersecurity procedures” DOT&E memoranda
- Themes:
  - Examine and apply intelligence resources to conduct system threat analyses
  - Identify and understand cyber requirements: Measurable, testable, meaningful, and achievable
  - Cyber T&E requirements inform system developer contract requirements up front
  - Expands data collection and seeks continuous analysis of the evolving attack surface
  - Conduct Mission Based Cyber Risk Assessments (more than one)
  - Conduct cyber T&E on prioritized subcomponents, components, subsystems, systems, and system-of-systems
  - Use test results to inform remediation, mitigation, maintenance and defender processes, and next cyber T&E
- Supports Adaptive Acquisition Framework

# Forthcoming DoD Cyber T&E Companion Guide

- Approach: "How" for Cyber T&E; DOT&E and DTE&A co-developed; updates and renames existing DoD Cybersecurity T&E Guidebook
  - "DoD Cybersecurity T&E Guidebook v2.1" → "Cyber T&E Companion Guide v3"
  - Focuses on cyber T&E "how" for Adaptive Acquisition Framework (AAF) Pathways
  - Facilitates tailoring, and agile approaches for AAF pathways
    - Programs design the cadence for the capability needed and the desired program timeline
    - Phases still accepted as DoD programs transition to the new adaptive model
- Increased emphasis:
  - Iterative, continuous, agile testing using automated and integrated testing approaches
  - Testing recover, resilience, and survivability capabilities
  - Inclusion of enabling systems and support systems in mission/capability attack surface evaluations – consider full attack surface and full spectrum threats (EW, supply chain)
  - Contractor role and integration with the Government
  - Operational mission scenario considerations throughout

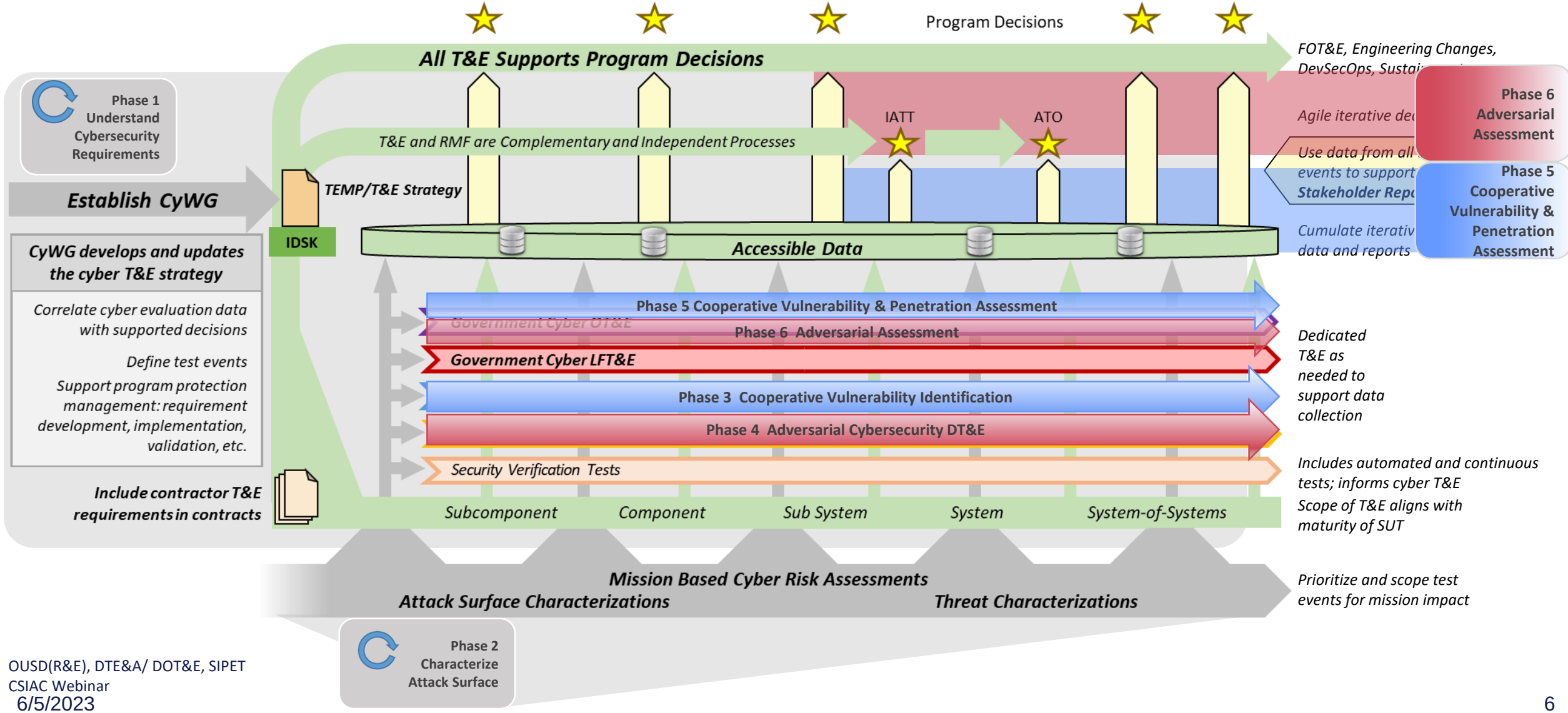
**Start Early (Shift Left) and Iterate**

# Cyber T&E Concepts




ATO = Authority to Operate, CyWG = Cyber Working Group, DT&E = Developmental Test and Evaluation, FOT&E = Follow on Test and Evaluation, IATT = Interim Authority to Test, IDSK = Integrated Decision Support Key, LFT&E = Live Fire Test and Evaluation, RMF = Risk Management Framework, OT&E = Operational Test and Evaluation, SUT = System Under Test, T&E = Test and Evaluation, TEMP = Test and Evaluation Master Plan

# (Future) Cyber T&E Alignment with (Current) Six Phases

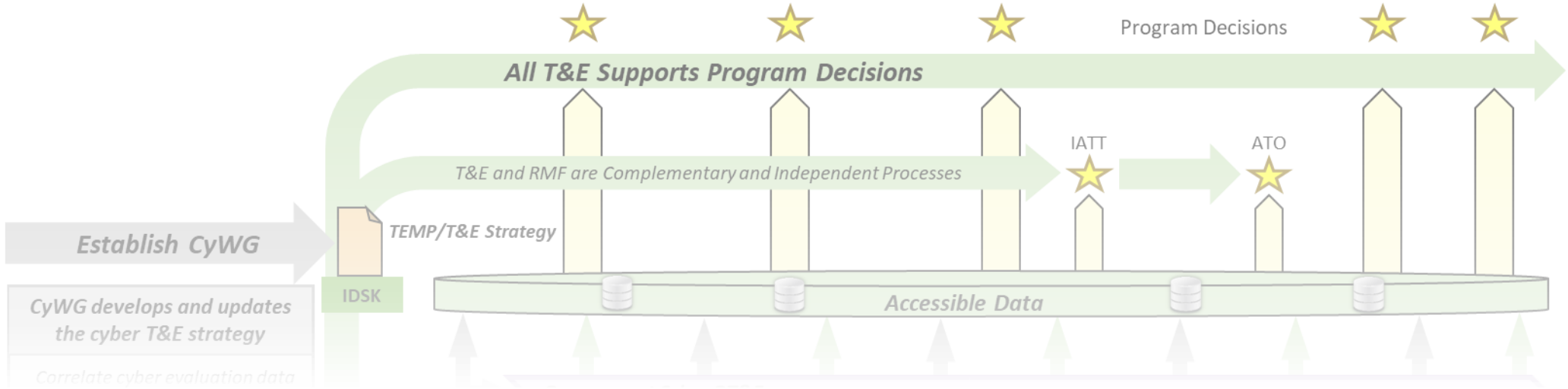


# Program Cyber Management, Cyber T&E Strategy, and the Integrated Decision Support Key (IDSK)

*Tactics without strategy is the noise before defeat.*

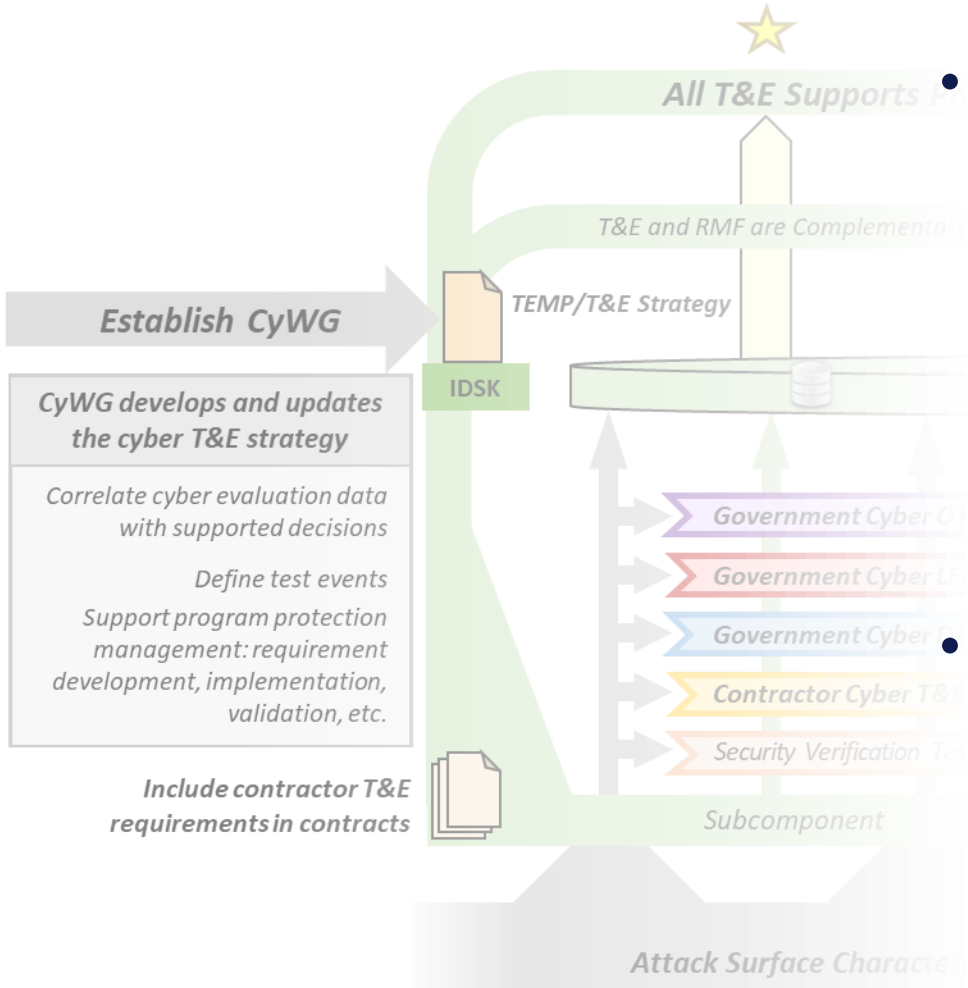
*-Sun Tzu, The Art of War*

# Cyber Working Group and Program Decisions




- Cyber Working Group (CyWG) leads program cyber T&E strategy development
  - Cyber T&E strategy is integrated into program T&E strategy
  - Plan cyber testing: contractor, integrated contractor and government, integrated cyber and non-cyber, log demos with cyber, government acceptance, government DT and OT
- Accessible databases enables data reuse and holistic analysis

# Required Data to Support Decision Making



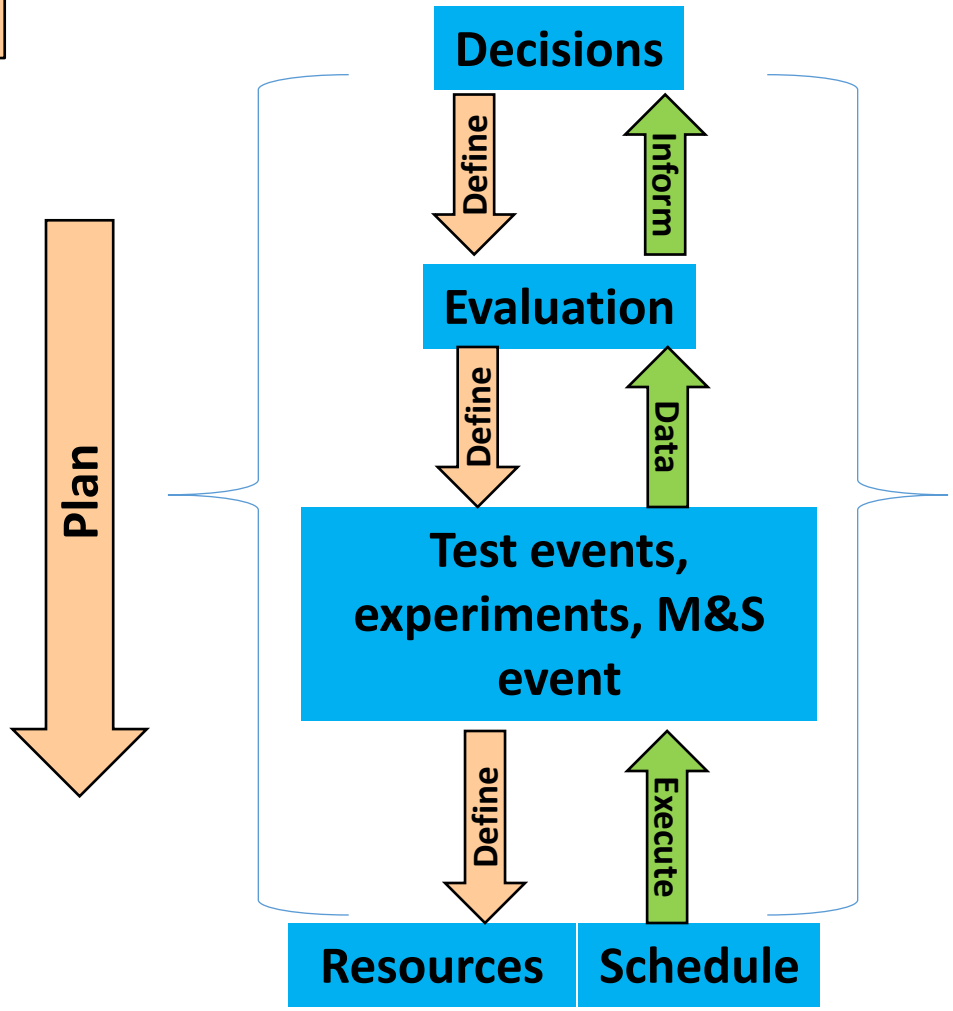

- Ensure cyber T&E is integrated into the Program's IDSK to schedule T&E around informing pathway decisions and milestones
  - Identify Critical Operational Issues impacted by cybersecurity and the data required to resolve those issues
  - Map issues to be addressed and data to be collected to inform certain decisions, capability releases or similar – collectively these should support final OT assessment
- Required for each data source and data collection event
  - Labs, facilities, test assets, operational platforms, test environments
  - System operators/defenders, vulnerability scanning teams, penetration teams

**IDSK helps determine data requirements for test events**

# Decision Supporting – Evaluation-Based – Test Design Thought Process

**T&E Strategy Captures:**

***Plan: Define decisions, capabilities & tests:*** Decisions & ***operational & technical info*** needs; ***operational & technical capabilities*** to evaluate; data generating events (experiments, tests, M&S)




***Execute: Test, Evaluate & Inform:*** Execute the test, M&S events to generate the data for capability evaluation, to inform decisions

**Shared Data, Independent Evaluations**

# Notional Cyber Attributes within the IDSK

DRAFT

Major Decision Points

Cyber Objectives

| Mission / Tasks & Operational Capabilities | Ops Capability Reqmt Doc Reference | Description | Technical Capabilities | Tech Capability Reqmt Doc Reference | Description | AAF Pathway and Program Defined Decision #1 | AAF Pathway and Program Defined Decision #2 | AAF Pathway and Program Defined Decision #N |
|---|---|---|---|---|---|---|---|---|
| | | | | | | ← Decision Support Questions → | | |
| **Operational Mission Effects** | Operator/Defender Response/Capabilities | | **System Data Security / Risk Management** | System prevents loss of data ***confidentiality*** | | | | |
| | | | | System prevents loss of data ***integrity*** | | | | |
| | | | | System prevents loss of data ***availability*** | | | | |
| **Survivability, Resilience, Mission Assurance** | Mission Critical Capabilities | | **System Resilience** | System ***prevents*** cyber intrusions | | | | |
| | | | | System ***mitigates*** the effects of cyber-attacks | | | | |
| | | | | System is able to ***recover and adapt*** from cyber-attacks | | | | |

Subcomponent, Component/ Sub-system, System, System of Systems CT, DT, LF, OT Events

Align and integrate test events

**IDSK illuminates integrated test opportunities**

# Types of Integrated Cyber Testing

| Integrated Test Type | Timeline | Description |
|---|---|---|
| **Integrated Contractor - Government Testing** | During engineering, development | Used to complete a comprehensive evaluation of system sub-components through fully integrated systems as early as possible in the acquisition pathway |
| **Integrated Functional-Cyber Testing** | During engineering, development, early government DT, Live Fire T&E | Early functional performance, lab-based, bench, or model-based engineering tests performed during system development to demonstrate technology maturity toward meeting the following types of threshold requirements:<br>• Key performance parameters (KPPs)<br>• Key system attributes (KSAs)<br>• Measures of effectiveness (MOE)<br>• Measures of performance (MOPs)<br>• Other performance and mission related measures unique to the program |
| **Integrated Government Cyber DT-OT** | After delivery to the government | Used to evaluate mission effects and the system/operator response while operating in a cyber-contested environment. |

**Independent assessment/evaluation of data**

# Cyber Working Group Activities for Scoping Cyber T&E

## Cyber Requirements, Threat Characterization, Attack Surface Characterization, Mission Based Cyber Risk Assessments, Using Cyber T&E

*To know your enemy, you must become your enemy.*

*-Sun Tzu, The Art of War*

# Examine and advise on Cybersecurity and Cyber Survivability Requirements

- Support the System Security Engineers to define performance specifications and a design accounting for mission risk and implementing prevent, mitigate (includes the ability to detect), recover/adapt capabilities
  - Follow Joint Staff Cyber Survivability Endorsement
- Develop metrics
- Take measurements
- Evaluate the results during testing to assess progress and make recommendations

**Repeat for Each Acquisition and IDSK Decision**

# Cyber Survivability Attributes (CSAs) are Threshold Performance Requirements

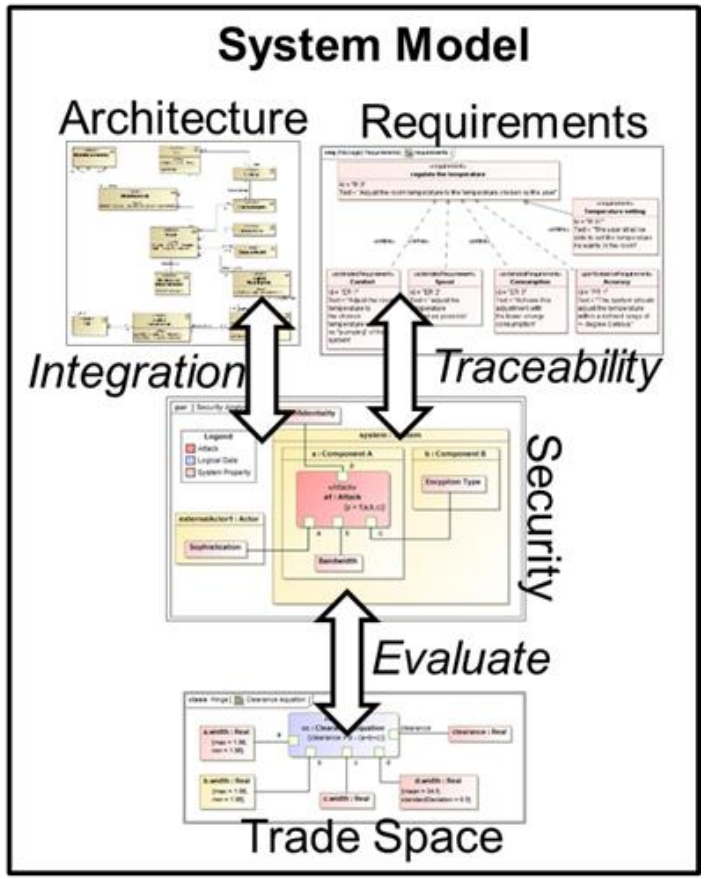
| SS KPP Pillars (Mandatory) | Cyber Survivability Attributes (CSAs) (All are to be considered; select those that are applicable) |
|---|---|
| Prevent | CSA 01 - Control Access |
| | CSA 02 - Reduce Cyber Detectability |
| | CSA 03 - Secure Transmissions and Communications |
| | CSA 04 - Protect Information and Exploitation |
| | CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels |
| | CSA 06 - Minimize and Harden Cyber Attack Surfaces |
| Mitigate | CSA 07 - Baseline & Monitor Systems, and Detect Anomalies |
| | CSA 08 - Manage System Performance if Degraded by Cyber Events |
| Recover | CSA 09 - Recover System Capabilities |
| Adapt for Prevent, Mitigate & Recover | CSA 10 - Actively Manage System's Configurations to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP) … applicable to legacy systems that did not consider CSAs during development … |

Resilience Starts Here

**Fundamental to CSE construct is selecting CSAs to achieve and maintain each Pillar -- # CSAs Expected for CSRC-5: 9-10, CSRC-4: 6-9, CSRC-3: 5-7, CSRC-2: 2-5, CSRC-1: 1-3**

CSE = Cyber Survivability Endorsement, CSRC = Cyber Survivability Risk Category

# Resilience Requires Engineering



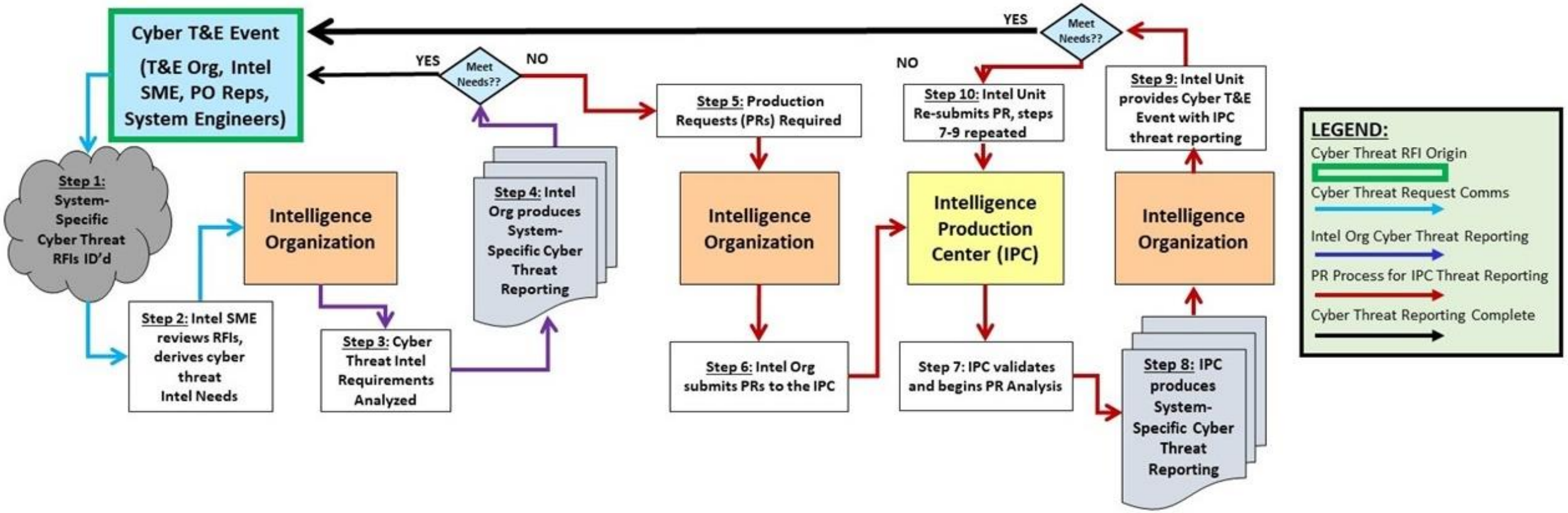

- CSAs are high level requirements
  - Engineers need lower level measurable requirements to demonstrate progress toward threshold during development
- Engineers define performance specifications (P-spec) that articulate CSAs as requirements for performance in cyberspace
  - No cookie cutter controls here!
  - Flow-down, map, and de-conflict security requirements (including technology and program protection) to the functional and technical / performance requirements
- Contractor decomposes P-spec into lower levels; government supports scope with mission and threat context
    - Define Technical Performance Measures (TPMs) that trace to P-Spec
    - DoD uses Mission Based Cyber Risk Assessments (MBCRAs)

# Conduct Iterative Activities to Inform and Use Testing Results

- Threat Assessment and Attack Surface Characterization
  - Cyber T&E input to the TEMP/T&E strategy, will be based on the system-relevant intelligence product(s) as the threat, system, operational environment, or mission evolves
  - Cyber T&E input will consider the systems' characterized attack surface based on program and system artifacts, contractor and operational processes, the supply chain, system components, technologies, and interfaces
- Mission Based Cyber Risk Assessments (MBCRAs)
  - The process of identifying, estimating, and prioritizing risks to DOD operational missions resulting from cyber effects on the system(s) being employed in support of the missions
  - Uses current attack surface and threat characterizations
  - Uses results of any previous testing
  - Repeat or update in response to new or changing requirements, design, mission, functions, interfaces, or threats


**Impossible to conduct exhaustive testing – scope to what matters**

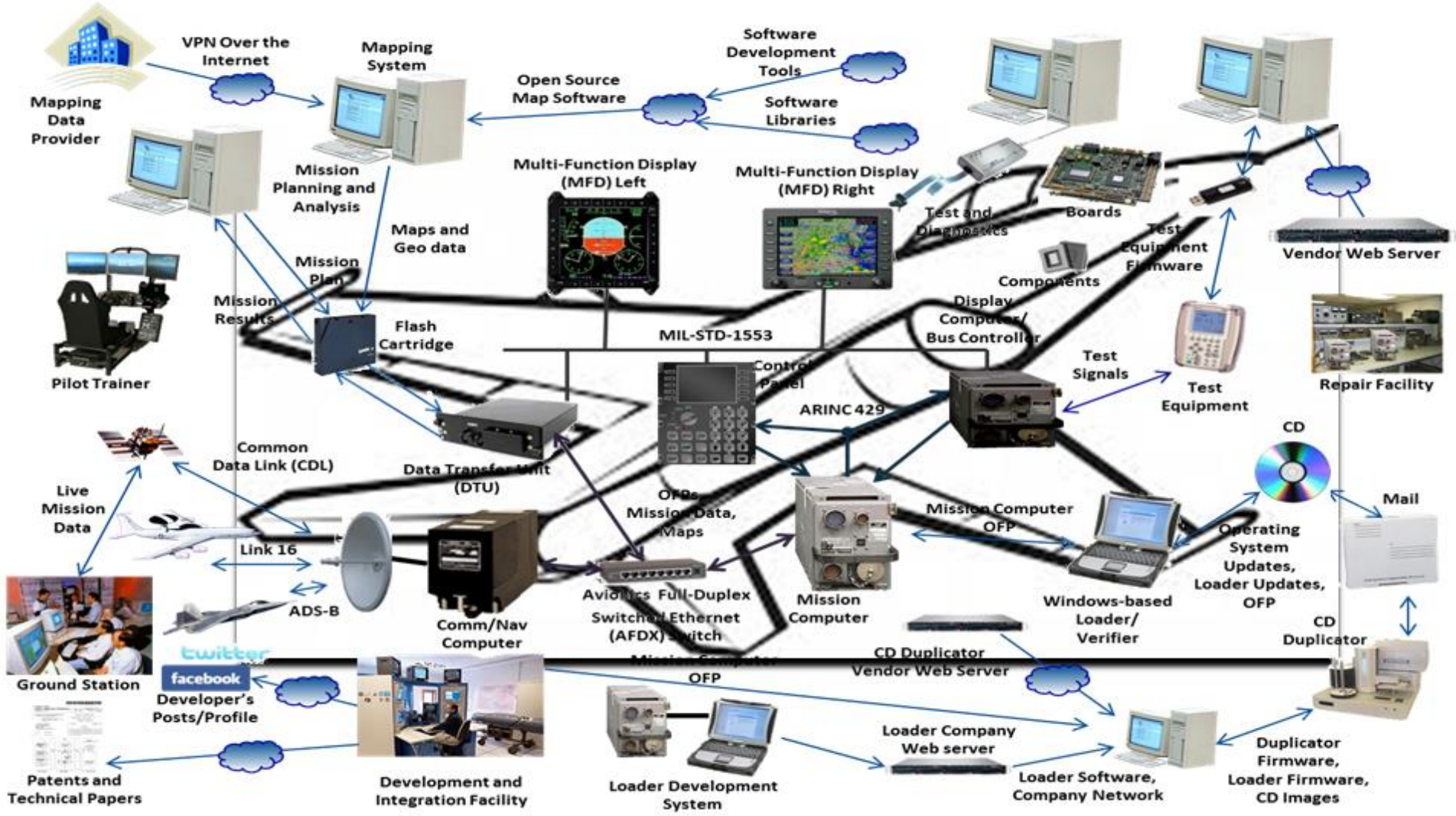
# Threat Characterization – Working with the Intelligence Community




**Having an intelligence liaison supporting the test organization is a critical enabler to this process**

**Repeat for Each Acquisition and IDSK Decision**

# The cyber-attack surface consists of the system's reachable and exploitable cyber vulnerabilities, including reliance on supporting / underlying infrastructure

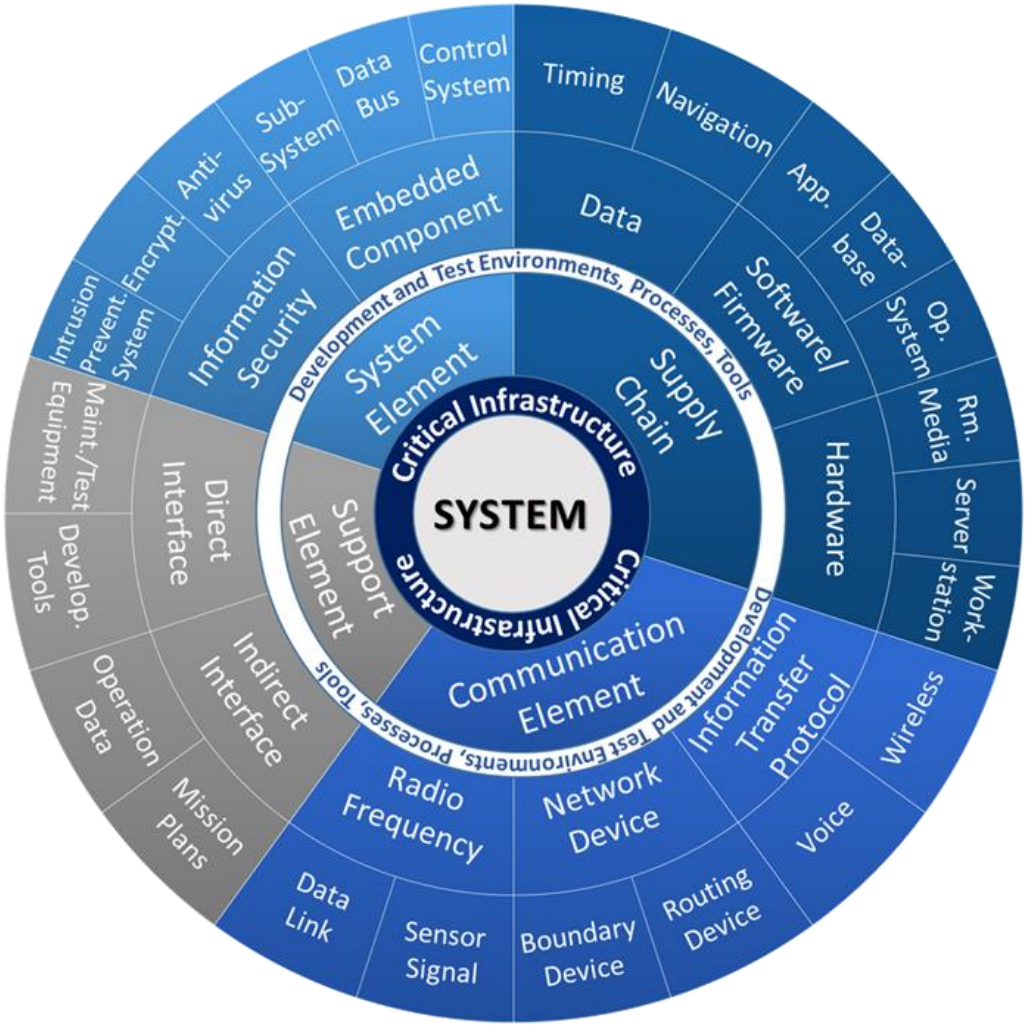


# Examples of Evolving Attack Surface Elements

- Additive and Computer-Aided Manufacturing
- Artificial Intelligence, Machine Learning, and Big Data Applications
- Commercial Cloud Environments and Cloud Services
- Defense Industrial Base (DIB)
- DoD Infrastructure and Enterprise Services
- Electromagnetic Spectrum Operations (EMSO)
- Inter- and Intra-System Architecture Network Interfaces
- Interfaces with Interagency, Industry, Academia, Foreign Networks, and/or Human Processes
- Real-Time, Safety-Critical Systems (e.g., Industrial Control Systems, Supervisory Control and Data Acquisition)
- Software Factories
- Supply Chain
- System Architecture and Design Choices

# Attack Surface Characterization

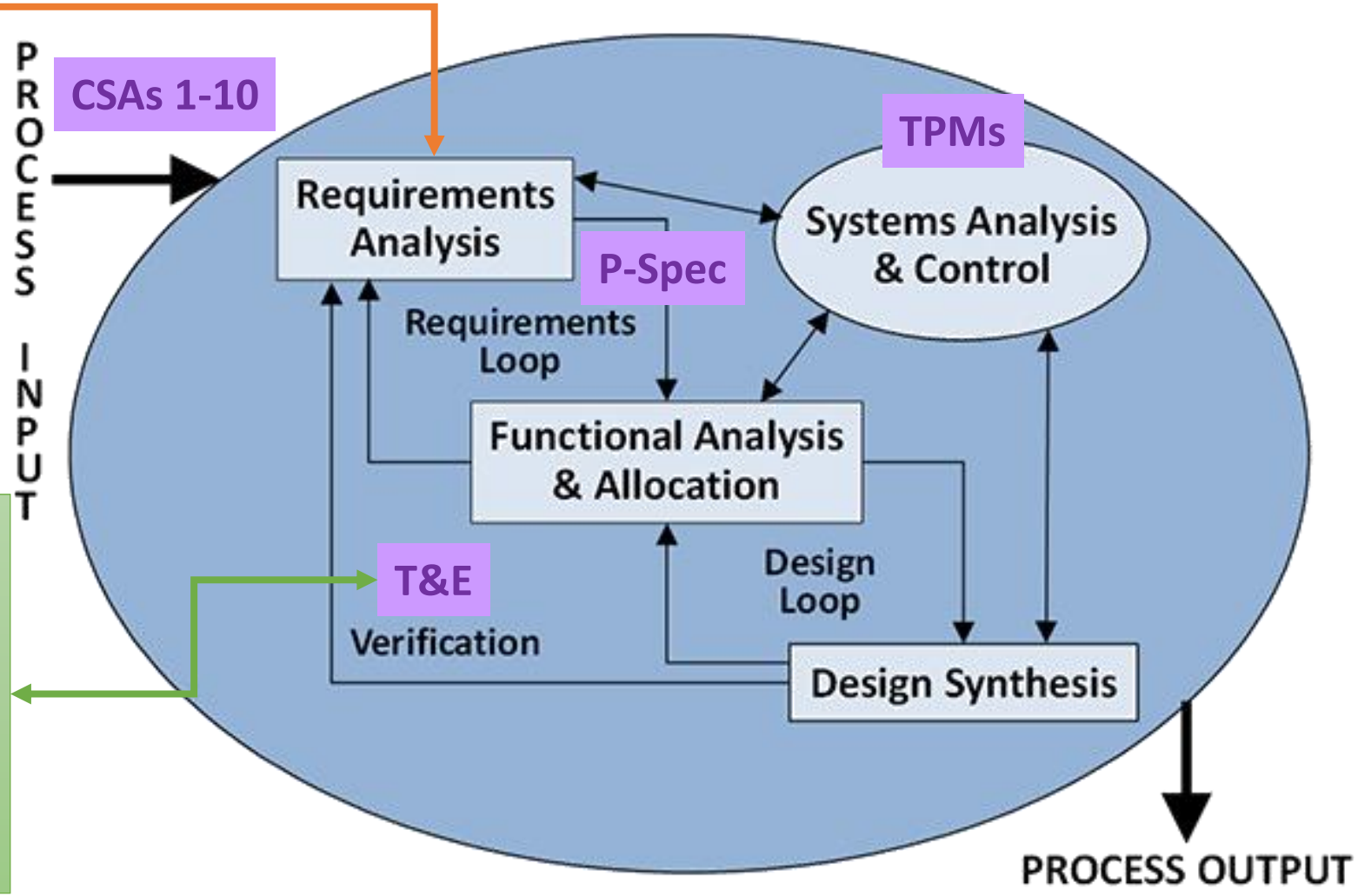
- In conjunction with, or separate from, MBCRA, with program protection team
- Entry points, exit points, interfaces, data exchange, data
  - Consider evolving attack surface elements
  - Supply chain, development, test, and manufacturing processes, tools, people, environments
- Mission decomposition, system capabilities
  - Trace mission and capability dependencies
  - Paths to critical functionality, data
- Characterize threat
- Document attack surface list, critical components and data, analysis, known vulnerabilities, recommended activities




**Repeat for Each Acquisition and IDSK Decision**

# MBCRAs in Systems Engineering Processes Model

**Requirements Analysis Process**
- Analyze capability and adversity driven by mission, operations, sustainment and environments
- Identify functional requirements
- Define performance and design constraint requirements




**MBCRA Informs Engineering and Test**
- Identify the mission essential functions and the MBCRA in-scope system critical components
- Map mission dependence at the component, system, and mission thread level
- Determine how the expected threat adversary could access the system and exploit mission critical functions
- Characterize and prioritize attacks for testing based on mission criticality
- Generate attack scenarios for test
- Recommend remediation or mitigations

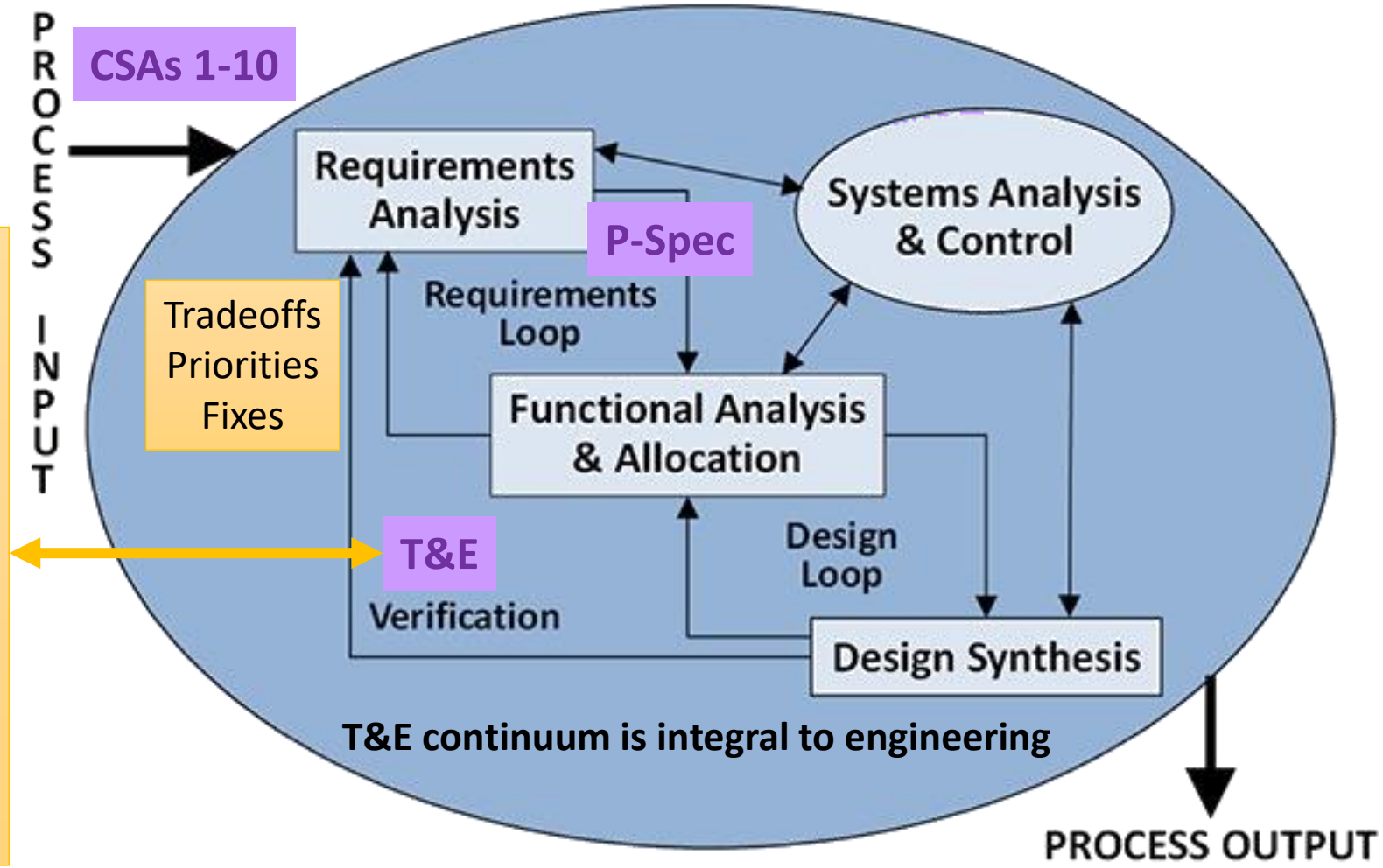
# Mission Based Cyber Risk Assessments (MBCRAs)

- Early MBCRAs inform concept selection and design, later MBCRAs track system progress and inform specific test event planning
- MBCRA minimum inputs:
  - Latest available system details (e.g., mission, functions, mission critical functions, architectures, software, hardware, data flows, interfaces, protections, maintenance processes)
  - Current threat characterization
  - Listing and analysis of existing/known vulnerabilities (including bill of material analysis)
- MBCRA minimum outcomes:
  - Mission impact estimates using input from the operational users, defenders, maintainers, developers, engineers
  - Attack surface characterizations, to inform test objectives for future testing
  - Reports will detail the attack scenarios and threat vignettes with recommendations for remedies, mitigations, and testing

**Companion Guide will Provide Additional Detail on MBCRA Activities**

# Plan to Use Test Results

- Cyber T&E informs engineering, remediation, mitigation, maintenance, sustainment, defender processes
  - Models
  - Simulations
  - Prototypes
  - Similar systems and technologies
  - Prior increment
  - Subcomponents
  - Components
  - Sub systems
  - System, full system
  - Integrated, interoperable systems



# Cyber Testing
# (Test Plans, Execute Tests, Test Reports)

*Confront them with annihilation, and they will then survive; plunge them into a deadly situation, and they will then live. When people fall into danger, they are then able to strive for victory.*

*-Sun Tzu, The Art of War*

# Cyber Test Plan Data

| Topic | Description |
|---|---|
| **System**<br>What is being tested? | Describe the architecture of the system(s) or system-of-systems or unit and provide detailed network diagrams |
| **Test Environment**<br>Where is the test being done? | Describe conditions, assumptions, and limitations affecting overall test conduct<br>Describe the cyber environment for the system |
| **Time and Resources**<br>When and who, using what? | Provide the schedule of test events and resources |
| **Vulnerability Tracking and Retesting**<br>How | Describe how the test team will use results from prior security verification tests and conduct the test activities to gather the required data<br>Describe the process to document, track, and determine severity of vulnerabilities during the test |
| **Cyber Test Activities**<br>How | Describe how the test team will conduct the test activities and gather required data |
| **Defensive Capabilities**<br>How | Describe how during or after an attack the test will collect the observations and actions of the operators; Metrics; Defensive cyber tools |

# Plan and Conduct Contractor, Developmental, Live Fire, and Operational Test

- Security verification conducted by the contractor and the program office, in coordination with the LDTO
  - Includes automated and continuous tests, compliance scans and security control assessments – finds known software vulnerabilities and configuration mistakes
  - Data informs cyber testing
- Cyber T&E includes data and measures to inform evaluations of defensive, resilience, and survivability capabilities
- Tests to determine access to vulnerabilities, system exposures, and points of penetration – informs vulnerability remediation priorities early and continuous monitoring
- Tests which exploit any vulnerabilities using realistic threat profiles and measure the mission impact upon exploitation - informs remediation and mitigation priorities, maintainer, defender processes


- Tests on critical and integrated subcomponents through full system with proxy users/defenders, then on operational relevant/representative system in OT with trained operators and defenders

**Update for Each Acquisition and IDSK Decision**


# Cyber Developmental Test and Evaluation

*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*

*-Sun Tzu, The Art of War*

# Cyber DT&E – Much more than Vulnerability Scans!

- Identify and mitigate risks of technical vulnerabilities and susceptibilities affecting functional mission execution, recoverability, and overall cyber survivability
- Identify engineering and technical issues in the system within the mission context to manage and reduce cyber threat unique risks during system development
- Measure specified requirements for system capabilities to prevent, mitigate, and recover/adapt
- Verify products are compliant with contractual and technical requirements including Security Technical Implementation Guides and exposure to known vulnerabilities within the National Vulnerability Database

- Contractor cyber T&E
  - Contracts will require contractors to measure, and report on contractual and technical requirements early enough to identify vulnerabilities, implement improvements, and mitigate or remediate risks
- Government acceptance cyber T&E
  - Prior to accepting the system under test (e.g., minimum viable capability release, subsequent software release, increment, or other intermediate deliverable)
  - Include technical personnel from both the contractor and the government
- Government cyber DT&E
  - Components, subsystems, prototypes, and developmental systems continuing to undergo design changes

**Multiple targeted tests on critical subcomponents, components, and sub systems**

# Cyber Operational Test and Evaluation

*Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.*

*-Sun Tzu, The Art of War*

# Cyber OT&E

- OTAs must evaluate operational effectiveness and suitability of DoD systems with trained users and defenders, in operationally representative contested cyberspace
- Cyber OT&E supports all planned OT&E events, including early operational assessments (EOAs), operational assessments (OAs), initial operational test and evaluation (IOT&E), follow-on operational test and evaluation (FOT&E), and operational demonstrations (Ops Demos)
- Include system-of-systems together with operationally representative information flows, production-/fielding-representative configurations, operational users including cyber defenders at all appropriate echelons, and an operationally representative environment

# Cyber OT&E Demonstrates Mission Impacts from Cyber Effects

- Identify exposures in the end-to-end execution of mission scenarios and assess the capabilities of the users, maintainers, and cyber defenders to identify and mitigate cyber threats
- Use known and newly discovered exposures to attempt to degrade critical component, subsystem, system, and mission functions while the users are conducting missions;
  - Assess the capabilities of the users, maintainers, and cyber defenders to identify and mitigate cyber threats

# Cyber OT&E Includes Users and Defenders

- Observe and evaluate the results of actions performed by users, maintainers, and cyber defenders in a maintainability demonstration as part of a cyber-incident response scenario, including recoverability and continuity of operations, through full restoration of the affected system
- Include the unit trained and equipped with the system in an operationally representative environment and evaluate:
  - Threat-representative cyber effects on operational effectiveness, suitability, survivability, and lethality of a unit trained and equipped with the system during and after cyber actions.
  - Effectiveness of defensive capabilities (including those of an assigned CSSP or local defender) on the susceptibility to cyberspace attack and subsequent effect on vulnerability and recoverability and effects on mission effectiveness, suitability, survivability, and lethality.

# Cyber Live Fire Test and Evaluation

*Thus, what is of supreme importance in war is to attack the enemy's strategy.*

*-Sun Tzu, The Art of War*

# Cyber Live Fire T&E

- Pursuant to Section 4172 of Title 10, U.S.C., Section 223 of Public Law 117-81 and in accordance with DoDI 5000.89, **realistic survivability** testing of systems will include cyber threat effects
- May be based on the use of operationally representative threat surrogates, testing against components, subsystems, and subassemblies together with performing design analyses, modeling and simulation, and analysis of combat data
- Starts in initial stages of system development to manage and reduce cyber threat unique vulnerabilities at the subcomponent, component, subsystem, and system levels
- Confirm cyber CT&E, DT&E, and OT&E provide the data to enable realistic survivability evaluation including the evaluation of the physical effects of the identified cyber vulnerabilities on residual mission capabilities, recoverability, and user casualties, if applicable

# Cyber Test Reporting

| Topic | Information |
|---|---|
| **Test Conduct** | Test execution context |
| **System Configuration** | Contextual data about actual system configuration, as tested |
| **Cyberspace Attack Scenarios** | Contextual data describing the threat |
| **Supply Chain** | Supply side context |
| **Vulnerability and Exposure Identification – Scans** | Knowable openings |
| **Vulnerability and Exposure Exploitation** | Where openings lead |
| **Integrated Cyber EMSO Testing** | Describe how EMS did or could enable or hinder aggressive cyber activities |
| **Operational Mission Effects including Force Protection** | Report observed, anticipated, or estimated cyber vulnerabilities |
| **Prevent** | Identify, Protect |
| **Mitigate** | Detect, System Monitoring, System Response Actions |
| **Recover/Adapt** | System or Operator Recovery/ Adaptation and Restoration Actions |

# Summary

- Fundamental *iterative* (and recursive) activities in current guidance are still necessary
  - Identify and understand cyber requirements
    - Measurable, testable, meaningful, and achievable
  - Examine and apply intelligence source system threat analyses
  - Characterize the attack surface to identify threat vectors
    - Mission decomposition
    - System functional alignment to mission
  - Use test results to inform remediation, mitigation, maintenance and defender processes, and next cyber T&E
    - Subcomponents, components, subsystems, systems, system of systems
  - Conduct Mission Based Cyber Risk Assessments
  - Conduct cyber T&E, informed by security verification test data
- Data driven testing

**Don't just count vulnerabilities!**
**Measure performance and capabilities when in contested cyberspace**

***Attack is the secret of defense; defense is the planning of an attack.***

*The Art of War -Sun Tzu*

# Questions?

sarah.m.standard.civ@mail.mil

nilo.a.thomas.civ@mail.mil