SLIDES ONLY
NO SCRIPT PROVIDED

DoD Manual (DoDM) 5000.96 Operational and Live Fire Test and Evaluation of Software

Mr. Nilo Thomas
Director, Operational Test and Evaluation (DOT&E)

Introduction to DoDM 5000.96

What is New or Emphasized in the DoDM 5000.96?

This slide highlights the major shifts within the DoDM, relating to acquisition planning and software development.

DURING ACQUISITION PLANNING

- Participation in Requirements Development

- LFT&E Requirements

- Test and Evaluation Strategy

- Decision Analysis ad Evaluation Frameworks (IDSK, RALOT)

- Test Automation and Test Management Tools

- Digital Engineering and Model-Bases Systems Engineering (MBSE)

- OT Interests into Acquisition Contracts

DURING SOFTWARE DEVELOPMENT

- Gathering Evidence in Opportunities in "The Software Test Factory"

- Assessing Data and Artifacts:

  - In Simple Code and Sub-components

  - In Components and Subsystems

  - In Systems and System-of-Systems

- OT Interests in Test Activities in the Software Test Factory

■ **NEW**

Purpose and Applicability

The DoD Manual (DoDM) 5000.96 provides procedures for T&E of all DoD software intensive systems and software embedded in systems.

High-Level Purpose	Implements policy, assigns responsibilities, and provides procedures for OT&E and LFT&E of DoD software-intensive and software embedded in systems and services, In Accordance With (IAW) DoDD 5141.02 and DoDI 5000.98.

DoD MANUAL 5000.96

OPERATIONAL AND LIVE FIRE TEST AND EVALUATION OF SOFTWARE

Originating Component:
Office of the Director, Operational Test and Evaluation

APPLIES TO:

- All DoD Components
- DoD systems acquired via the Defense Acquisition System
- DoD systems under special access controls
- Non standard acquisition systems
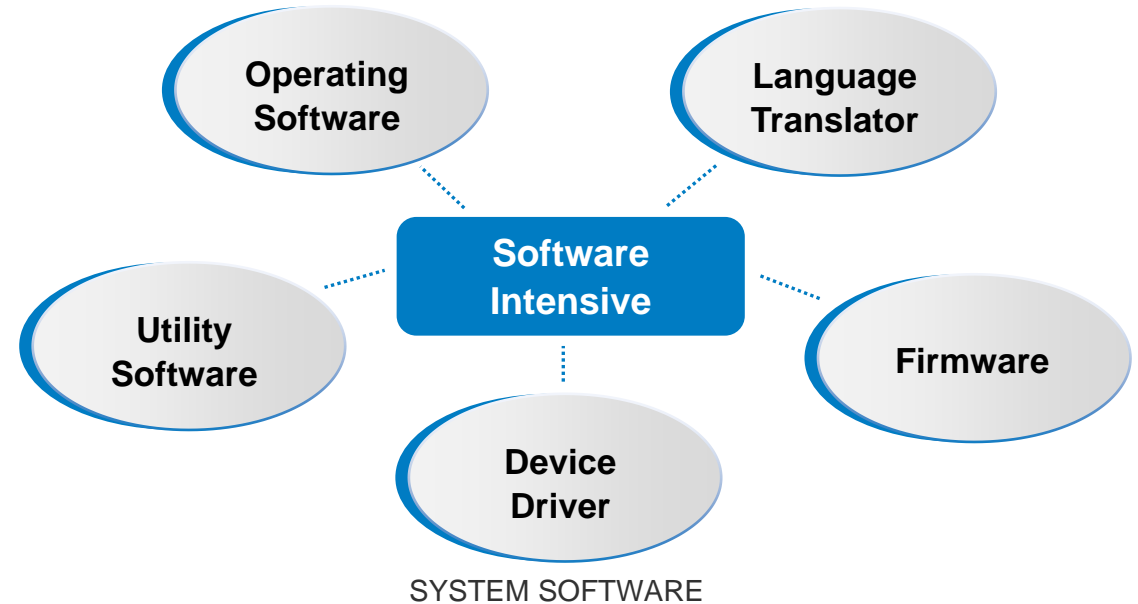
Significance and Key Policy

IAW DoDI 5000.98, this manual will evaluate the operational effectiveness, suitability, survivability and lethality of software-intensive or software embedded in DoD systems.

Software Intensive Systems

Software represents the **largest segment** in one or more areas within a system.

Embedded in Software
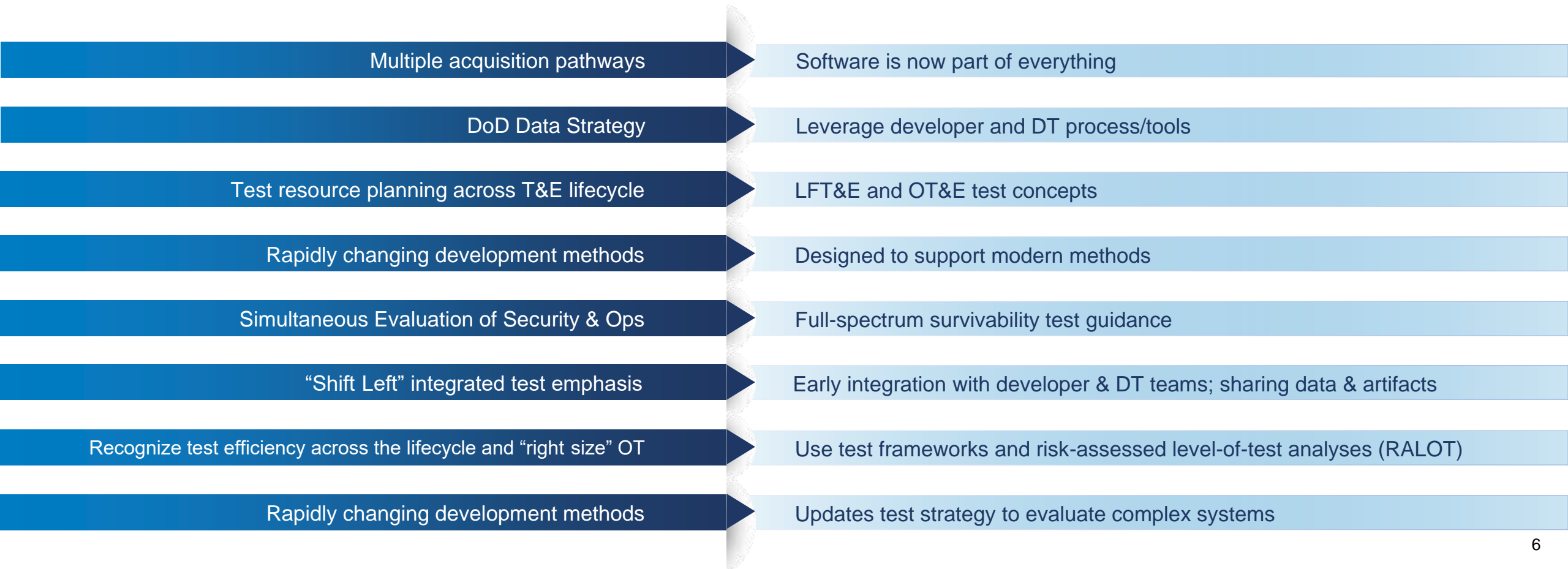
Software with a **dedicated function** within a larger mechanical or electrical system.

Operating Software

Language Translator

Utility Software

Software Intensive

Firmware

Device Driver

SYSTEM SOFTWARE

Embedded Processor

5

Rapidly Evolving Software Development Methods

This policy was created for rapidly evolving software development methods

|	
Multiple acquisition pathways	Software is now part of everything
DoD Data Strategy	Leverage developer and DT process/tools
Test resource planning across T&E lifecycle	LFT&E and OT&E test concepts
Rapidly changing development methods	Designed to support modern methods
Simultaneous Evaluation of Security & Ops	Full-spectrum survivability test guidance
"Shift Left" integrated test emphasis	Early integration with developer & DT teams; sharing data & artifacts
Recognize test efficiency across the lifecycle and "right size" OT	Use test frameworks and risk-assessed level-of-test analyses (RALOT)
Rapidly changing development methods	Updates test strategy to evaluate complex systems

Software OT&E and LFT&E Overview

Software OT&E and LFT&E Across the Acquisition Life Cycle

Software is a critical element in the acquisition of most DoD systems pursuing any of the acquisition pathways within the Defense Acquisition System.

Agile is a methodology emphasizing on **flexibility**, **collaboration**, and **customer satisfaction.**

- Planning activities **prioritize**, **allocate**, and **decompose** requirements for future iterations.
- An Agile team will address any identified **defects and vulnerabilities** during planned iterations.
- Once **quality criteria** and **metrics** have been satisfied, the decision authority will **"release" the software.**
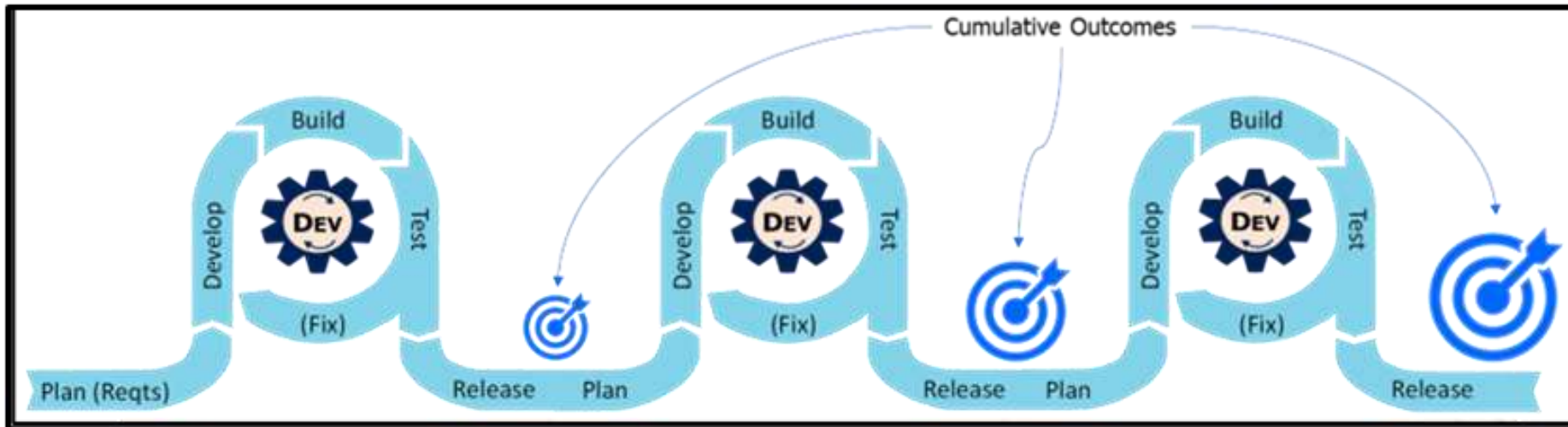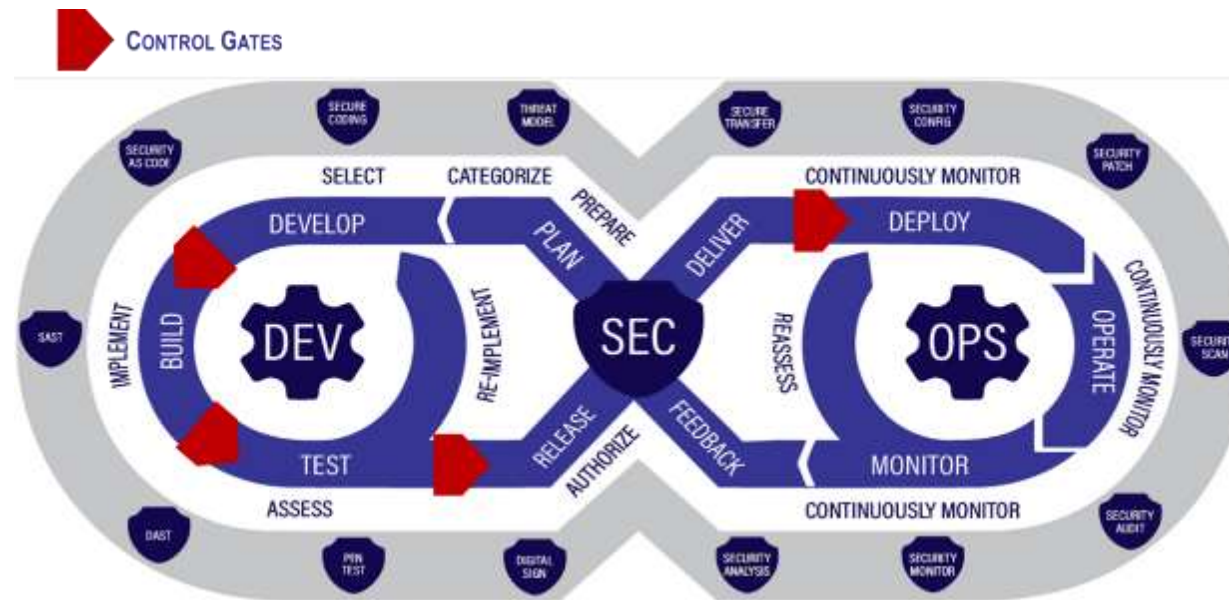

Notional Agile Iteration Cycle

To view tables and figures containing baseline software test data and activities, please refer to the Appendix on Slides 28-31.

Software OT&E and LFT&E Across the Acquisition Life Cycle

Software is a critical element in the acquisition of most DoD systems pursuing any of the acquisition pathways within the Defense Acquisition System.

DevSecOps is a framework that **integrates security** into all phases of the software development lifecycle.

- **10 phases** from build to deployment with constantly **integrated security.**
- **Feedback** mechanisms and decision points are used to **move forward** to the next phase.
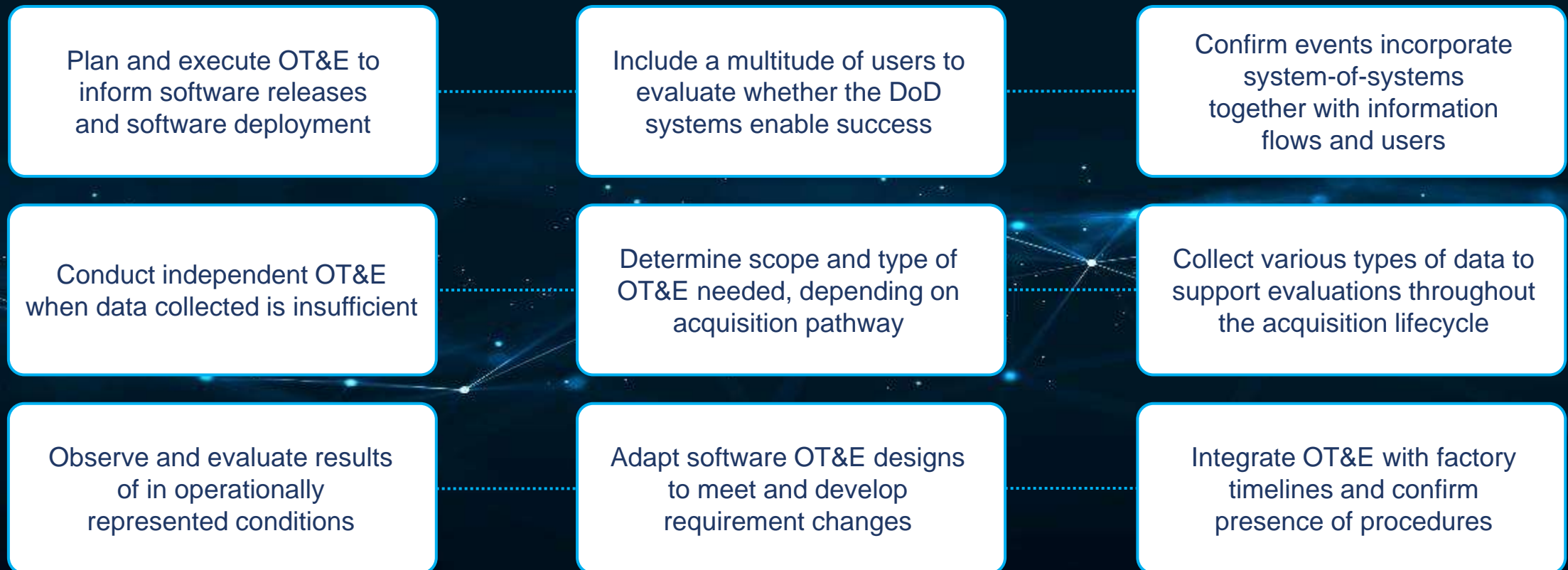- **Generated feedback** will be used to **identify potential defects** ahead of time.

DevSecOps Cycle with Control Gate Overlay

To view tables and figures containing baseline software test data and activities, please refer to the Appendix on Slides 28-31.

Operation Test and Evaluation (OT&E)

Section 3.3 in DoDM 5000.96 focuses on OT&E, with a specific focus on Operational Test Agencies (OTAs).

OTAs will…*

Plan and execute OT&E to inform software releases and software deployment

Include a multitude of users to evaluate whether the DoD systems enable success

Confirm events incorporate system-of-systems together with information flows and users

Conduct independent OT&E when data collected is insufficient

Determine scope and type of OT&E needed, depending on acquisition pathway

Collect various types of data to support evaluations throughout the acquisition lifecycle

Observe and evaluate results of in operationally represented conditions

Adapt software OT&E designs to meet and develop requirement changes

Integrate OT&E with factory timelines and confirm presence of procedures

* Please refer to Table 1, "Baseline Software Test Data and Activities", in the Appendix for required OT&E activities (e.g. Definition of Done, Unit Testing, Functional Testing, etc.).

Live Fire Test and Evaluation (LFT&E)

LFT&E will focus on realistic, full spectrum survivability and lethality testing for software intensive and software embedded in DoD systems IAW Paragraph 3.4 of DoDM 5000.99.

Full spectrum survivability T&E will use vulnerabilities and limitations identified in software survivability tests.	**Full spectrum survivability T&E for software-intensive DoD offensive capabilities will include:**
• Software factories and cloud environments **provide unique attack vectors** • Systems with **unique defensive missions or capabilities** will be assessed to measure **countermeasures against adversarial attacks** • **Risk-based level of assessments** and **MBRAs** that consider software factory **security testing** informs **full spectrum survivability testing**	• **Deny, degrade, disrupt, destroy, exploit,** or **influence** capabilities • Known network or system **defenses and adversarial Tactics, Techniques, and Procedures (TTPs)** designed to deter **lethal actions**

Realistic, full spectrum survivability and lethality test data will be acquired by early and often providing data for the evaluation of operational effectiveness and suitability.

Management (1/2)

Section 3.7 of DoDM 5000.96 lays out the roles and responsibilities of the key actors involved as it relates to OT&E and LFT&E of software.

PROGRAM MANAGER

- **Codify** user engagement for **software development**

- **Integrate** software into **software pipeline** and systems engineering

- **Incorporate** automation **throughout** development

- **Ensure** OTA and LFT&E have **contractor information** and **provide input** to their test plans

- **Budget** for integration with **software factories** and **DevSecOps platforms**

- **Develop** and implement a data **management strategy**

- **Provide** a test **environment** that represents both **pre-production and production**

- **Provide** test data to **evaluate the security** of the software factory

Management (2/2)

Section 3.7 of DoDM 5000.96 lays out the roles and responsibilities of the key actors involved as it relates to OT&E and LFT&E of software.

OTA Organizations

Support the **development** of capstone capability requirements throughout the software development

LFT&E Organizations

Identify test **requirements** to be considered by the software development teams and integrated T&E

As Resources allow for both organizations

- **Integrate** people, processes, and tools
- **Integrate** test, data analysis, and evaluation processes and tools
- Identify test requirements
- **Provide** risk assessments and evaluation
- **Identify** test requirements to evaluation of operational effectiveness and suitability
- **Observe, support, and collect** data from contractor iterations and support the planning and execution integrated T&E

T&E WIPT/ITT

Reviews:

- Development processes on code quality
- Team-oriented quality practices
- Capability and system-level quality practices
- Overall software quality assurance
- Relevant code testing

- **Confirm** competency in the automated test tools
- **Implement** constant feedback mechanisms
- **Coordinate** with user community
- **Ensure** overall system incorporates software
- **Ensure** user stories have traceability to higher requirements

13

Reflections – What Does This Mean for DOT&E AO Program Oversight?

Early and Frequent OT&E Integration into Program Acquisition

- Integrated test approach with contractor and developmental testing

- Augmenting agile software requirements with mission context

- Risk Acceptance Level of Testing – designing operational tests to collect data for ESS assessments

- Designing an integrated decision support key that repeats through each software release decision process

  - Integrating operational testing and evaluation to support software release decisions

  - Leveraging and maturing software factory test processes to collect ESS data

  - Ensuring software factory testing is operationally representative with representative users

Drafting OT&E and LFT&E plans and reports

- Develop software plans for each test type

- The TEMP/T&E strategy will outline the processes, frequency, and approval process for tests

- Test reports that are streamlined to support release in synchronization with development cadence