



# JITC Joint Interoperability Test, Evaluation, and Certification Overview

November 2016



# Agenda



- **Joint Interoperability Policy and Guidance**
- **Requirements and Evaluation Framework**
- **Joint Interoperability TE&C Process**
- **Links to Cyber Security**
- **Summary**



# Joint Interoperability Policy & Guidance



## United States Code, Title 10 – Armed Forces

- Chapter 131 requires the Secretary of Defense and the DoD Chief Information Officer to ensure that business systems, information technology, and national security systems are interoperable.

## DoDI 5000.02, Defense Acquisition System

- Provides detailed procedures guiding the operation of the Defense Acquisition System.
- Directs the Program Manager to ensure that interoperability certification is achieved in accordance with DoDI 8330.01.

### DoDI 8330.01

- Establishes interoperability policy, responsibilities, and procedures
- Overarching policy

### CJCSI 5123.01

- Defines JCIDS roles and responsibilities
- Absorbed portions of cancelled CJCSI 6212.01F

### DoDI 8100.04

- Establishes policy for the acquisition of network products.
- Process includes interoperability certification and cybersecurity evaluation

### IPG

- Implementation instructions for DoDI 8330.01
- Actionable procedures
- Contains list of NR KPP supporting DoDAF products

### CJCSI 3170.01

- Instructions for JCIDS process
- Provides a framework for process activities described in the JCIDS manual

### UCR

- Identifies the minimum requirements and features for UC products

### JITC 380-50-02

- JITC Policy for joint interoperability and standards conformance Test & Evaluation and Certification

### JCIDS Manual with Content Guide for NR KPP

- JCIDS requirements document content
- Guidance and procedures for NR KPP development, staffing, and certification
- Incorporates the NR KPP “how to” procedures from cancelled CJCSI 6212.01F
- Intelink on-line publication

### APL Process Guide

- Establishes and defines the process for listing a product on the APL

### JITC Evaluation Guidebook

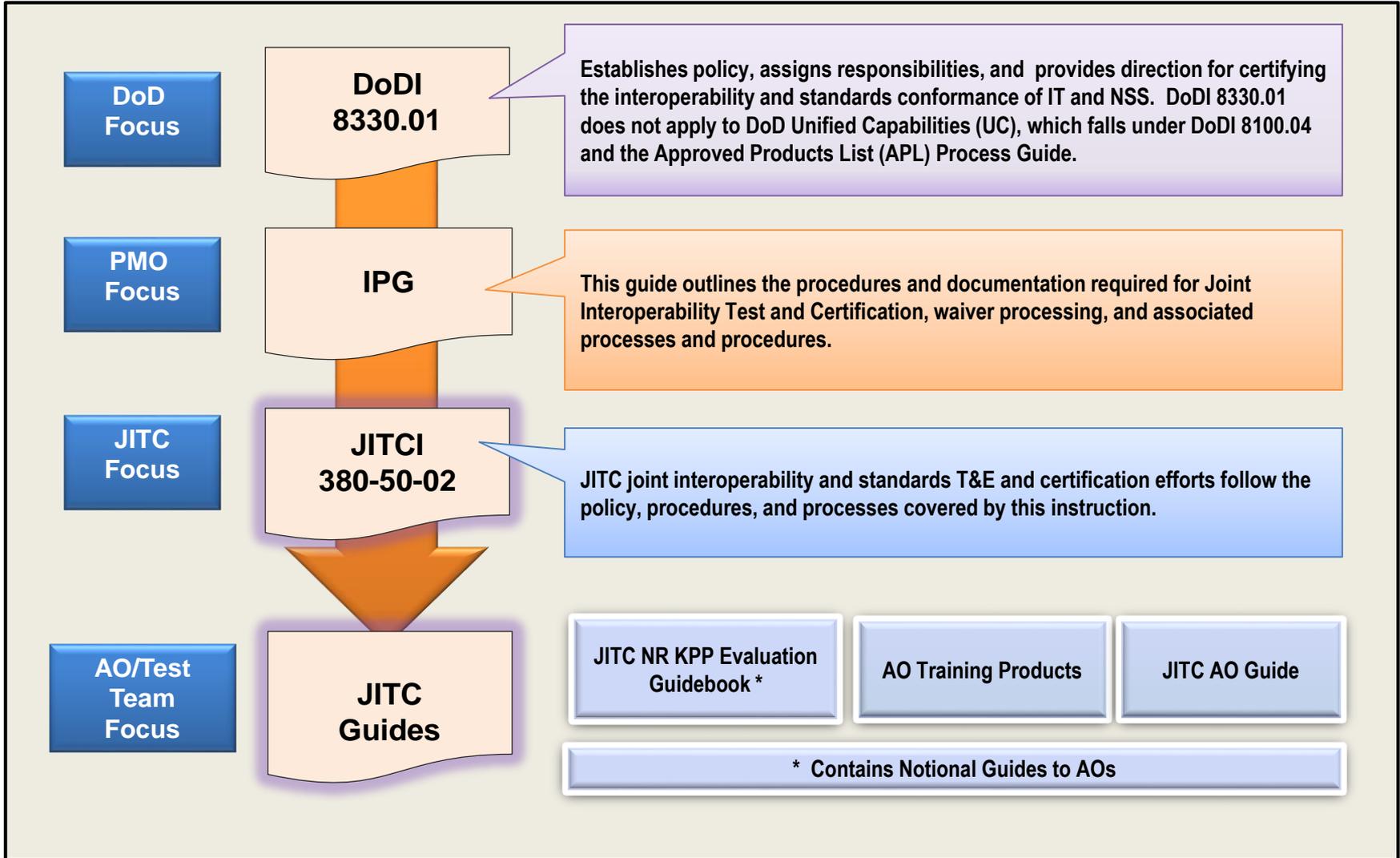
- “How-to” guide for evaluating joint interoperability based on the NR KPP
- Written for JITC AOs and testers

### Distributed Testing UC Implementation Guide

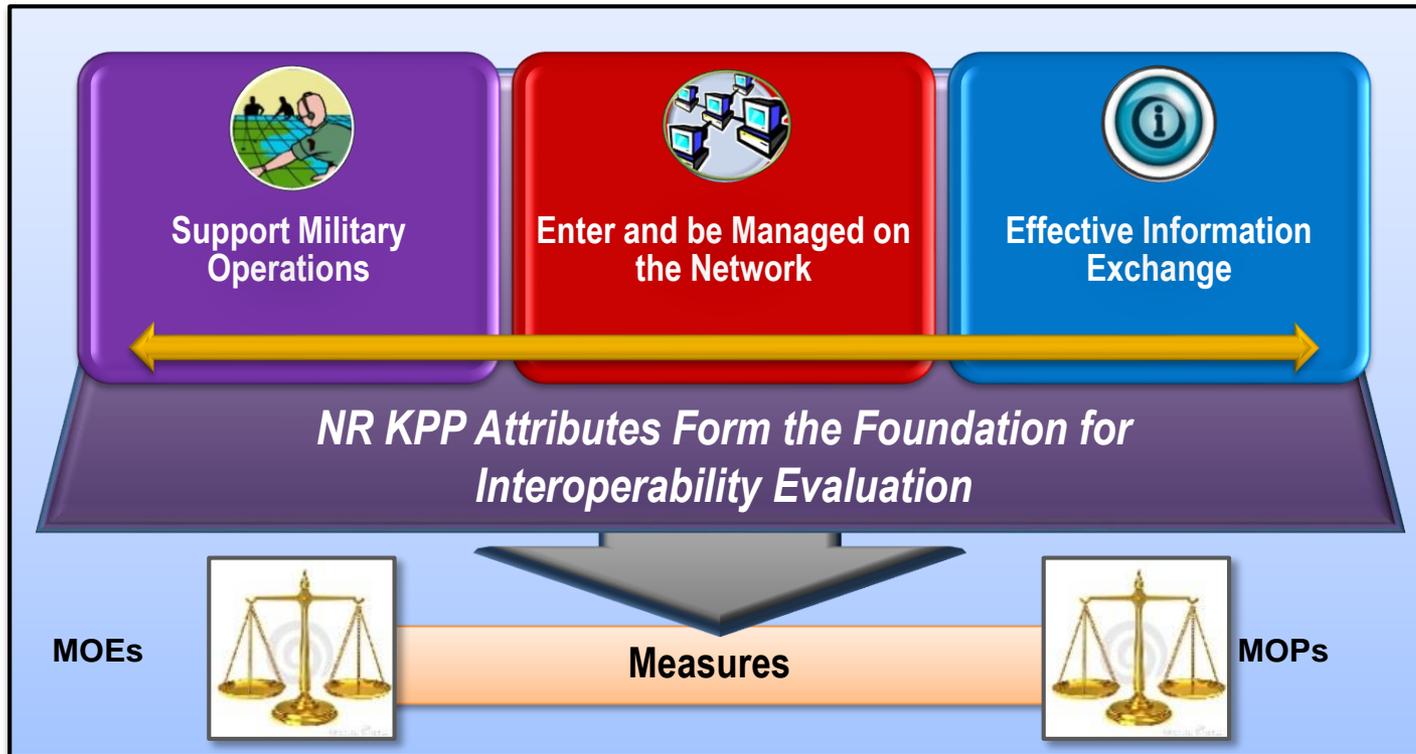
- Provides UC Action Officers and Test Officers with guidance on executing the UC APL process consistently across JITC and the U.S. Distributed Test Facilities

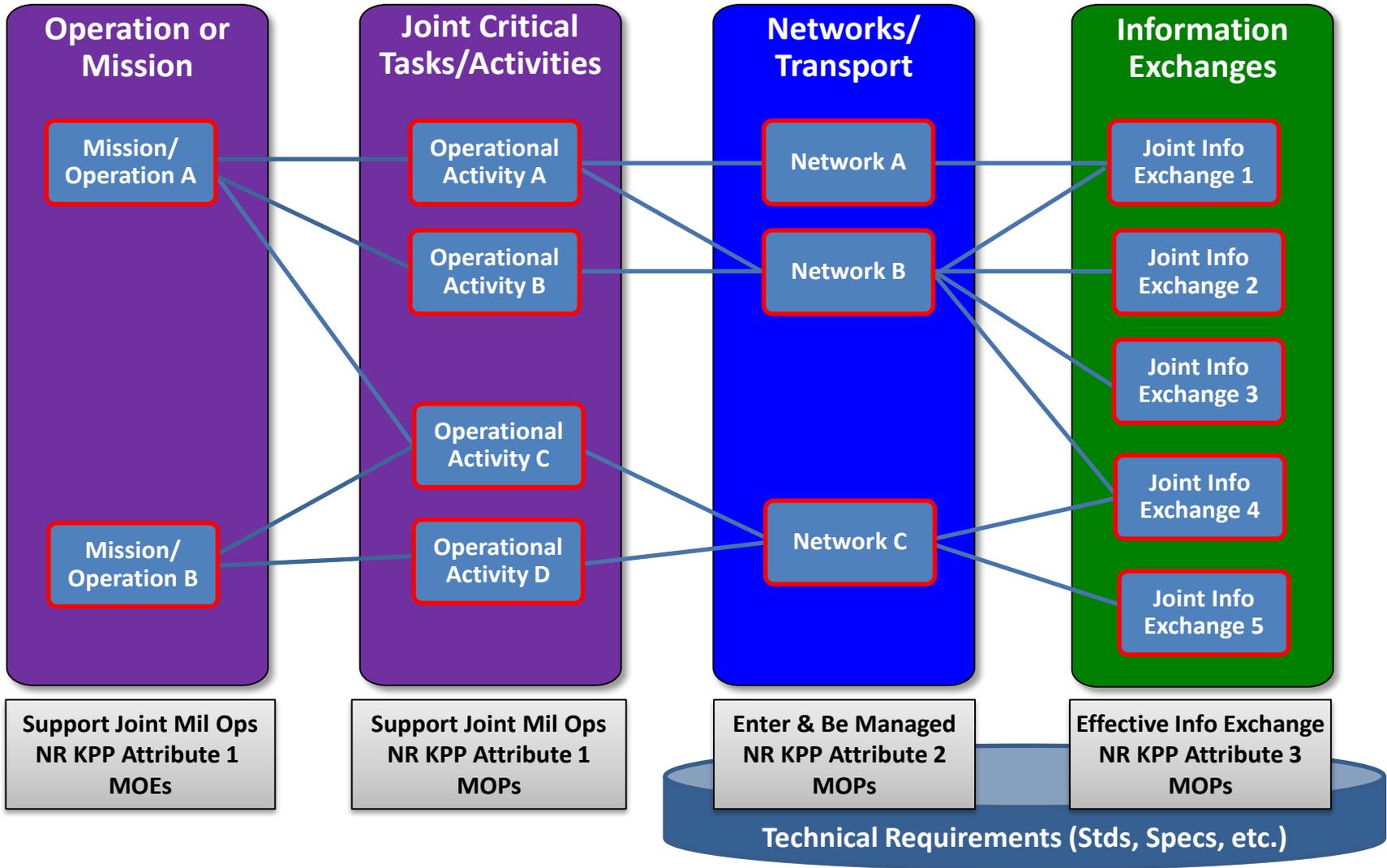


# Joint Interoperability Policy & Guidance



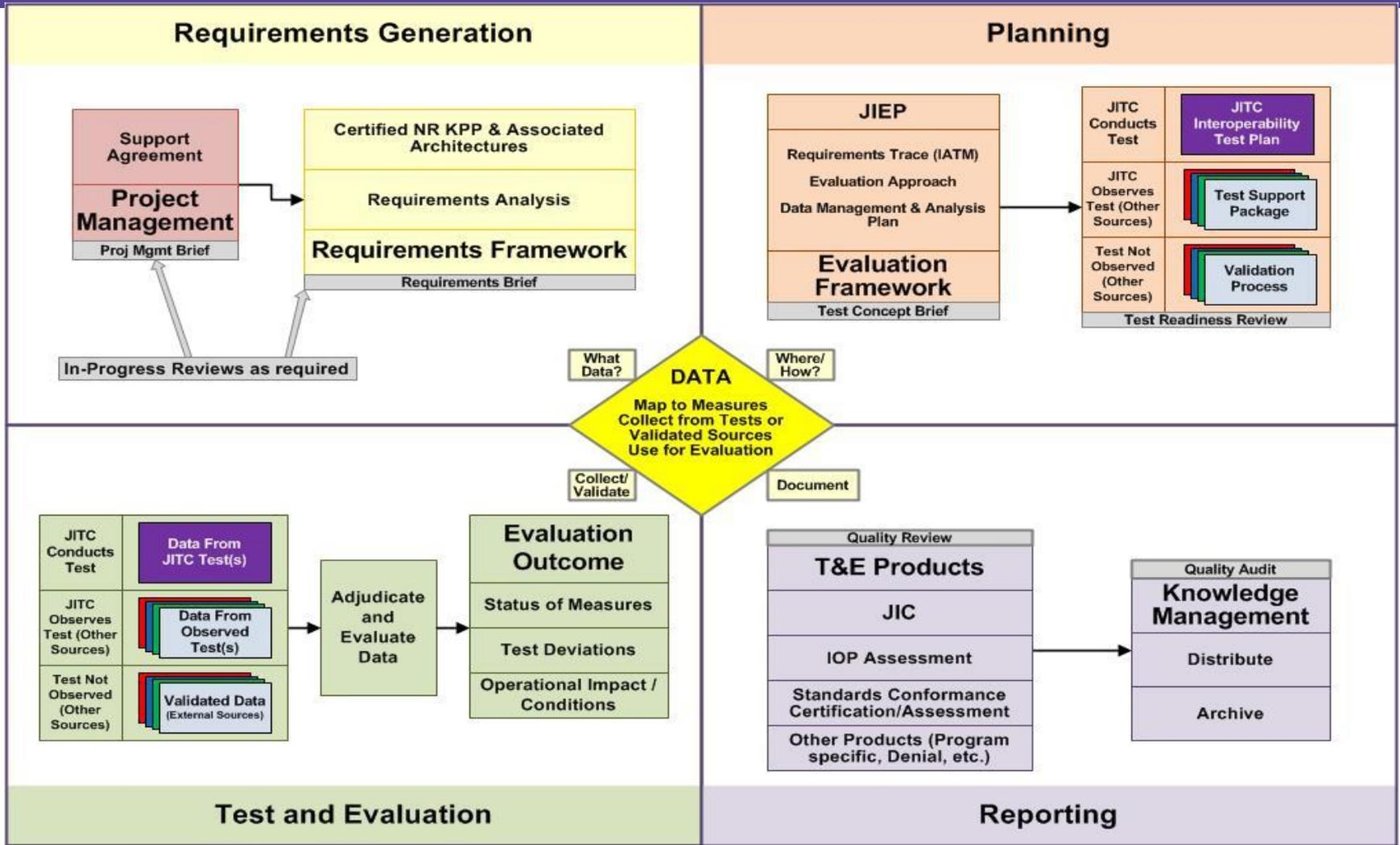
- CJCS updated Net-Ready KPP (circa 2012) to assess interoperability in terms of operational impact
- NR KPP is augmented with architecture viewpoints to complete requirements definition for attributes







# Joint Interoperability T&E Process Overview

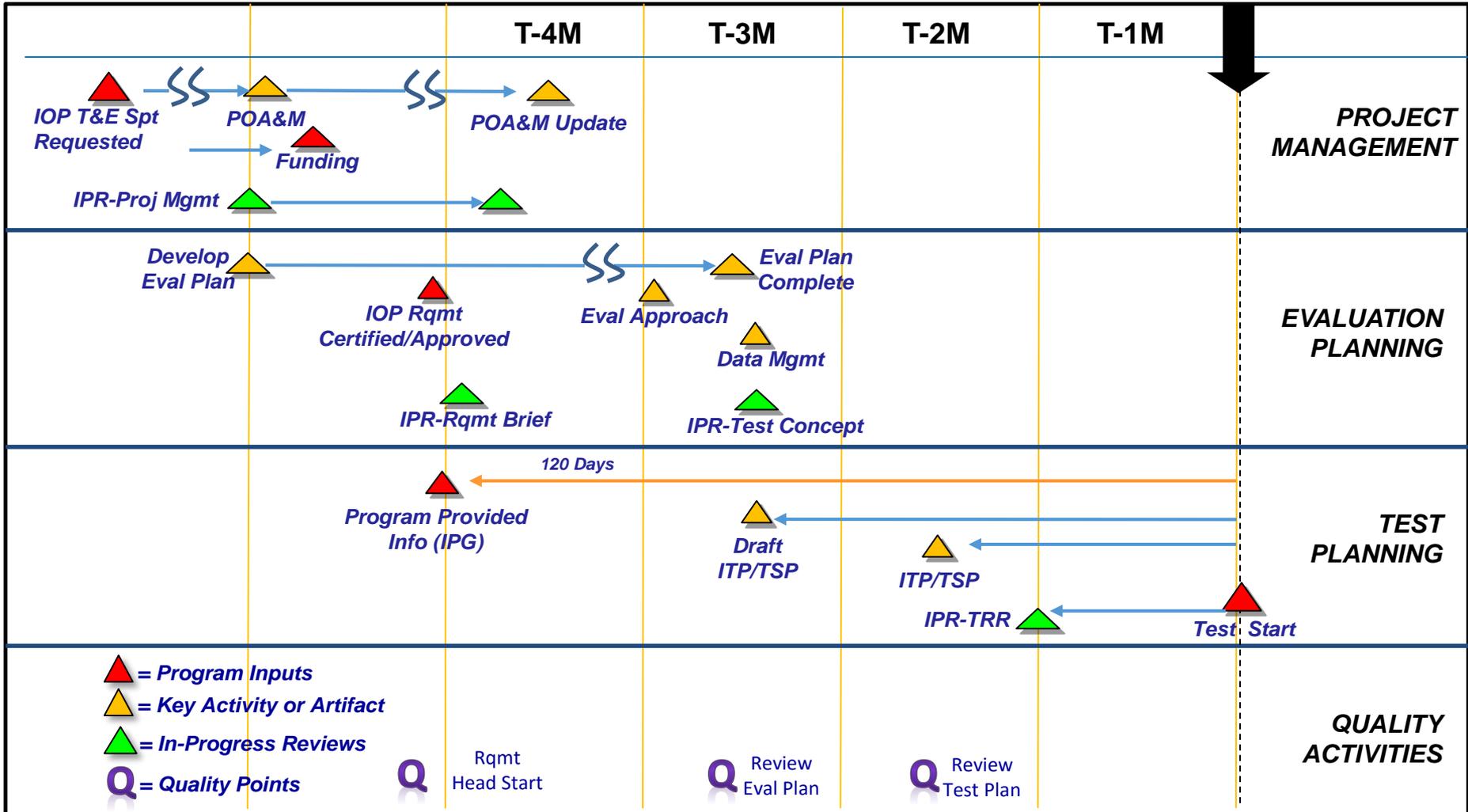


**Standardized Processes, Leveraging Data Reciprocity**



# Joint Interoperability T&E Process Overview

## Notional Pre-Test Milestones





# Joint Interoperability T&E Process Overview

## Links to Cyber Security



- **Test in operationally realistic environment to the extent feasible**
  - **Representative enterprise environment/configuration**
  - **Include Cyber/NetOps monitoring tools**
- **Test with production representative system**
  - **IT/NSS w/ Cyber accreditations to be on network/enterprise**
  - **Record IT/NSS Cyber configuration w/ cert**
- **Requirements for Enter/Be Managed under Attribute 2**



## Summary



- **Joint interoperability certification process is based on synchronized policies and guidance**
- **Standardization in Requirements Framework presents opportunity for automation and efficiencies**
- **Interoperability T&E augments Cyber security assessment through test environments and Attribute 2**
- **Interoperability Evaluation Framework augments OT&E, leveraging DT and mapping technical issues and performance shortfalls to operational impact**



**DEFENSE INFORMATION SYSTEMS AGENCY**  
The IT Combat Support Agency

**UNITED IN SERVICE TO OUR NATION**



# Standards Risk Assessment



## Overview

- **Assess risk associated with implementation of standards in context with the system under test**
- **JITC Action Officers leverage risk assessment during the formal joint interoperability review process (requirements generation)**
- **Information supports and promotes risk based 'trade' analysis during joint interoperability T&E planning**



## Standards Risk Assessment (continued)



- **JITC Standards Risk Assessment Methodology**
  - Develop and maintain Joint-Risk Assessment Database (J-RAD) using DISR, tester feedback, COIs
  - Identify critical implementations of standards (StdV-1)
  - Quantify risk factors and calculate risk for each implementation following the DoD Risk Methodology
- **Execution**
  - Conduct standards risk assessment for all 'Watch Listed' systems (using StdV-1)
  - Support additional risk assessments upon Branch or Division Chief request

J-RAD Login Page: <https://jitcweb4.fhu.disa.mil/JDMT/login.asp>



## Summary



- **Joint interoperability certification process is based on DoD policies and guidance**
- **Standardization in Requirements Framework presents opportunity for automation and efficiencies**
- **JITC's Joint Interoperability Evaluation Framework leverages DT, maps technical and performance issues to operational impact, which augments OT&E**
- **JITC employs a risk based approach to support 'trade analysis' during joint interoperability T&E planning**