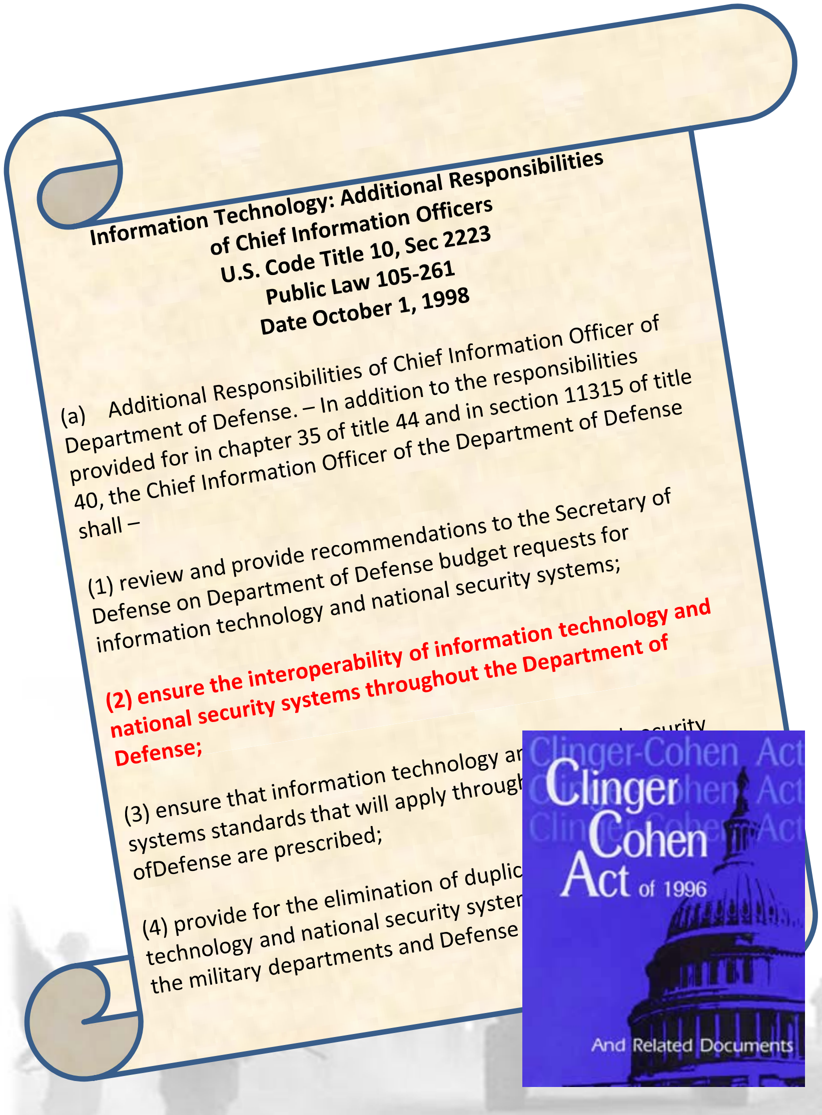
DoD Interoperability Policy and Process

National Defense Industrial Association

October 29, 2014

DoD Statutory Responsibility



Information Technology: Additional Responsibilities of Chief Information Officers
U.S. Code Title 10, Sec 2223
Public Law 105-261
Date October 1, 1998

(a) Additional Responsibilities of Chief Information Officer of Department of Defense. – In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of the Department of Defense shall –

(1) review and provide recommendations to the Secretary of Defense on Department of Defense budget requests for information technology and national security systems;

(2) ensure the interoperability of information technology and national security systems throughout the Department of Defense;

(3) ensure that information technology ar security
systems standards that will apply through
ofDefense are prescribed;

(4) provide for the elimination of duplic
technology and national security syster
the military departments and Defense

TITLE 10--ARMED FORCES

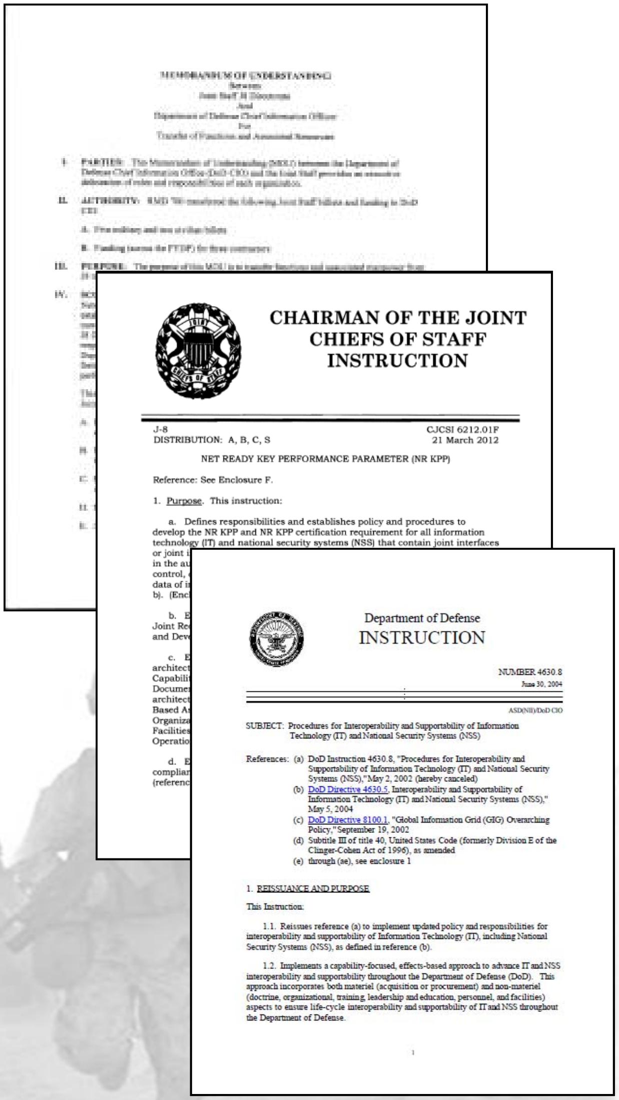
Sec. 2223. Information technology: additional responsibilities of Chief Information Officers

The DoD CIO shall:

Ensure the interoperability of information technology and national security systems throughout the Department of Defense

Impetus for Change

- **MOA between DoD CIO and JS (September 2011)**
  - Transferred Interoperability Certification Panel (ICP) and Interoperability Panel (IP) to DoD CIO
  - Transferred responsibility for Interoperability Test and Certification to DoD CIO
  - Maintained JS role as certifier of the NR KPP
- **CJCSI 6212.01F, Net Ready Key Performance Parameter (NR KPP), 21 March 2012**
  - Reflects MOA changes in roles and responsibilities
  - Eliminates guidance for interoperability test and certification
  - Establishes procedures for the NR KPP certification
- **DoD 4630.5/8 series, last issued in 2004, required update**



MEMORANDUM OF UNDERSTANDING
Between
Joint Staff J6 Directorate
And
Department of Defense Chief Information Officer
For
Transfer of Functions and Associated Resources

I. PARTIES: This Memorandum of Understanding (MOU) between the Department of Defense Chief Information Officer (DoD CIO) and the Joint Staff provides an executive delineation of roles and responsibilities of each organization.

II. AUTHORITY: RMD 700 transferred the following Joint Staff billets and funding to DoD CIO:

A. Five military and two civilian billets

B. Funding (across the FYDP) for three contractors

III. PURPOSE: The purpose of this MOU is to transfer functions and associated manpower from J6

IV.

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
INSTRUCTION

J-8
DISTRIBUTION: A, B, C, S

CJCSI 6212.01F
21 March 2012

NET READY KEY PERFORMANCE PARAMETER (NR KPP)

Reference: See Enclosure F.

1. Purpose. This instruction:

a. Defines responsibilities and establishes policy and procedures to develop the NR KPP and NR KPP certification requirement for all information technology (IT) and national security systems (NSS) that contain joint interfaces or joint i
in the au
control,
data of i
b). (Encl

b. E
Joint Re
and Deve

c. E
architect
Capabilit
Documen
architect
Based A
Organiza
Facilities
Operatio

d. E
complian
(referenc

Department of Defense
INSTRUCTION

NUMBER 4630.8
June 30, 2004

ASD(NII)/DoD CIO

SUBJECT: Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

References: (a) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002 (hereby canceled)
(b) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) Subtitle III of title 40, United States Code (formerly Division E of the Clinger-Cohen Act of 1996), as amended
(e) through (ae), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues reference (a) to implement updated policy and responsibilities for interoperability and supportability of Information Technology (IT), including National Security Systems (NSS), as defined in reference (b).

1.2. Implements a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability throughout the Department of Defense (DoD). This approach incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership and education, personnel, and facilities) aspects to ensure life-cycle interoperability and supportability of IT and NSS throughout the Department of Defense.

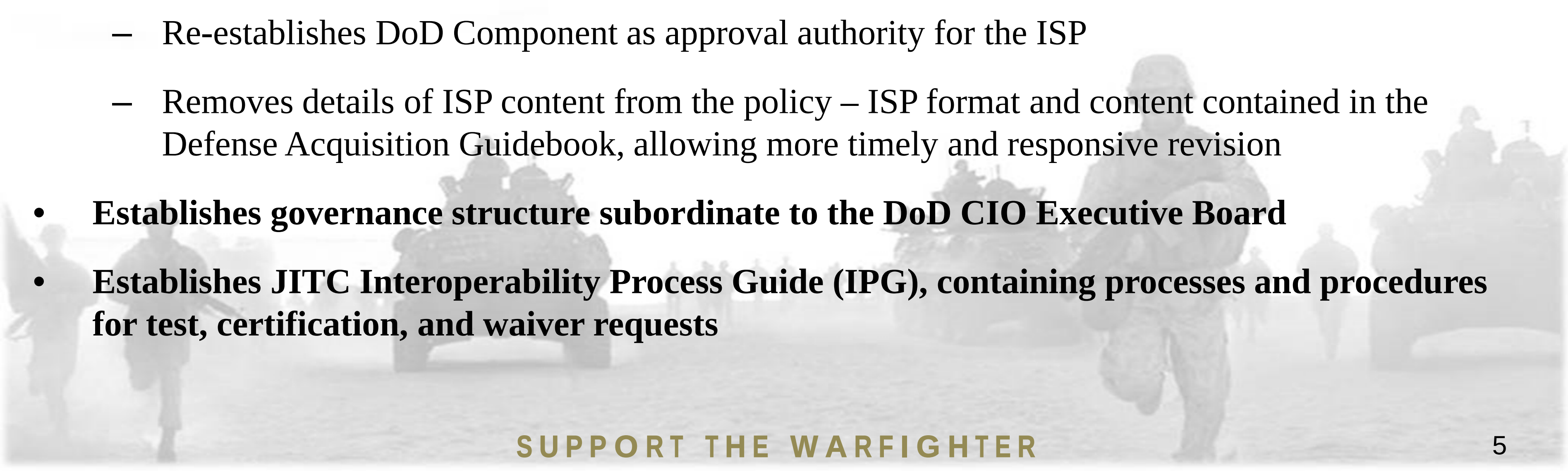
1

DoDD/I 4630 Interoperability Policy Issues

- No forcing function
- Interoperability governance structure outdated
- Previous JFCOM responsibilities unassigned
- USSTRATCOM/USCYBERCOM responsibilities not reflected
- Current Information Support Plan (ISP) process required update

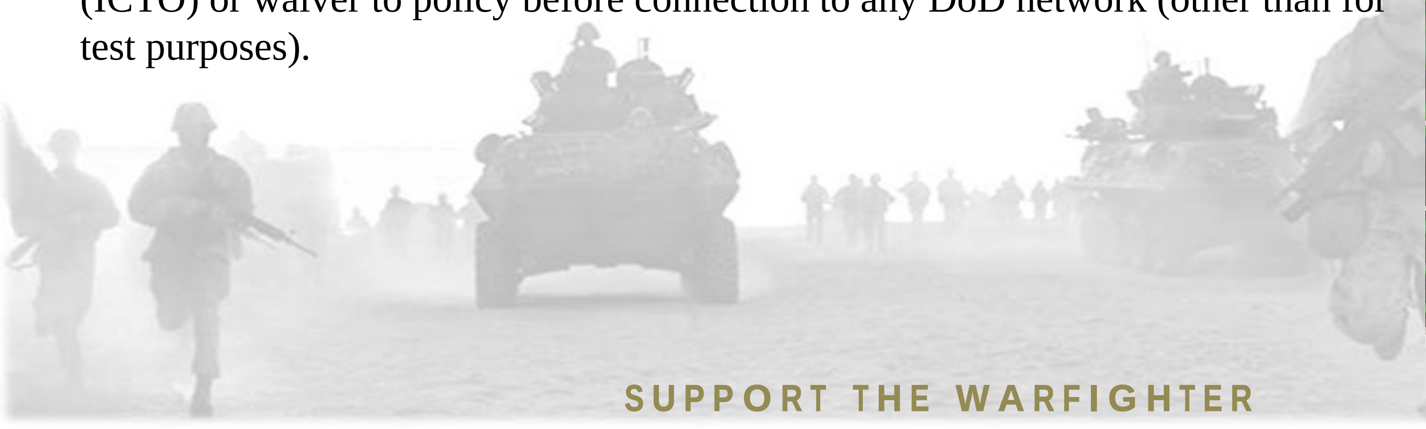
DoDI 8330.01 Interoperability Approach

- **Restricts policy to only interoperability – removes responsibilities and processes covered under separate policy (IA, standards, architecture)**
- **New division of roles and responsibilities:**
  - Joint Staff responsible for the interoperability requirement (NR KPP)
  - DoD CIO responsible for interoperability test and certification, and interoperability governance
- **Creates forcing function – interoperability test and certification a prerequisite for connection of IT, including NSS**
- **Streamlines the ISP process:**
  - Re-establishes DoD Component as approval authority for the ISP
  - Removes details of ISP content from the policy – ISP format and content contained in the Defense Acquisition Guidebook, allowing more timely and responsive revision
- **Establishes governance structure subordinate to the DoD CIO Executive Board**
- **Establishes JITC Interoperability Process Guide (IPG), containing processes and procedures for test, certification, and waiver requests**



Interoperability Policy Precepts

- IT that DoD Components use must interoperate with existing and planned systems (including applications) and equipment of joint, combined, and coalition forces, other U.S. Government departments and agencies, and non-governmental organizations
- IT interoperability must be evaluated early and with sufficient frequency throughout a system’s life cycle to capture and assess changes affecting interoperability in a joint, multinational, and interagency environment.
- All IT, including defense acquisition and procurement programs and enterprise services, must have a net ready key performance parameter (NR KPP) as part of its interoperability requirements documentation.
- IT must be certified for interoperability, or possess an interim certificate to operate (ICTO) or waiver to policy before connection to any DoD network (other than for test purposes).



DoD Instruction 8330.01

Interoperability of IT, Including National Security Systems

- Updated/replaced DoD's 10 year old interoperability policies (DoDD/DoDI 4630)
- Established policy, assigned responsibilities, and provided direction for certifying the interoperability of IT
  - Requires Interoperability Certification prior to connection to a DoD network
  - Establishes 2 tiers of interoperability certification:
    - *For IT with joint, multinational, or interagency interoperability requirements: Joint Staff certifies the NR KPP, JITC tests and certifies the system against the NR KPP*
    - *For all other IT: individual DoD Components certify the NR KPP, and test and certify the system against the NR KPP*
  - Streamlined the ISP review process
  - Formally established the Interoperability Steering Group (ISG) to provide oversight
- Signed by Acting DoD CIO 21 May 2014

Interoperability Governance

The Interoperability Steering Group (ISG):

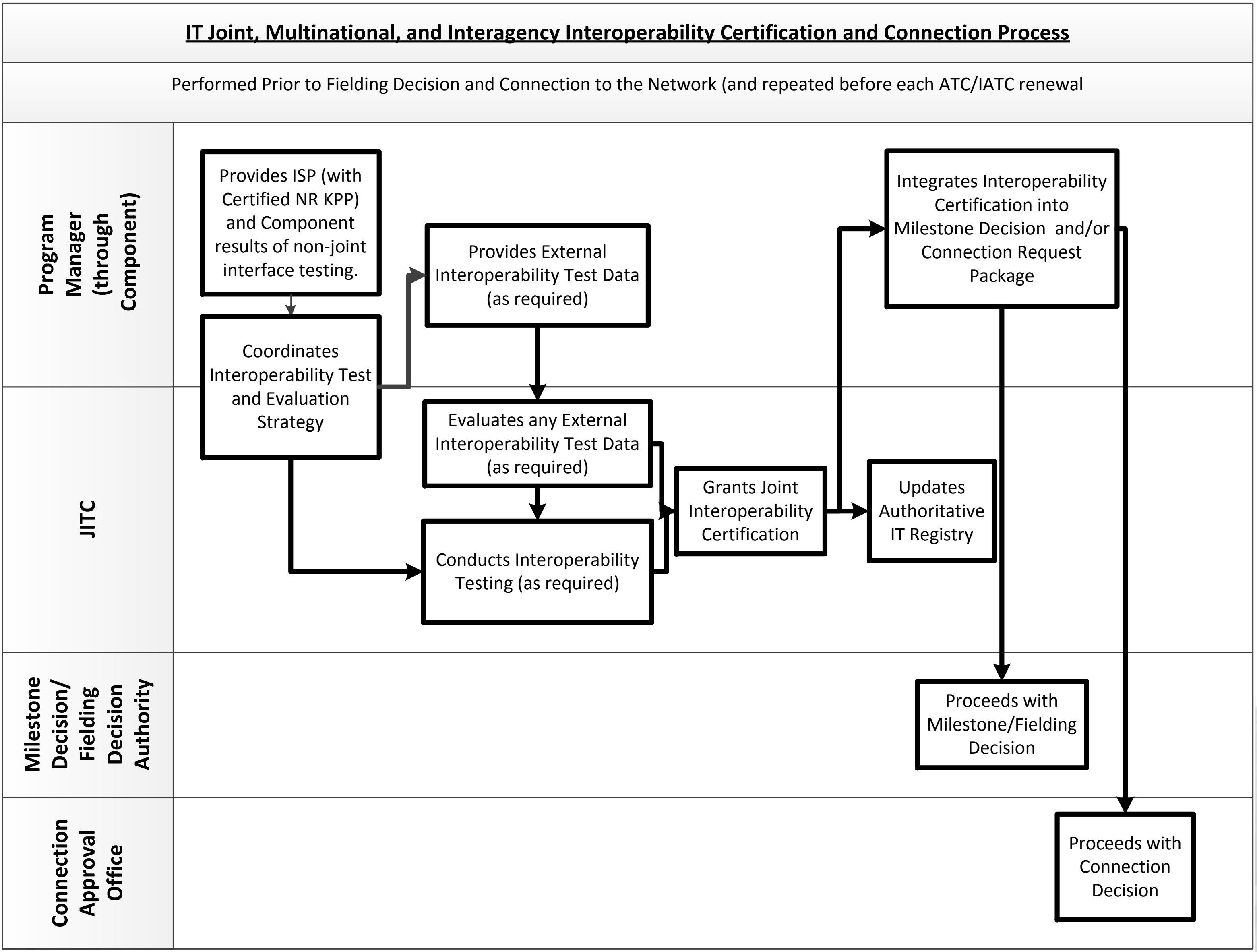
- Replaces both the Military Communications Electronics Board’s ICP and IP
- Is subordinate to the CIO Executive Board
- Is tri-chaired by representatives from DoD CIO, AT&L, and CJCS
- Proposes, reviews, and coordinates interoperability policies; reviews critical interoperability issues; and adjudicates requests for Interim Certificates to Operate (ICTOs) and waivers to policy

DoD Interoperability Steering Group (ISG)

- Purpose: Provides a forum to coordinate policy and provide oversight and direction across DoD organizations in ensuring the interoperability of IT and NSS. The ISG proposes, reviews, and coordinates interoperability policies; reviews interoperability issues; and reviews and approves requests for Interim Certificates to Operate (ICTOs) and waivers to policy.
- Tri-chaired by representatives from the DoD CIO, USD (AT&L), and the CJCS
- Meets every other month in person—handles routine ICTO and waiver requests out-of-cycle
- Value added:

CY	ICTOs	Waivers	Joint IOP Certs
2011	310	116	252
2012	232	114	314
2013	158	32	319
2014 *(to date)*	*119*	*32*	*234*

IT Interoperability Certification and Connection Process



IT Joint, Multinational, and Interagency Interoperability Certification and Connection Process

Performed Prior to Fielding Decision and Connection to the Network (and repeated before each ATC/IATC renewal

Program Manager (through Component)

- Provides ISP (with Certified NR KPP) and Component results of non-joint interface testing.
- Coordinates Interoperability Test and Evaluation Strategy
- Provides External Interoperability Test Data (as required)
- Integrates Interoperability Certification into Milestone Decision and/or Connection Request Package

JITC

- Evaluates any External Interoperability Test Data (as required)
- Conducts Interoperability Testing (as required)
- Grants Joint Interoperability Certification
- Updates Authoritative IT Registry

Milestone Decision/ Fielding Decision Authority

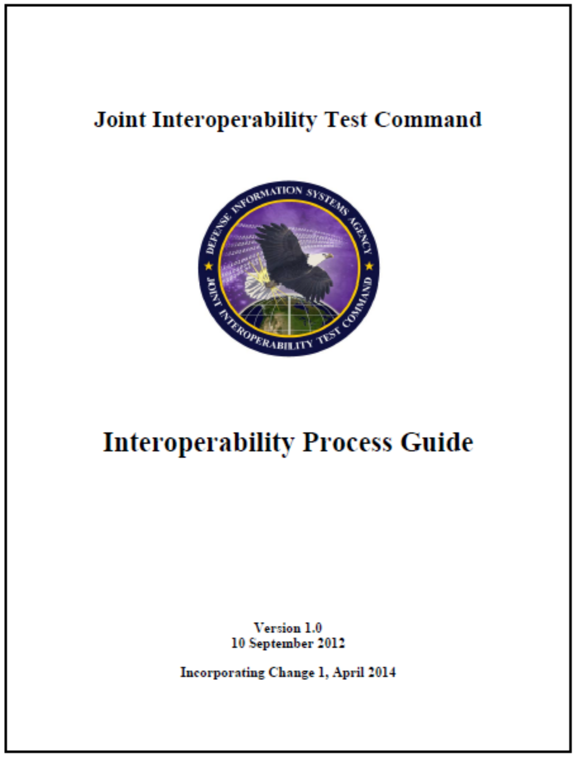
- Proceeds with Milestone/Fielding Decision

Connection Approval Office

- Proceeds with Connection Decision

DoD Interoperability Process Guide (IPG)

- Outlines the procedures and documentation required for Joint Interoperability Test and Certification, waiver processing, and associated processes and procedures
- *IPG Version 1* was jointly signed by DISA T&E Executive and Director A&I in 2012
- *Change 1* to the IPG issued to update and revise the IPG to include:
  - Fact-of-life changes
  - Updated waiver and Interim Certification to Operate processes
  - Operating at Risk List processes
  - Guidance to define the minimum architecture data needed for interoperability certification



Joint Interoperability Test Command

Interoperability Process Guide

Version 1.0
10 September 2012

Incorporating Change 1, April 2014

- <u>Status</u>:
  - *IPG Version 1 Change 1* was co-signed by DISA Test & Evaluation Executive and Acting DCIO(IE) PD 30 April 2014

Architecture Viewpoints Required for Interoperability Certification

Viewpoint	Description
REQUIRED Architecture Viewpoints for Joint Interoperability Certification	
AV-1	Overview of architecture scope and context, describes the concepts contained in the OV-1.
AV-2	Integrated Dictionary – defines all terms and metadata used in the architecture.
OV-1	High Level Operational Concept Graphic – describes operational concept.
OV-2	Operational nodes, needlines, and activities - information exchanges between operational nodes.
OV-3	Information exchanges and associated measures and metrics.
OV-5b	Operational Activity Model - NR KPP Missions/Tasks - activity level depiction.
OV-6c	Event-Trace Description - lifelines (nodes) and events.
SV-1	Systems Interface Description - defines system functions and information flow among systems.
SV-2	Systems Resource Flow Description - communications links, networks, and systems.
SV-5a	Maps system functions (activities) to operational activities.
SV-6	System data exchanges & associated measures and metrics.
SV-7	Complete set of system performance parameters (measures).
CONDITIONAL Architecture Viewpoints for Joint Interoperability Certification	
DIV-2	Logical Data Model - architecture data definitions.
DIV-3	Physical Data Model - describes how DIV-2 is implemented.
StdV-1	Standards Profile - list of implemented technical standards, rules, and guidelines.
SV-5b	Maps systems to operational activities.
SvcV-1	Services Context Description – identifies services and their interconnections.
SvcV-2	Specifies resource flows exchanged between services, and may list protocol stacks.
SvcV-4	Depicts allocation of service functions and data flows between service functions (activities).
SvcV-5	Maps services (activities) to operational activities.
SvcV-6	Maps service data exchanges with associated measures and metrics.
SvcV-7	Complete set of performance parameters (measures) of the services.
OPTIONAL Architecture Viewpoints for Joint Interoperability Certification	
CV-all	Capability Viewpoints – taxonomy, capability evolution, etc.
OV-4	Key architecture players and organizational relationships.
OV-5a	Describes capabilities and operational activities.
PV-all	Project capability delivery and dependencies.
StdV-2	Emerging standards (may be conditional if emerging standards are implemented and not in StdV-1).
SV-4	Defines data flow input and output by each function (activity).