

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive current as of 11 May 2011

J-6

DISTRIBUTION: A, B, C, J, S

CJCSI 8410.01A

20 March 2009

WARFIGHTING MISSION AREA INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT AND NET-CENTRIC DATA SHARING

References: See Enclosure D.

1. Purpose. This instruction establishes policies and procedures for the Warfighting Mission Area (WMA) Information Technology (IT) portfolio management and net-centric data sharing processes. The WMA IT portfolio management process implements references a through c in support of the Functional Capability Boards (FCB) (reference d) and facilitates IT investment (acquisition programs, information systems, and initiatives) management within the joint WMA. The detailed WMA IT portfolio management process is described in Enclosure B. The WMA net-centric data sharing process, detailed in Enclosure C, establishes processes to adjudicate conflicts in metadata agreements among WMA-affiliated Communities of Interest (COI) per reference e.

2. Cancellation. CJCSI 8410.01, 22 June 2007, "Warfighting Mission Area Information Technology Portfolio Management and Net-Centric data sharing," is canceled.

3. Applicability. In accordance with references b, c, and e, this instruction applies to the DOD components, including the Joint Staff, Military Departments, Services, combatant commands, Defense agencies, and joint and combined activities. This instruction also applies to all unclassified, classified, collateral, compartmented, legacy, and developing warfighter IT (to include National Security Systems (NSS)) investments (acquisition programs, information systems, and IT initiatives) and associated COIs.

4. Overview

a. WMA's objective is to enable joint military operational effectiveness

through effective warfighter IT. WMA was established to manage warfighter IT investments as portfolios focusing on improving joint capabilities and mission outcomes (reference b). WMA IT investments, to include NSS, automated information systems (reference f), and models and simulations support and enhance the Chairman of the Joint Chiefs of Staff's (hereafter, "Chairman") joint warfighting priorities. WMA IT investments also support actions to create a net-centric, distributed force capable of full spectrum dominance through decision and information superiority. WMA IT domains accomplish IT portfolio management processes in support of their associated FCBs (reference d). Through the FCBs, WMA will provide input to the Planning, Programming, Budgeting, and Execution (PPBE) System (reference g) and Defense Acquisition System (DAS) (reference f) processes. Inputs will include life cycle (e.g., capabilities, resources, acquisition, development, operations, upgrades, deactivation, and retirement/reutilization or demilitarization) oversight (reference c).

b. Recommendations to initiate, continue, modify, or terminate WMA IT investments (references b and c) will be warfighter focused; will enable jointness; will support combined coalition and interagency operations; will align resources, processes, and communications supporting DOD's missions and priorities and "*The Capstone Concept for Joint Operations*;" will manage risk; and will enable change. IT investment recommendations will provide technical solutions that enable timely, relevant, and accurate information sharing. These investments are built on integrated military and civilian strategic, operational, tactical, and support direction and guidance and are designed to interoperate with other instruments of national power.

5. Policy. The WMA IT portfolio management process enables effective IT capability fielding, implementation, and sustainment to satisfy Joint Requirements Oversight Council (JROC) validated capability requirements, enable successful mission outcomes, and integrate with Joint Capabilities Integration and Development System (JCIDS) (reference h), DAS (reference f), and PPBE (reference g) decision systems. WMA IT portfolio management identifies and recommends balanced and prioritized IT investments to the FCBs to enable the joint warfighter to accomplish their assigned missions. Joint Staff policy requires WMA IT portfolio management to:

a. Manage IT investments (whether in acquisition, fielding, or sustainment) as portfolios and ensure they support the Department of Defense's vision, mission, and goals and the Chairman's priorities (reference i) to ensure efficient and effective joint warfighting abilities and to maximize return on investment to the enterprise. Each portfolio will be managed in support of the appropriate FCB using architectures, plans, risk management techniques, capability goals and objectives, and scoring criteria to defend our national interests; reset, reconstitute, and revitalize our armed forces; and balance global strategic risk.

b. Minimize IT investment risk by identifying and recommending balanced and prioritized IT capabilities to ensure the joint warfighter has the right tools to accomplish the mission within resource constraints. WMA IT investments will also include functionally aligned non-DOD systems (sponsored by other departments or coalition/allies) used to support the joint warfighter as discussed in reference c.

c. Use a standardized portfolio management process. Develop capability based IT portfolios for analysis/evaluation, selection, and control through standardized WMA scoring criteria and integrated portfolio management activities. Provide IT portfolio management results to JCIDS through the FCB process. The WMA scoring criteria will include FCB developed Joint Capability Area (JCA) metrics, as appropriate. Additionally, provide WMA portfolio management IT investment recommendations to the FCBs to support their participation in the PPBE and DAS processes. Document IT investment recommendations in the WMA Roadmap (reference c) as described in Enclosure B.

d. Provide lifecycle IT investment oversight through program, system, or initiative termination. Exercise sound investment strategy and best practices and reduce unnecessary IT capability duplications and gaps to improve warfighting effectiveness.

e. Align the WMA IT domain portfolio with the appropriate FCB (reference d) and employ the Joint Capabilities Board (JCB) and the JROC for governance to satisfy JROC validated capabilities and mission outcomes.

f. Provide FCBs with IT portfolio management results. FCBs will, in turn, provide input to the Capability Portfolio Managers (CPM) (reference j) and the other DOD decision support processes (DAS and PPBE).

g. Manage the WMA IT portfolio according to reference k with focus on efforts to minimize duplication of DOD and government wide initiatives.

h. Integrate scoring criteria within the portfolio management process as discussed in Enclosure B, including implementing JCA metrics to assess IT investment contributions through the analysis of enterprise architecture. Scoring criteria will evaluate both portfolio management and data sharing implementation and effectiveness.

i. Develop a standardized portfolio management process and WMA Roadmap to enhance the FCBs' ability to identify IT capability gaps and overlaps.

j. Develop a standardized process to keep portfolio management current on information sharing decisions.

k. Support the FCBs as Capabilities Based Assessments (CBA) (reference h) are developed and JCIDS documents are reviewed.

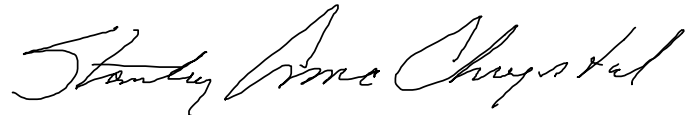
6. Definitions. See Acronyms and Glossary (Enclosure GL).

7. Responsibilities. See Enclosure A.

8. Summary of Changes. Clarified IT domain support to FCBs who, in turn, coordinate with CPMs to eliminate process duplication. Updated Chairman's guidance in the WMA overview and objectives with a reference to the guidance. Replaced JCA-specific domain descriptions with the JCA URL to maintain currency as JCAs are changed/updated. Changed the WMA binning process to the WMA portfolio development process. Eliminated example scoring criteria questions. Combined WMA IT portfolio management analysis and evaluation phases to eliminate overlaps. Updated domain implementation plans to FCB IT implementation plans based on lessons learned. Updated data sharing direction. Updated references.

9. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.

10. Effective Date. This instruction is effective upon receipt.



STANLEY A. MCCHRYSTAL
Lieutenant General, USA
Director, Joint Staff

Enclosures:

- A -- Responsibilities
- B -- WMA IT Portfolio Management Process
- C -- WMA Net-Centric Data Sharing Process
- D -- References
- GL -- Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
Secretary of State.....	2
Secretary of Defense.....	2
Director of National Intelligence	2
Department of Transportation	2
United States Coast Guard.....	2

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	Page
ENCLOSURE A RESPONSIBILITIES	A-1
The Joint Staff/J-6.....	A-1
The Joint Staff/J-8.....	A-4
The Joint Staff/J-7	A-4
The Joint Staff, Directorate of Management	A-4
The WMA IT Domain Owners	A-4
The WMA IT Domain Owner Council	A-7
The Combatant Commands	A-8
Services	A-9
Other DOD Components.....	A-10
ENCLOSURE B WMA IT PORTFOLIO MANAGEMENT PROCESS.....	B-1
Introduction	B-1
The IT Portfolio Management Relationship Between Functional Capability Boards and Capability Portfolio Managers.....	B-1
WMA IT Domain Scope	B-2
WMA IT Investment Portfolio	B-3
Develop WMA IT Investment Portfolio	B-3
Develop Standardized Mission Area-wide and Domain Specific Criteria ..	B-8
Analyze/Evaluate IT Investments	B-10
Select IT Investments	B-12
Control IT Investments (Recommendations)	B-14
Informing the JCIDS Process	B-17
WMA IT Portfolio Management of Defense Business Systems	B-18
ENCLOSURE C WMA NC DATA SHARING PROCESS	C-1
Overview	C-1
COI Activities	C-1
Enabling COIs	C-1
Governance and Management	C-2
COI Resourcing	C-2
WMA Data Sharing Working Group	C-2
ENCLOSURE D REFERENCES	D-1
ENCLOSURE GL GLOSSARY	GL-1

FIGURE	PAGE
B-1 The Relationship of IT Portfolio Management to the Functional Capabilities Board and the Capability Portfolio Manager	B-1
B-2 The WMA IT Portfolio Management Process	B-2
B-3 Develop the WMA IT Investment Portfolio	B-4
B-4 Develop Mission Area-wide and Domain Specific Criteria	B-9
B-5 Analyzing/Evaluating WMA IT Investments	B-11
B-6 Selecting WMA IT Investments	B-13
B-7 Controlling WMA IT Investments	B-14
B-8 How IT Portfolio Management Can Inform the JCIDS Process.....	B-17

ENCLOSURE A
RESPONSIBILITIES

1. The Joint Staff, J-6. J-6 will:

- a. Serve as the Chairman's WMA lead (IT integrator) to implement references a-c.
- b. Provide guidance to WMA domains to develop the WMA IT investment portfolio consistent with DOD Information Enterprise Architecture (DOD IEA) and to develop the Global Information Grid (GIG 2.0) architecture. The GIG 2.0 architecture is JCA based to enable joint warfighting priorities.
- c. Develop WMA IT portfolio policy and guidance for CJCS approval as directed by reference b.
- d. Provide WMA IT support to the FCBs, which are responsible for coordinating capability portfolio management activities with CPMs per reference j.
- e. Represent WMA on the DOD Chief Information Officer (CIO) Executive Board (reference l) and on other mission area portfolio management forums (reference c), and coordinate with the DOD CIO to issue policy and procedures for WMA IT support to the FCBs (reference b).
- f. Leverage the JCIDS governance structure as the WMA IT portfolio management governance forum.
- g. Ensure WMA IT portfolio management is incorporated into and integrated with the JCIDS process.
- h. In coordination with DOD CIO, ensure DOD IT portfolio management policy is incorporated into National Defense University's Information Resources Management College and other DOD and joint schools' curriculum, as appropriate.
- i. Approve overarching, joint scoring criteria for WMA-wide IT investment portfolio analyses and evaluation to ensure an adequate evaluation is conducted. The scoring criteria will reflect the Chairman's and combatant commanders' warfighting priorities and the IT investment's ability to meet WMA

20 March 2009

DOD IEA criteria (e.g., DOD IEA and GIG 2.0 requirements) and appropriate capability portfolio management metrics and capability delivery increment goals (as directed by the FCB).

j. Approve WMA Roadmap after coordination with Services, combatant commands, and the other DOD components prior to signature.

k. Determine whether WMA IT portfolio management results improved/decreased joint warfighter information technology capability.

l. Facilitate WMA Net-Centric Data Strategy (NCDS) and Net-Centric Services Strategy (NCSS) (references m and n) implementation, including leading appropriate WMA NCDS/NCSS related bodies, such as the WMA Data Sharing Working Group (WG), and resolving NCDS, NCSS, and related issues across domains, components, and capability portfolios.

m. After final coordination with the FCBs, provide the approved WMA Roadmap to the CPMs.

n. Assign a WMA IT integration staff that will accomplish day-to day portfolio management responsibilities for the J-6 integrator, to include:

(1) Resolve WMA-wide process, procedure, and cross-domain issues.

(2) Coordinate WMA IT investment issues and recommendations to initiate, continue, modify or terminate the investments among FCB working groups via the O-6 and general/flag officer (G/FO) FCB Integration Meetings (reference d), and among DOD mission areas, Services, and other DOD components. Review proposed IT investment mission area or domain/FCB assignment changes within the DOD IT Portfolio Repository (DITPR). Ensure the FCB's IT domain reviews recommended changes with both affected (losing and gaining) mission areas sub-portfolios/domains or WMA domains/FCBs (reference c). Adjudicate unresolved mission area assignment conflicts with mission area leads when their sub-portfolios and WMA domains/FCBs are unable to reach agreement regarding IT investment ownership and recommend a course of action, as required. If agreement can not be reached with the other mission area leads, elevate portfolio assignment disconnects to the DOD CIO Enterprise Governance Board (EGB) for adjudication (reference c). Within WMA, determine IT investment domain ownership when FCBs are unable to reach resolution.

(3) Develop, coordinate, and issue overarching IT portfolio management scoring criteria for J-6 approval.

(4) Provide requirements to the Joint Staff Director of Management, Office of the Chief Information Officer to acquire a WMA IT portfolio

20 March 2009

management analysis tool (Joint Information Technology Analysis and Management (JITAM)) to accomplish WMA IT portfolio management. Develop implementation business rules for JITAM. Ensure business rules include doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) implications. Facilitate access to JITAM and manage JITAM's configuration through the Joint Staff Office of the CIO (reference o). Make the tool available, as appropriate, to affected DOD components.

(5) Consolidate FCB approved implementation plans (see enclosure B for the implementation plan template) with recommendations to initiate, continue, modify, and terminate IT investments into the WMA Roadmap according to reference c. Coordinate the WMA Roadmap with the Services, combatant commands, CPMs, and DOD components.

(6) Support the FCBs' work with the CPMs (reference j) to eliminate process duplication.

(7) Coordinate with the DOD CIO and the other mission area leads to promote IT portfolio management strategy, plans, and process consistency.

(8) Ensure WMA participation in the DOD IT Portfolio Management Community of Practice forum and at other mission area lead governance forums to develop portfolio strategic direction, identify IT investment opportunities, and resolve cross-mission area issues.

(9) Facilitate WMA domain access to the DITPR and coordinate with DOD CIO regarding WMA recommended changes to DITPR.

(10) Participate in the DITPR technical solutions Integrated Process Team and DITPR Design Reviews and support J-6 participation in DITPR In-Progress Review/Requirements Review Board and DITPR working groups.

(11) Provide DITPR configuration, policy, and guidance updates to the combatant commands as they occur.

(12) Assist WMA IT domain owner efforts to promote net-centric data sharing, effectively enable COIs, adjudicate conflicts in metadata agreements, coordinate Service Oriented Architecture (SOA) development, and identify authoritative sources as directed by reference e.

(13) Participate in FCB Working Group and Integration Meetings, as appropriate (reference d).

(14) Chair the WMA IT Domain Owner Council.

(15) Develop the GIG 2.0 architecture consistent with the DOD IE architecture which describes the high-level operational characteristics, activities, systems, services, standards and interfaces of the domain. Ensure the architecture is Department of Defense Architecture Framework (DODAF) compliant and includes, at a minimum, the following architecture descriptions/views: All Views (AV) (AV-1 and AV-2); Operational Views (OV) (OV-1, OV-4, and OV-5); System Views (SV) (SV-4 and SV-5); and Technical View (TV) (TV-1 and TV-2). Coordinate with other DOD architecture leads to ensure linkage and alignment. GIG 2.0 architecture products will be available for review by the combatant commands, Services, DOD agencies, program managers, and system developers on the DOD Architecture Repository System.

3. The Joint Staff, J-8. J-8 will:

a. Facilitate WMA IT portfolio management activities (references b and d) through the O-6 and GO/FO Integration Meetings, the JCB, and the JROC.

b. Incorporate WMA Roadmap recommendations into Chairman approved PPBE issue papers, Guidance for Development of the Force (GDF) inputs, Chairman's Program Assessments (CPA), and Chairman's Program Recommendations (CPR) (reference p), as appropriate. Provide feedback to the integrator staff when the IT portfolio recommendations are inappropriate.

c. Provide Joint Potential Designator (JPD) guidance (reference h) to WMA IT portfolio management domain owners for legacy systems not subject to the JCIDS process.

d. Provide JCIDS advice and guidance on WMA IT portfolio management Support.

3. The Joint Staff, J-7. J-7 will provide JCA guidance and updates to WMA IT portfolio management domain owners and FCBs.

4. The Joint Staff, Directorate of Management will:

a. Implement and provide technical management for JITAM.

b. Accomplish component-level IT portfolio management on Joint Staff systems per reference c.

5. The WMA IT Domain Owners. The WMA is organized into IT domains which support the JCIDS FCB structure. The IT domain is led by a Joint Staff assigned FCB lead or liaison. WMA IT domain owners will:

a. Develop a FCB approved IT investment portfolio.

- (1) Coordinate WMA assignment issues with other WMA domain owners, as applicable.
- (2) Elevate unresolved IT investment assignment issues with other mission areas to the WMA integrator for resolution.
- (3) Review mission area or domain assignment changes or additions within DITPR to determine if the change affects the domain's portfolio.
 - b. Recommend JPD assignments through the WMA IT integrator for consolidation and J-8 gatekeeper approval for WMA IT investments not processed through JCIDS.
 - c. Recommend IT investment JCA assignments to the FCB when the investment's Budget Initiative Number (BIN) (reference q) and/or Program Element (PE) (reference g) can not be determined.
 - d. Participate in developing WMA-wide portfolio management scoring criteria with the WMA IT integrator.
 - e. Develop IT domain specific scoring criteria that reflect FCB developed and prioritized capabilities identified by the combatant commands in universal joint task lists (UJTls), integrated priority lists (IPLs), and gaps (identified in purple sheets and planning input memoranda (PIM)).
 - f. Research authoritative information sources (described in Enclosure B) for IT investment information. When that information is incomplete, work with the IT investment's owning component to obtain the information. If information regarding an IT investment is different or contradictory, coordinate with the owning component to determine the correct and complete information.
 - g. Assign, score, analyze/evaluate, and select WMA IT investments via the JITAM in relation to UJTls, IPLs, PIMs, and gaps.
 - h. Coordinate with DOD components, Services, combatant commands, and FCB leads regarding IT investment recommendations.
 - i. Develop an annual FCB IT implementation plan (reference c), including IT investment recommendations (to initiate, continue, modify, or terminate) according to FCB working group's direction and priorities. Obtain FCB approval in the implementation plan.
 - j. Provide FCB IT implementation plan to the WMA IT integrator for consolidation and coordination as the WMA Roadmap. Adjudicate comments regarding their implementation plan submissions.

20 March 2009

- k. Develop PPBE recommendations resulting from IT investment analysis and selection and provide them to the FCB for consideration and forwarding to J-8, Program and Budget Analysis Division (reference p). These recommendations shall support the Chairman's input to the GDF, CRA, CPA, and CPR.
- l. Support FCB efforts to assess and evaluate capability issues and support PPBE activities through analysis, assessment, and study using JITAM.
- m. Assist FCBs in developing joint concepts from a portfolio management perspective.
- n. Support CBAs as directed by the FCB.
- o. Attend FCB working groups and FCB meetings (reference d) and provide executive summaries to the net-centric working group.
- p. In coordination with J-6, identify the domain's technical infrastructure, core enterprise services, and integration requirements.
- q. Participate in the WMA IT Domain Owner Council and appropriate net-centric Data/Services strategy related bodies and fora.
- s. Coordinate IT investment priorities with the FCB and support FCB coordination with CPM (reference j).
- t. Coordinate with other mission area sub portfolios or domains regarding IT investments of mutual interest.
- u. Provide domain specific input to GIG 2.0 architecture development.
- v. Leverage and coordinate with combatant command liaisons regarding domain portfolio management activities.
- w. Facilitate implementation of the WMA NCDS and NCSS (references m and n).
- x. In their COI governance role (reference e) to implement NCDS and NCSS, WMA IT domain owners will:
- (1) Promote net-centric data sharing and enable COIs, including adjudicating conflicts in metadata agreements and identifying authoritative sources.
 - (2) Approve/disapprove COI requests for primary domain affiliation to ensure COIs have only one primary domain affiliation.

(3) Identify information sharing problems within their domains, designate COIs to address the problems, and designate a DOD component lead for the COIs.

(4) Establish a COI governance process, including a structured mechanism for informing the Department's portfolio management processes relative to information sharing decisions. Reference c contains additional guidance.

(5) Develop domain scoring criteria to assess both NCDS and NCSS implementation and effectiveness.

(6) Resolve issues raised within the domain by primary affiliate COIs, elevate unresolved issues through the FCBs, and, if necessary, to the JCB and the JROC.

(7) Participate in appropriate net-centric NCDS and NCSS related forums.

(8) Register the domain with the Meta Data Registry (MDR). When needed, update domain point of contact on the MDR COI Directory.

(9) Ensure domain affiliated COIs register and update the COI Directory (part of the MDR).

(10) Ensure domain affiliated COIs expose and register their data and services on the MDR and affiliated/federated catalogs and registries.

6. The WMA IT Domain Owner Council. This council is chaired by the WMA integrator staff and focuses on IT support to the FCBs. Voting membership includes a representative from each FCB working group. WMA IT support team members will advise to their FCB working group participants. WMA IT Domain Owner Council advisory members include combatant command, Service portfolio managers, other DOD components, and the other DOD mission areas. The WMA IT Domain Owner Council will:

- a. Meet monthly.
- b. Provide and approve WMA IT domain requirements for JITAM.
- c. Coordinate on WMA IT integrator developed strategic objectives, policies, procedures, and scoring criteria.
- d. Provide IT investment guidance in support of the FCBs.

7. The Combatant Commands will:

a. Identify theater-wide portfolio management issues for their area of responsibility and provide a prioritized list of needed capabilities through the JCIDS process in reference h.

b. Establish a combatant command IT investment portfolio and accomplish IT portfolio management (reference b).

c. Coordinate with mission areas regarding primary and secondary mission area and domain assignment for their IT investments. Advise mission area leads when IT investment assignment conflicts arise.

d. Assist WMA IT domain owners with IT investment analysis. In particular, clarify IT priorities and capability and resource mismatches (gaps, shortfalls, and redundancies).

e. Coordinate on WMA IT domain owner portfolio management recommendations to the DOD decision support systems.

f. Ensure WMA IT domain owner recommendations to initiate, continue, modify, or terminate an IT investment are incorporated into the combatant command portfolio per reference b.

g. Participate in the WMA IT Domain Owner Council and appropriate net-centric data/services strategy related forums such as the WMA Data Sharing WG to identify common problems in IT portfolio management, data sharing processes and solutions that are in the warfighter's best interest.

h. Ensure all IT investments are registered in DITPR or the DOD SECRET Internet Protocol Router Network (SIPRNET) IT Registry per reference c and r and WMA requested information is completed for WMA primary and secondary IT investments.

i. Assume responsibility for leadership and management of assigned COIs.

(1) As needed, lead the COI, including developing appropriate management documents, such as, Plan of Action and Milestones (POAM), charter, or work plan.

(2) Appoint a primary COI point of contact.

(3) Ensure COIs are registered in the COI directory (part of the MDR), and that metadata is registered on the MDR and appropriate catalogs.

(4) Promote data sharing policies and practices and participate in component and Joint COIs.

(5) Develop scoring criteria to assess both NCDS and NCSS implementation and effectiveness.

(6) Oversee development and exposure of data and services, shared vocabularies, and associated metadata. Ensure they are registered in the appropriate catalog or registry (e.g., DOD MDR, Services Registry).

8. Services. The Services will:

a. Establish a Service IT investment portfolio and accomplish portfolio management (reference b).

b. Coordinate with mission areas regarding primary and secondary mission area and domain assignment for their IT investments. Advise mission area leads when IT investment assignment conflicts arise.

c. Identify and prioritize needed warfighting IT capabilities through the JCIDS process in reference h and UJTLs, IPLs, and gaps (identified in purple sheets and PIMs).

d. Assist WMA IT domain owners with IT investment analysis. In particular, clarify IT issues, priorities, and capability and resource mismatches (gaps, shortfalls, and redundancies).

e. Ensure WMA IT domain owner recommendations to initiate, continue, modify, or terminate an IT investment are incorporated into the Service portfolio per reference b.

f. Ensure all IT investments are registered in DITPR or the DOD SIPRNET IT Registry (references c and r) and WMA requested information is completed for WMA primary and secondary IT investments.

g. Implement NCDS and NCSS by establishing appropriate plans, programs, policies, processes, and procedures according to references e, m, and n.

h. Participate in the WMA IT Domain Owner Council and appropriate net-centric data/services strategy related fora, such as the WMA Data Sharing WG, to identify common problems in IT portfolio management and data sharing processes and provide solutions that are in the warfighter's best interest.

i. Assume responsibility for leadership and management of assigned COIs.

(1) As needed, lead the COI, including developing appropriate management documents, such as charters, POAMs, charter, work plan, and the like.

(2) Appoint a primary COI point of contact for each COI.

(3) Ensure COIs are registered in the COI Directory (part of the MDR), and that metadata is registered on the MDR and appropriate catalogs.

(4) Promote data sharing policies and practices for data sharing and participate in cross-component and Joint COIs.

(5) Develop scoring criteria to assess both NCDS and NCSS implementation and effectiveness.

(6) Oversee development and exposure of data and services, shared vocabularies, and associated metadata. Ensure they are registered in the appropriate catalog or registry (e.g., DOD MDR, Services Registry).

9. Other DOD Components. The other DOD components (reference b) will:

a. Establish a component IT investment portfolio according to reference b.

b. Coordinate with mission areas and their domains regarding IT investment primary and secondary mission area and domain assignment. Advise mission area leads when assignment conflicts arise.

c. Identify and prioritize needed warfighting IT capabilities through the JCIDS process in reference h.

d. Ensure WMA IT domain owner recommendations to initiate, continue, modify, or terminate an IT investment are incorporated into the component portfolio per reference b.

e. Ensure all IT investments are registered in DITPR or the DOD SIPRNET IT Registry (references c and r) and WMA requested information is completed for WMA primary and secondary IT investments based on a FY annual review.

f. Implement net-centric data sharing, by establishing appropriate plans, programs, policies, processes, and procedures according to reference e.

g. Participate in the WMA IT Domain Owner Council and the appropriate net-centric data/services strategy related forums such as the WMA Data Sharing WG to identify common problems in IT portfolio management and data sharing processes and provide solutions that are in the warfighter's best interest.

h. Assume responsibility for leadership and management of assigned COIs.

(1) As needed, lead the COIs, including developing appropriate management documents, such as POAM, charter, work plan, and the like.

(2) Appoint a primary point of contact for each COI.

(3) Ensure COIs are registered in the COI Directory (part of the MDR), and that metadata is registered on the MDR and appropriate catalogs.

(4) Promote data sharing policies and practices, and participate in cross-component and Joint COIs.

(5) Develop scoring criteria to assess both NCDS and NCSS implementation and effectiveness.

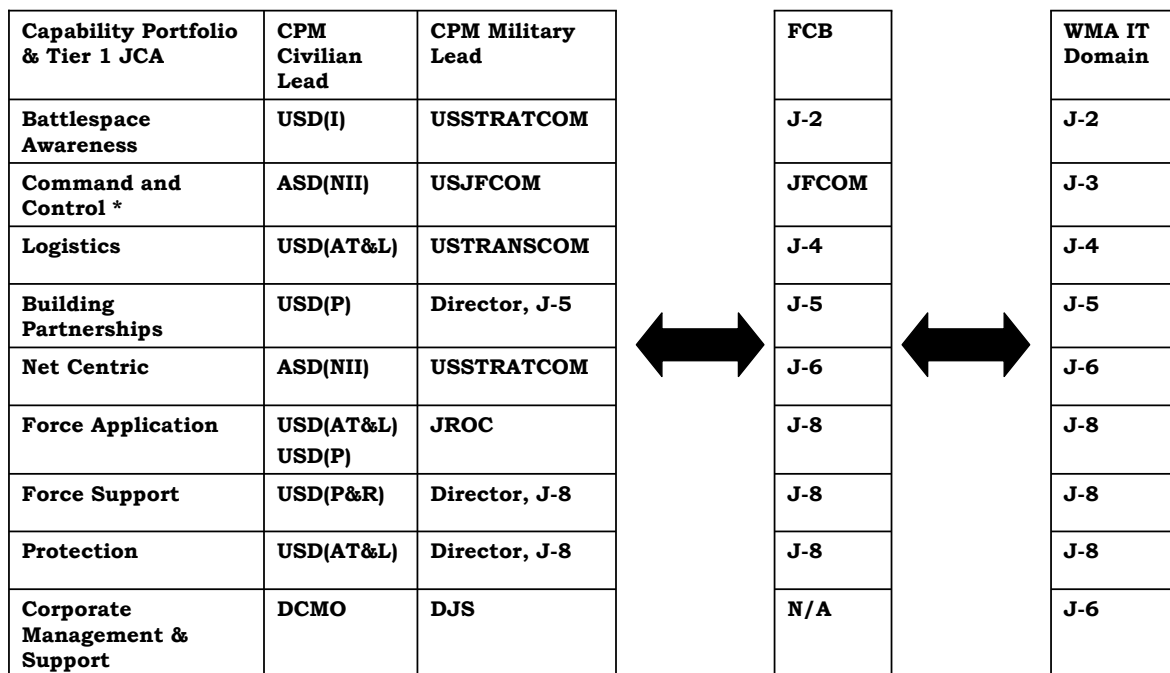
(6) Oversee development and exposure of data and services, shared vocabularies and associated metadata. Ensure they are registered on the appropriate catalog or registry (e.g., DOD MDR, Services Registry).

(INTENTIONALLY BLANK)

ENCLOSURE B

WMA IT PORTFOLIO MANAGEMENT PROCESS

1. Introduction. The WMA provides life cycle oversight to applicable DOD component IT investments, including the Joint Staff, Military Departments, Services, combatant commands, Defense agencies, and joint and combined activities IT investments (acquisition programs, systems, and initiatives) per the direction in references b, c, d, f, and g. WMA IT investments support and enhance the Chairman’s joint warfighting priorities while supporting actions to create a net-centric distributed force, capable of full spectrum dominance through decision and information superiority. WMA IT investments ensure combatant commands can meet the Chairman’s strategic priorities.



* Reference s

Figure B-1, The Relationship of IT Portfolio Management to the Functional Capability Boards and Capability Portfolio Managers

2. The IT Portfolio Management Relationship Between the FCBs and CPMs. The Department of Defense manages all capabilities (both material and non-material, including weapon systems) as portfolios to advise the Deputy Secretary of Defense and the Deputy's Advisory Working Group (DAWG) to optimize capability investments across the Defense enterprise to minimize risk in meeting DOD capability needs in support of strategy. Figure B-1 depicts a JCA based structure (reference j) that establishes DOD's common framework and lexicon to organize capability portfolios. The capability portfolios are managed by civilian and military co-leads. In coordination with the FCBs, CPMs plan, manage, and assess inputs to and outputs from their capability portfolio and make recommendations to DOD component heads and the DAWG to ensure that approved capability solutions (including legacy, planned, and programmed IT and NSS capabilities and models and simulations) are developed and implemented in a timely, coordinated, and interoperable manner. WMA IT portfolio management is aligned to the FCBs and focuses on the IT in each FCB's portfolio.

3. WMA IT Domain Scope. IT domain portfolios are focused on a specific Tier 1 JCA and its subordinate JCAs. The WMA IT domain should include IT investments in the portfolio based on the investment's capabilities, the JCAs those capabilities perform, and the FCB owning the JCA. The JCA taxonomy and lexicon (definitions) can be found at http://www.dtic.mil/futurejointwarfare/cap_areas.htm (reference t).

4. WMA IT Portfolio Management Process

a. Process Overview. Figure B-2 is the WMA IT portfolio management process overview. The process consists of IT portfolio development, criteria determination, analysis and evaluation, selection, and control as outlined in reference b. The IT portfolio management process will provide IT investment recommendations to the FCBs to inform the DOD decision support systems (JCIDS, DAS, and PPBE) process leadership.

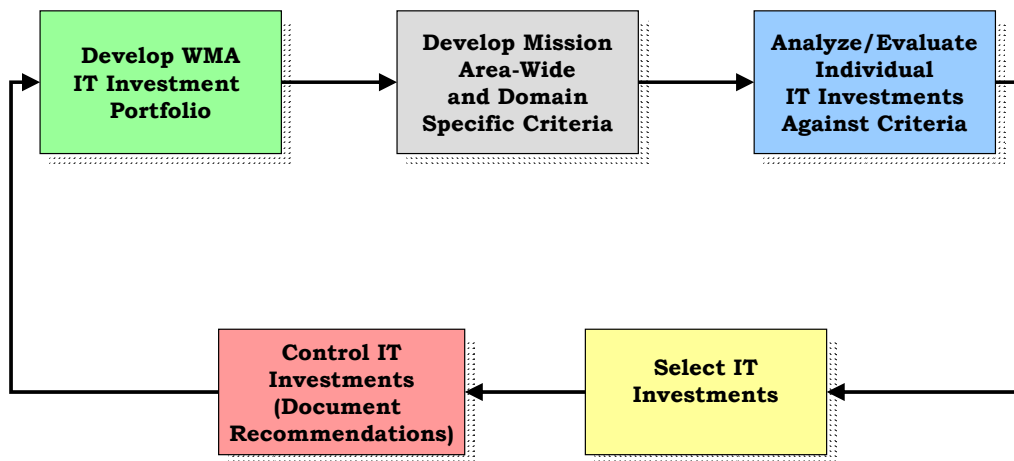


Figure B-2. The WMA IT Portfolio Management Process

b. WMA IT Portfolio Management Process Description. A general process and activities description follows:

(1) Develop WMA IT Investment Portfolio. Choose WMA IT investments from authoritative information sources. Determine which IT domain will manage the portfolio's investments.

(2) Develop mission area-wide and IT domain-specific criteria. WMA-wide and domain-specific scoring criteria are needed to evaluate an IT portfolio's and individual investment's risk, health, value, and alignment to strategic direction.

(3) Analyze/Evaluate Investments Against Criteria. Assess and prioritize IT investments against WMA scoring criteria. Link portfolio objectives to enterprise mission, vision, goals, objectives, and priorities; identify capability gaps, opportunities, and redundancies; identify risks; and provide for continuous process improvement. Evaluate actual IT investment contributions against established scoring criteria to enable improved capability as well as to support adjustments to the IT investment mix.

(4) Select IT Investments. Determine each WMA IT domain's optimum investment baseline and identify investment baseline changes, including capability identification, acquisition, and funding issues. Identify and select the best IT investment mix (acquisition programs, systems, and initiatives) to strengthen and achieve portfolio capability goals and objectives and demonstrate alternative IT investment strategies and funding level impacts.

(5) Control IT Investments (Recommendations). Document WMA IT investment recommendations (initiate, continue, modify, or terminate) in a FCB

IT implementation plan. Consolidate FCB implementation plans into a WMA Roadmap. Coordinate the WMA Roadmap with Joint, Service, and DOD leadership and note stake holder impact statements. Provide coordinated WMA Roadmap to DOD decision support system decision makers to provide prioritization and integration recommendations on WMA IT investments. Controlling, through the WMA Roadmap, ensures a portfolio is managed and monitored using established quantifiable scoring criteria and architectural goals to monitor and evaluate portfolios.

5. Develop the WMA IT Investment Portfolio. Figure B-3 illustrates the WMA IT investment portfolio development process.

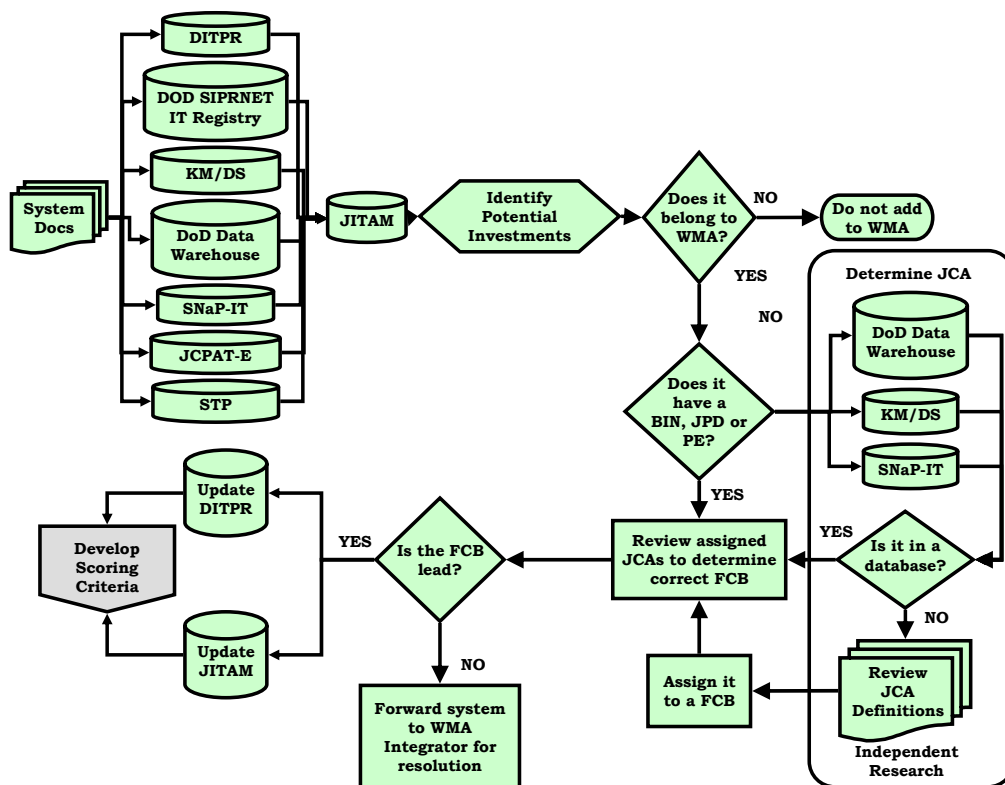


Figure B-3. Develop the WMA IT Investment Portfolio

a. Identify Potential WMA IT Investments in Authoritative Data Bases.

WMA will use the authoritative DOD repositories listed below to data mine and choose recommended WMA portfolio IT investments for the portfolio. The authoritative data sources include:

- (1) DITPR. The DOD CIO developed DITPR as the DOD's official, unclassified portfolio management data source (references c and r). All unclassified WMA IT and NSS investments to include unclassified component

20 March 2009

IT investments will be registered in DITPR according to reference r. DITPR data extracts are imported into JITAM to support portfolio development.

(2) The DOD SIPRNET IT Registry. The registry is maintained by DOD CIO on the classified network and implements title 40 direction to register all IT (references a and r).

(3) Knowledge Management and Decision Support (KM/DS). The JROC's KM/DS is used by the JCIDS gatekeeper to record JCIDS documents and decisions, including the JPD (reference h). It provides users with an electronic repository of guidance, issues, and results to facilitate decision-making in the JROC process and enables users to submit documents and briefings, research topics, and request JROC/JCB fora for associated topics online, using Web interface.

(4) DOD Data Warehouse. The Office of the Secretary of Defense, Director of Program, Analysis and Evaluation (OSD(D,PA&E's)) DOD Data Warehouse contains 5-year Defense program and other programming and budgeting data collected by OSD(D,PA&E) as part of the PPBE process, to include integrated and embedded platform IT. To facilitate research, the DOD Data Warehouse is organized into data centers.

(5) Select and Native Programming Data Input System - Information Technology (SNaP-IT). SNaP-IT contains DOD IT financial information and generates reports mandated by the Office of Management and Budget and Congress for the DOD IT budget (reference q). It was developed and maintained by OSD(D,PA&E) as a web-based application used to collect non-standard program and budget data requirements and is a DOD Data Warehouse feeder system.

(6) Joint C4I Program Assessment Tool-Empowered (JCPAT-E). JCPAT-E is an online tool and application suite used to assist OSD and the Joint Staff in accepting, staffing, reviewing, and evaluating Information Support Plans. Developed, maintained, and operated by the Defense Information Systems Agency (DISA), JCPAT-E provides the necessary electronic document distribution, comment collection and rollup, document storage, and management support necessary to evaluate draft documents. JCPAT-E is accessed on the classified network via <https://jcpat.disa.smil.mil>. It is accessed on the unclassified network via <https://jcpat.disa.mil>. JCPAT-E is also used to document IT investment interoperability certification information (reference u).

(7) System Tracking Program (STP). STP is the Joint Interoperability Test Command's web database to track a system's progress toward joint or combined interoperability certification. The STP tracks complete NSS IT life

20 March 2009

cycle requirements document validation, testing, and culminates with certification status. It is located at <http://stp.fhu.disa.smil.mil/> (reference v).

b. NSS and Coalition/Other Agency IT. Determine whether the IT investment is an NSS (reference v) integral to a weapon or weapons system, involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, is critical to the direct fulfillment of a military or intelligence mission or performs an FCB identified needed capability. These NSS should be included in the domain owner's portfolio. NSS integral to a weapon or weapons systems may be:

(1) Integrated IT capability that is a separate program of record, provided by another program manager for weapon or weapon system integration. Include these as separate, individual IT investments (reference u).

(2) Integral weapon system IT which connects to the GIG as described in references r and u. Weapon system IT meeting referenced criteria will be included in DITPR and in the WMA IT domain owner's portfolio. Weapon system IT that does not have a platform interconnection does not need to be included in the domain portfolio; however, it may be included for future consideration.

(3) Finally, IT investments sponsored by other federal departments and coalition/allies should be reviewed if they are used by the joint warfighter (reference c). A WMA IT domain owner will be assigned as the sponsor for those investments to ensure WMA equities are represented with those systems' sponsors and that they are addressed within the WMA IT portfolio management process.

c. Choose IT Investments For WMA Portfolio and Assign WMA IT Domain(s). To choose IT investments for their portfolio, the domain owner portfolio manager will review a candidate WMA IT investment's description in the authoritative databases to determine whether it is a warfighting investment. They will also considering the following:

(1) Per reference j, JCAs are the foundation for DOD capability management. JCAs are an integral part of capabilities planning intended to provide a common language across related DOD activities and processes. They are a collection of similar capabilities grouped at a high level in order to support decision-making, capability delegation, and analysis. Tier 1 JCAs are decomposed by logically breaking them down to their sub components. This further scopes, bounds, and clarifies JCAs by providing greater granularity and facilitates detailed analysis. Decomposition of JCAs continues until a group of distinct joint capabilities is reached. The number of levels required to decompose a top-level JCA down to its component capabilities is not a constant

across the JCAs. WMA uses JCAs to align IT investments to a WMA IT domain/FCB.

(2) The DAWG directed the D,PA&E to assign a tier 1 JCA to every DOD PE. For IT investments, DOD CIO assigns the tier 1 JCA to IT BINs. When WMA identifies a new IT investment, its BIN(s) and/or PE(s) are reviewed to determine which JCA(s) was assigned by D,PA&E and/or DOD CIO. The investment is managed by the FCB associated with the JCA. If WMA is unable to determine the IT investment's BIN and/or PE, the domain will search KM/DS to determine if the system was reviewed via the JCIDS process and whether a lead FCB and/or supporting FCBs were assigned. If an FCB(s) was assigned, it provides the linkage to a tier 1 JCA. If an FCB does not concur with the BIN and/or PE to JCA assignment, they will provide the disagreement with rationale and a recommended reassignment to the associated CPM for concurrence and forwarding to DOD CIO or PA&E for approval.

(3) If a BIN and/or PE is not available and no FCB was assigned, the domain will review the IT investment according to the JCA definitions to determine the appropriate IT domain and JCA assignment. JCA descriptions (reference t) can be found at <http://www.dtic.mil/futurejointwarfare/strategic/lexicon.doc>.

d. Coordinate and Approve Portfolio. WMA IT investment domain assignments are coordinated among other WMA and mission area domains, as appropriate, and approved by the FCB.

(1) Multiple mission areas and/or WMA IT domains may want an IT investment in their portfolio. IT investments will belong to only one primary mission area and domain in DITPR, the DOD SIPRNET IT Registry, and JITAM. IT investments may belong to multiple secondary mission areas and/or domains. Secondary mission areas may also conduct portfolio management activities on secondary IT investments (reference c). Recommended results for secondary IT investments will be included in the FCB implementation plan and coordinated as part of the WMA Roadmap.

(2) Within WMA, the IT domain owners coordinate among each other regarding IT investment primary management. If amplifying information is needed to make a decision regarding primary and secondary mission area and domain assignment, the domain will contact the investment's owning component and request the information. In addition, the domain will research authoritative data bases discussed above for supporting information to determine portfolio assignment. Once primary and secondary domain ownership agreement is reached, the WMA domains will be updated in DITPR or the DOD SIPRNET IT Registry and JITAM.

(3) If primary WMA domain assignment cannot be decided, the conflict with rationale from each domain is forwarded to the WMA IT integrator for resolution. Once a decision is reached, DITPR and JITAM will be updated. As discussed above, the first consideration for IT investment assignment is the Tier 1 JCA assigned to the investment's BIN and/or PE. If the BIN and/or PE JCA assignment information isn't available, IT investments processed through JCIDS with an assigned lead and support FCB (reference d) will be managed as indicated by the JCIDS process. Domain owners may work through their FCB to modify the lead and support FCBs; however, changes will not be made in DITPR or JITAM until the decision is made and approved by the Joint Staff/J-8 gatekeeper. DITPR and JITAM will reflect the JCIDS lead and support domains as identified in KM/DS.

(4) As discussed in reference c, domain owners may determine an IT investment that is primarily managed by other mission areas should be managed by WMA and their domain or they may determine the investment should be moved out of their WMA domain to other mission areas. The IT investment with rationale for changes is sent to the WMA IT integrator for coordination with the other mission area's integrator staff. DITPR and JITAM are updated when mission area consensus is reached.

(5) When the mission areas are unable to reach consensus, the issue will be raised to the DOD IT portfolio management lead (DOD CIO) for adjudication by the DOD CIO EGB.

(6) Using the process above, it may be determined other WMA domain(s) have secondary interest in the system. Secondary domain(s) assignment is coordinated between the primary and secondary domain(s) and DITPR and JITAM are updated. If an unresolved disagreement occurs regarding secondary domains, the disagreement is forwarded to the WMA integrator for adjudication.

(7) The FCB working group will review and approve IT investment domain portfolio contents. This will include the IT investments to be delegated back to the owning component for portfolio management per reference c. Portfolio development and revision is a continuous process to account for new IT investments identified in DITPR, the DOD SIPRNET IT Registry, KM/DS, or the other authoritative databases.

6. Develop Standardized Mission Area-wide and Domain-Specific Criteria. Standardized, clearly defined WMA IT domain scoring criteria development leads to a common basis for IT investment analysis/evaluation. Clear, standardized criteria contribute to the best IT investment selection for the warfighter and in support of DOD and joint strategic direction. WMA prioritized criteria are based on Joint Strategic Plans, Unified/Specified Command priorities, most pressing military issues (MPMI) and military utility

(e.g., warfighting capability enhancement, readiness, sustainability, and national security threat reduction). Figure B-4 illustrates the criteria development process. The WMA IT integrator will coordinate and consolidate the common WMA IT portfolio criteria with the domains to enable an objective portfolio analysis. WMA IT domain specific criteria will be developed, integrated, and approved by the domain's associated FCB.

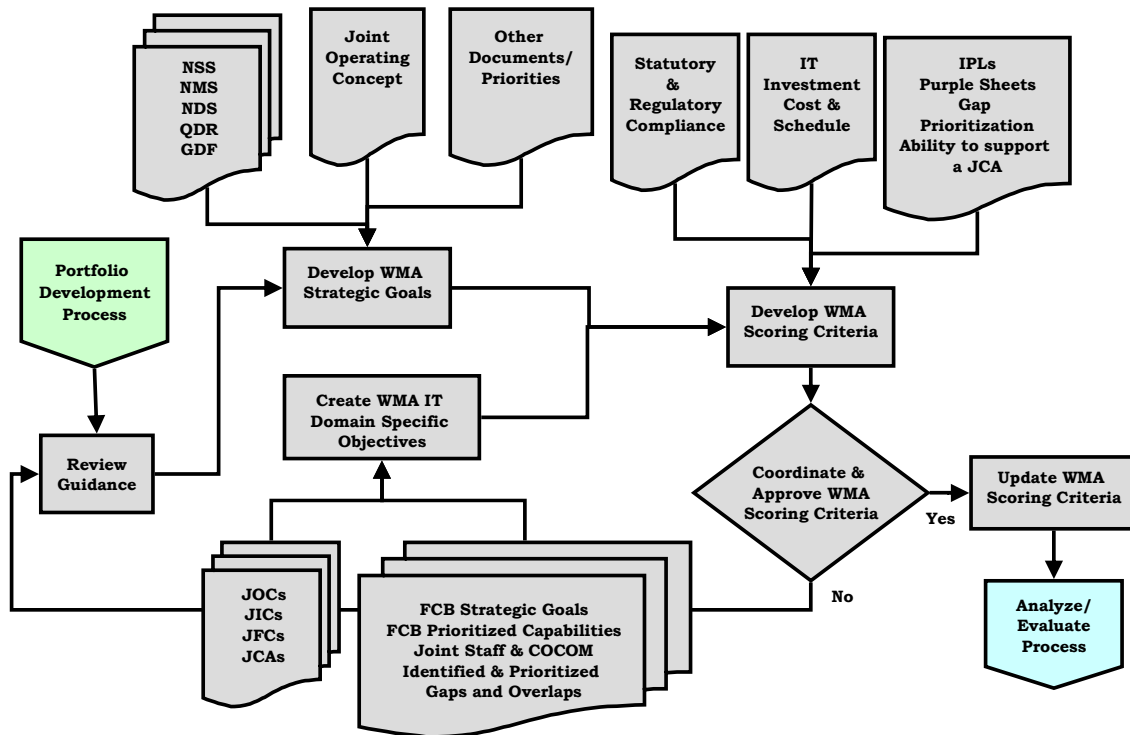


Figure B-4. Develop Mission Area-wide and Domain Specific Criteria

a. Develop WMA Strategic Goals. The WMA IT integrator will review the National Security Strategy, National Military Strategy, National Defense Strategy, the Quadrennial Defense Review, National Strategic Planning System, JROC approved MPMIs, and DOD component IT strategic plans to develop a vision, mission statement, and strategic WMA IT portfolio goals. The strategic goals will be common across the WMA IT domains and scoring criteria will support these strategic goals. The WMA IT portfolio vision, mission, and goals are specifically focused on the joint warfighting environment. WMA IT investment portfolio governance and management will be integrated with DOD decision support systems through the FCBs and effectively and rapidly facilitate warfighting capabilities that enable information and decision superiority and full spectrum dominance in the operations space and provide

capability that is fully secure, joint, multinational, and interagency interoperable.

b. Create IT Domain Portfolio Objectives. The WMA IT portfolio strategic goals are the baseline to develop WMA IT domain portfolio management objectives. WMA IT domain owners will develop specific objectives to select the best IT investment mix in support of the warfighter's mission capability needs. The objectives should also implement DOD CIO direction to increase and report the use of commercial software and services and DOD strategic direction (reference w). The WMA domain portfolio objectives will annually be reviewed and updated according to strategic document updates. The objectives should synchronize with the JCIDs process and FCB input. They should also enable portfolio management using GIG architecture, plans, risk management techniques, capability goals, and objectives.

c. Establish WMA and IT Domain Scoring Criteria. WMA scoring criteria will address alignment to strategic objectives; combatant command identified operational priorities identified in IPL; IT investment risk, health, and value; and implementation of the NCDS and NCSS. Alignment scoring criteria result from WMA strategic goal development and IT domain portfolio objectives discussed above. Risk scoring criteria are based on IT investment compliance with statutory and regulatory direction (e.g., security certification and accreditation (references x, y, and z), interoperability and supportability certification (references f and u), mission criticality, and acquisition category (reference z), whether the IT investment includes embedded training in a net-centric environment (reference aa), and, as applicable, operational requirements and their associated objective and threshold values and/or exit criteria. Health scoring criteria are based on IT investment's budget and schedule status (including modernization status). Value scoring criteria are based on the investment's ability to support a JCA and combatant commander priorities (e.g., IPLs, PIMs, gap prioritization results, and warfighter lessons learned). As directed by the FCB, scoring criteria may also include CPM metrics and capability development increments. The WMA IT integrator will collaborate with the IT domains to identify standard scoring criteria for approval by the FCB. The scoring criteria will be coordinated among the FCBs and approved by the Joint Community Warfighter CIO (reference l). All WMA IT investments will be analyzed using these standard criteria. WMA IT domain owners may also develop specific criteria to reflect domains specific objectives. WMA scoring criteria are annually updated.

7. Analyze/Evaluate IT Investments. IT investment analysis and evaluation is accomplished on the approved domain portfolio using the scoring criteria discussed above, the FCB capabilities analysis directed in references h and bb, and information research in authoritative and other data repositories. Figure B-5 illustrates the investment analysis process.

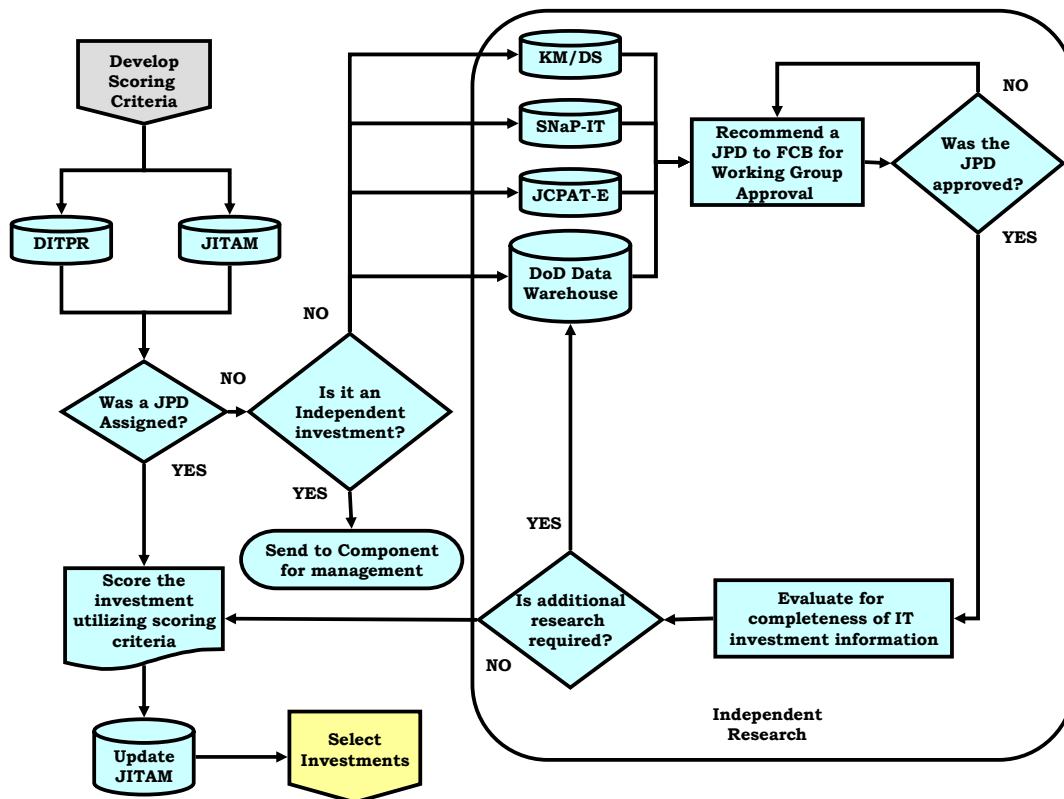


Figure B-5. Analyzing/Evaluating WMA IT Investments

a. Determine IT Investments to Score. Review the IT investment in DITPR to determine whether a JPD was assigned (reference h). The Joint Staff/J-8 gatekeeper assigns JPDs when programs and systems enter the JCIDS process and documents them in KM/DS to specify JCIDS validation, approval, and interoperability expectations. All IT investments with a JROC Interest, JCB Interest, Joint Integration, or Joint Information JPD should be portfolio managed and scored by the assigned WMA IT domain(s). If the JPD is not available in DITPR, research KM/DS for IT investment JPD information in JCIDS documents available for the IT investment.

b. Recommend a JPD. If the IT investment did not come through the JCIDS process and no JPD is assigned, the FCB IT domain will review all available information on the IT investment and recommend a JPD assignment in DITPR for FCB working group approval.

c. Independent IT Investments. Management of independent IT investments may be delegated to the owning component for their IT portfolio management activities (reference c). The WMA IT domain owner will consider delegated IT investments when necessary, for example when analyzing capability gaps. JPDs specify JCIDS validation, approval, and interoperability requirements.

d. Evaluate IT Investment Information for Completeness. In preparation for scoring the portfolio's IT investments, the FCB domain will review the IT investment's information in JITAM for completeness. If information is missing, the domain will research the authoritative databases discussed above to complete the information needed for scoring the investment.

e. Score the IT Investment. IT investment analysis results will enable IT investment selection and recommendations and will be included in the FCB's IT implementation plan. To analyze the IT investments, the domain owner will:

(1) Research available CBA (reference h) results to support IT investment scoring.

(2) Score each IT investment in the portfolio using JITAM. The resulting scores will indicate each IT investment's health, value, risk, and alignment to capability requirements and enable the domain to determine if their IT investment portfolio provides capabilities required to meet joint warfighting requirements and/or where capability gaps and overlaps exist. The IT domain owner's goal is to enable the best possible mission success through mission-oriented investment analysis to maximize return on investments while minimizing portfolio risk.

(3) Provide IT investment analysis results to the FCB to update their CBA results.

8. Select IT Investments. IT investment selection will result in the domain owner's prioritized IT investment portfolio and recommendations to initiate, continue, modify, or terminate an IT investment. Figure B-6 illustrates the select IT investment process.

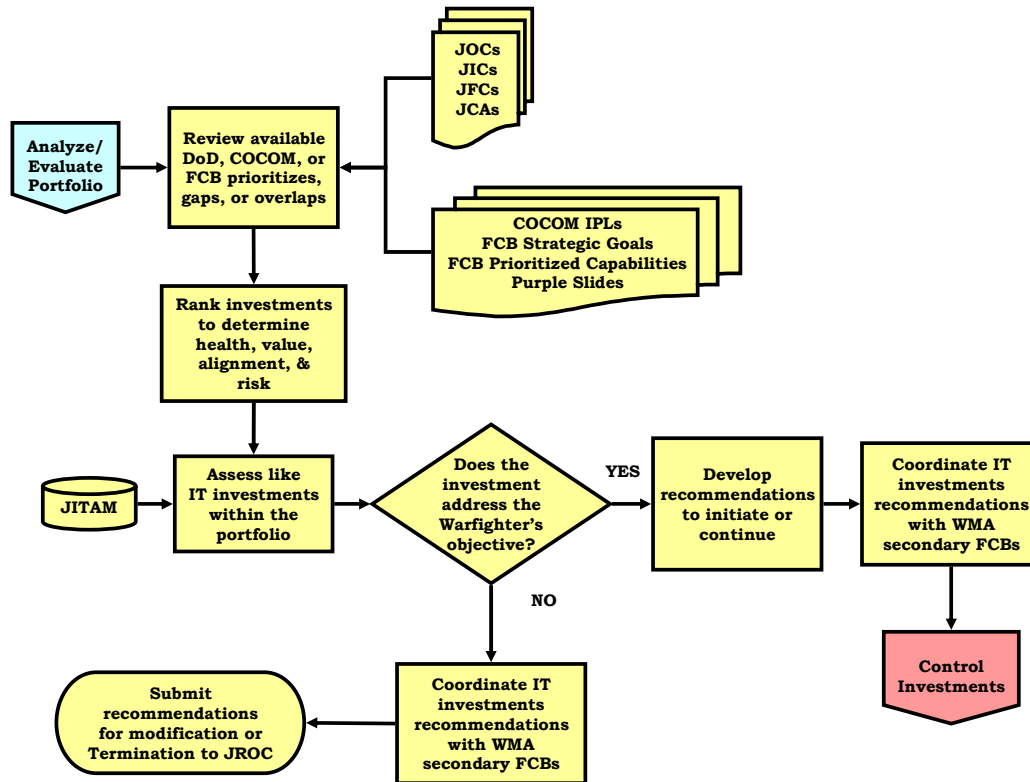


Figure B-6. Selecting WMA IT Investments

a. Apply Scoring Results. WMA IT domain owners will analyze JITAM results to determine how well (health, value, alignment, and risk) each IT investment meets the domain's warfighting objectives, to identify IT investment capability gaps and overlaps, and to prioritize and select IT investments. JITAM investor maps provide a multi-axis, pictorial view of scored IT investment health, value, alignment, and risks information. Using analysis results and considering DOD and joint strategic direction regarding joint warfighting and combatant command priorities, the domain owner will prioritize and select IT investments through recommendations to initiate, continue, modify, or terminate them.

b. Coordinate and De-conflict IT Investment Recommendations. If an IT investment is assigned to secondary domains or mission areas, the primary WMA IT domain owner will coordinate the recommended IT investment changes with the secondary mission area and domain owners. The primary WMA IT domain owner must make significant effort to gain consensus on the recommended change. When consensus cannot be reached, the WMA IT domain owner will develop a recommended best course of action, noting dissenting comments, and forward their recommendation through the FCB adjudication process (reference h and bb) for resolution. The WMA IT domain owners should collaborate with the FCBs and the affected combatant

command(s), Service(s), and other DOD mission area(s), and other interested parties (e.g., program offices and budget analysts) on all IT investment recommendations as they develop the FCB implementation plan.

9. Control IT Investments (Recommendations). WMA implements IT investment control through FCB IT implementation plans and WMA Roadmap development. The implementation plans and WMA Roadmap provide inputs to the JCIDS, DAS, and PPBE processes and to Service and combatant commands for consideration in Program Objective Memorandum (POM) development. Figure B-7 illustrates the FCB implementation and WMA Roadmap development and coordination process.

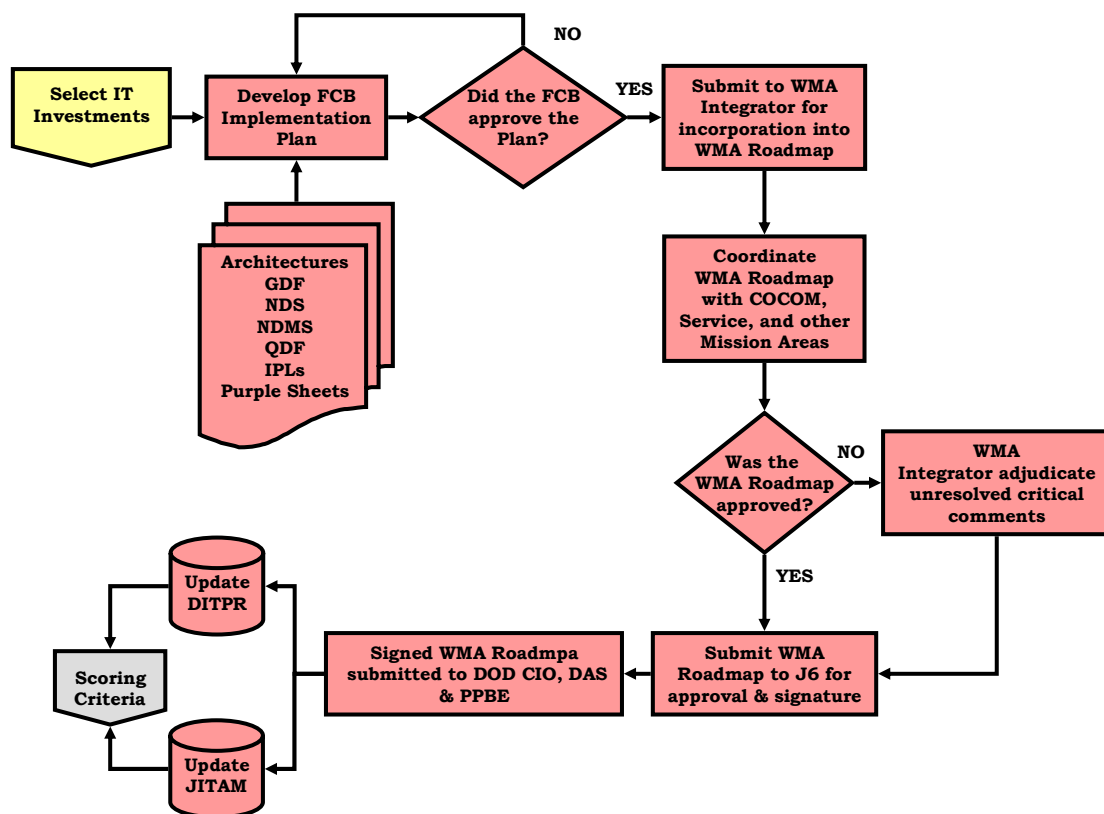


Figure B-7, Controlling WMA IT Investments

a. Develop FCB IT Implementation Plan. The WMA IT domain implementation plan is a roadmap to guide WMA IT capability implementation and shall be based on IT portfolio management processes and applicable enterprise warfighter architectures. FCB IT implementation plans will be consolidated into a WMA Roadmap.

(1) The FCB IT implementation plans and the WMA Roadmap will include:

(a) Domain IT investment priorities developed from DOD and joint strategic and concept guidance. Sources should be included.

(b) Known warfighter and developing GIG 2.0 enterprise architecture information contained in the operational activity models (OV-5), systems/services functionality descriptions (SV-4), and operational activity to systems/services functionality descriptions (SV-5), at a minimum, that are applicable to the domain. Additionally, include known “new start” architecture and architecture required for Joint Interoperability Test Command tested systems. Additional architecture views will be added as they are developed.

(c) Identified GIG infrastructure support requirements (e.g., communications).

(d) Interdependencies with other mission areas and WMA domains.

(e) Summarized IT investment implementation plan recommendations (initiate, continue, modify, and terminate).

(f) IT investments identified by the domain and approved by the FCB as their baseline portfolio. Include the following information and JITAM scoring results for each IT investment in the portfolio:

1. IT investment name and acronym.
2. DITPR identification number.
3. IT investment budget information to include the SNaP-IT BIN, PEs, and POM information.
4. JROC memorandum number associated with the IT investment applicable to the IT investment recommendations.
5. Statutory or regulatory direction regarding the IT investment applicable to the IT investment recommendations.
6. Assigned JPDs and JCAs.
7. System description.
8. IT investment schedule.

9. Gap and overlap information regarding the IT investment in relation to the domain's objectives.

10. Combatant command, Service, other mission area, and WMA domain comments from coordination (highlighting unresolved disagreements).

b. Coordinate IT Investment Recommendation with Secondary FCBs. When other FCBs have secondary portfolio management responsibilities for a system, the primary FCB should coordinate their recommendations with the secondary. If any unresolved disagreement occurs, it will be included in the FCB implementation plan and provided to the FCB lead for review and a decision.

c. Obtain FCB Approval. The FCB will approve the IT implementation plan for forwarding to the WMA integrator for consolidation and formal staffing.

d. Consolidated WMA Roadmap. The WMA IT integrator will consolidate the approved FCB IT implementation plans into the WMA Roadmap. The WMA Roadmap will be considered for issue paper, GDF, CPR, and CPA development and to guide IT investment decisions in DOD decision support system processes (reference b). The WMA Roadmap will include:

(1) An executive summary with overarching recommendations and lessons learned.

(2) An appendix for each FCB IT implementation plan.

(3) A glossary.

e. Coordinating the WMA Roadmap. The WMA IT integrator staff will coordinate the WMA Roadmap with the FCBs and other stakeholders (combatant commands, Services, other DOD mission areas, CPMs, and other interested organizations). WMA IT domains will coordinate with stakeholders and adjudicate comments on their individual implementation plans and the integrator will adjudicate comments on the executive summary and glossary. Unresolved critical stakeholder comments will be identified in the executive summary and the WMA Roadmap will be provided to J-6 for final approval and forwarding to DOD CIO per reference c.

f. Provide Inputs to Services, Combatant Commands, and Other DOD Components. Provide IT investment recommendations to the Services, combatant commands, and other DOD agencies for their consideration during their POM build, program management document development, and IPL/UJTL development and for consideration by defense acquisition system program managers.

g. Provide Inputs to JCIDS, DAS, and PPBE. IT Investment recommendations support FCBs in their JCIDS activities, including CBAs. The resulting gap and overlap information and recommendations to initiate, continue, modify, or terminate IT investments is provided to the FCB lead and J-8 Program Budget Analysis Division for inclusion in PPBE issue paper recommendations and GDF and CPA/CPR recommendations. The resulting information will also be provided to acquisition program managers and OSD D,PA&E for consideration during analysis of alternative evaluation. It is also provided as an input to Acquisition Program Baselines and Acquisition Decision Memorandum, and for program milestone reviews.

h. Update Plans. The FCB IT implementation plans and WMA Roadmap will be annually updated and provided to DOD CIO by 30 June each year

10. Informing the JCIDS Process. Figure B-8 depicts points where WMA IT portfolio management provides information to support the JCIDS process. FCBs should review WMA IT portfolio management analysis, evaluation, selection, and control results as they review and comment on JCIDS documentation and as CBAs and analyses of alternative are prepared.

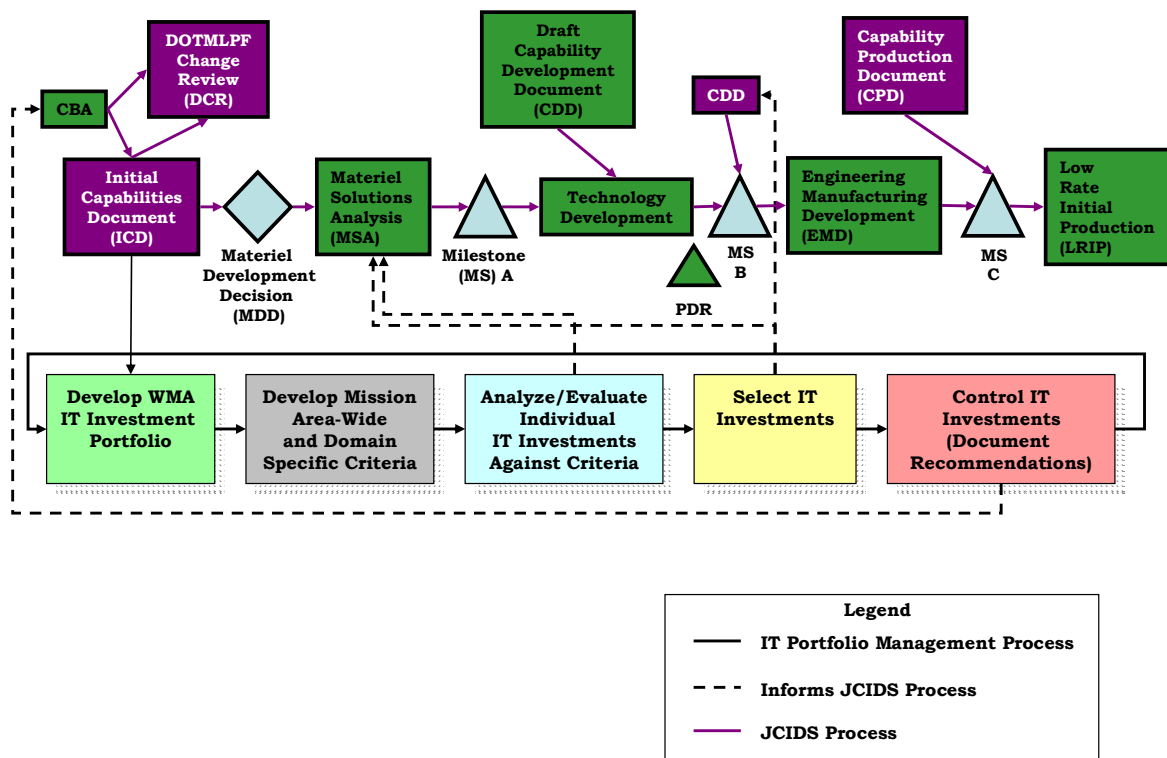


Figure B-8, How IT Portfolio Management Can Inform the JCIDS Process

11. WMA IT Portfolio Management of Defense Business Systems (DBS). Reference cc stipulates DBS modernization in excess of \$1,000,000 must be certified by the cognizant Investment Review Board (IRB) and the Defense Business System Management Committee, as complying with the DOD Enterprise Architecture, as is articulated in the Business Enterprise Architecture. DBS of interest to WMA FCBs will be included and managed as described above and the resulting IT portfolio management recommendations will be shared by the FCB IT support with the appropriate IRB for their consideration.

ENCLOSURE C

WMA NC DATA SHARING PROCESS

1. Overview. The Department of Defense is transforming to a net-enabled information-sharing environment where authorized users or applications can seamlessly share information. In this environment, people, processes, and technology work together to facilitate timely and trusted information access and sharing. Making information accessible enables decision makers at all levels to make better decisions faster resulting in improved operational effectiveness.

a. COIs defined in reference m identify and address information sharing problems. COIs may include representatives from combatant commands, Services, and agencies; program and system sponsors; or any other organizational entities with shared goals, interests, missions, or business processes. COI members actively share information and cooperate to accomplish a specific information-sharing mission or task. Due to the potential for authorized but unanticipated users, COIs strive to make their data visible, accessible, and understandable to those inside and outside their community. Reference e directs the use of COIs and references m and n contain additional guidance.

b. Participating in COIs is one way that programs and systems can comply with the NCDS and NCSS. Compliance will be verified through interoperability and supportability certifications as described in reference u.

c. Viability of COIs is dependent on the availability of funding. COI resourcing comes from the members and must be a consideration as they form.

d. Detailed instructions for implementing net-centric data sharing are available at reference dd.

2. COI Activities. COIs focus on making information visible, accessible, understandable, and trustable (reference e).

3. Enabling COIs. WMA-affiliated COIs will be enabled by the appropriate WMA IT domain owner/FCB.

a. Primary Domain Affiliation. A COI may be associated with multiple domains (inside or outside of the WMA) but can have only one primary domain affiliation. The affiliation becomes the COI governance channel.

(1) COIs request primary domain affiliation when they register in the COI Directory accessible through the MDR home page reference ee. WMA IT domain owners will periodically review the DOD COI Directory and communicate with the COI leads to confirm or change requested primary domain affiliation. WMA IT domain owners approve COI requests for primary domain affiliation through direct COI lead contact.

(2) COIs seeking primary domain affiliation will provide a copy of their mission statement, charter, POAM, or other information, as requested by the WMA IT domain owner, for review and consideration. COIs are not affiliated until approved by the primary domain owner.

b. Oversight of COIs. WMA IT domain owners will resolve issues that are raised by COIs that have a primary affiliation with their domain. Unresolved issues will be brought to the WMA Data Sharing WG (description below) for resolution. If this fails, issues may be elevated to the FCBs and, if needed, to the JCB and JROC.

c. Information Sharing Problems. WMA IT domain owners will respond to information sharing problems identified within their domains by proposing COIs and lead organizations to satisfy the need.

4. Governance and Management

a. COI Governance. COI governance is externally focused; involving such things as COI domain affiliation, issue resolution, boundaries.

b. COI Management. COI management is internally focused; e.g., day-to-day operations, sponsorship, resourcing, development/management of shared vocabularies, interfaces with enterprise services, and coordination within its community, other COIs, and DOD components.

5. COI Resourcing. Reference e directs the DOD component heads to ensure implementation of net-centric data sharing and establish supporting plans, programs, policies, processes, and procedures. The programs and organizations that participate in COIs are responsible for resourcing them.

6. WMA Data Sharing Working Group (WMA DSWG)

a. Working Group Description. The WMA DSWG is a flexible advisory group that promotes interaction among COIs, mission areas, domains, DOD components, and other mission partners. The WMA DSWG assists the Chairman's WMA Lead and IT integrator by facilitating resolution of data sharing issues at the lowest level possible. The WMA DSWG supports WMA

NCDS implementation by providing recommendations to WMA IT domain owners.

b. Oversight of COIs. WMA IT domain owners will resolve issues involving COIs having primary affiliation with their domain.

c. WMA DSWG includes (* Indicates voting members):

- (1) Joint Staff/J6 – Chair.*
- (2) WMA IT domains.*
- (3) Combatant commands.
- (4) Services.*
- (5) Others, such as:
 - (a) Defense agencies.
 - (b) DOD field activities.
 - (c) ASD(NII)/DOD CIO.
 - (d) Mission partners (e.g., Department of Homeland Security).

d. WMA DSWG activities include:

(1) Assist WMA IT domain owners in identifying data sharing problems within their domains, proposing COIs to address the problems, and proposing a DOD component lead for each COI.

(2) Assist WMA IT domain owners in developing domain specific scoring criteria to assess both data sharing implementation and effectiveness.

(3) At the request of a domain owner, coordinate resolution of cross-domain data sharing issues with other mission areas, DOD components, mission partners, ASD(NII)/DOD CIO, etc.

(INTENTIONALLY BLANK)

ENCLOSURE D

REFERENCES

- a. Title 40 United States Code (USC), Subtitle III, Chapter 113, Subchapter 1, Section 11302
- b. DOD Directive 8115.01, 10 October 2005, "Information Technology Portfolio Management"
- c. DOD Instruction 8115.02, 30 October 2006, "Information Technology Portfolio Management Implementation"
- d. CJCSI 3137.01 Series, "The Functional Capabilities Board Process"
- e. DOD Directive 8320.2, 2 December 2004 (certified current as of 23 April 2007), "Data Sharing in a Net-Centric Department of Defense"
- f. DOD Directive 5000.01, 12 May 2003 (certified current as of 24 November 2003), "The Defense Acquisition System"
- g. DOD Directive 7045.14, 28 July 1990, "The Planning, Programming, and Budgeting System (PPBS)"
- h. CJCS Instruction 3170.01 Series, "Joint Capabilities Integration and Development System"
- i. Chairman of the Joint Chiefs of Staff Guidance to the Joint Staff
- j. DOD Directive 7045.20, 25 September 2008, "Capability Portfolio Management"
- k. E-Government Act of 2002 (Public Law 107-347), 17 December 2002
- l. CJCSI 8010.01 Series, "Joint Community Chief Information Officer"
- m. DOD CIO Memorandum, 9 May 2003, "DOD Net-Centric Data Strategy" (<http://www.defenselink.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf>)
- n. DOD Chief Information Officer, 4 May 2007, "DOD Net-centric Services Strategy"

- o. Joint Staff Instruction 8000.01C, 2 November 2007, “Joint Staff Chief Information Officer”
- p. CJCSI 8501.01A, 3 December 2004, “Chairman of the Joint Chiefs of Staff, Combatant Commanders, and Joint Staff Participation in the Planning, Programming, Budgeting, and Execution System”
- q. DOD Financial Management Regulation, Volume 2B, Chapter 18, June 2006
- r. “DOD Deputy CIO Memorandum, Department of Defense (DOD) Information Technology (IT) Portfolio Repository (DITPR) and DOD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007-2008”, 6 September 2008
- s. CJCSI 3265.01, 22 September 2008, “Command and Control Governance and Management”
- t. Joint Capability Area Lexicon (http://www.dtic.mil/futurejointwarfare/strategic/jca_lexicon.doc)
- u. CJCSI 6212.01 Series, “Interoperability and Supportability of Information Technology and National Security Systems”
- v. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, August 2003, “Guideline for Identifying an Information System as a National Security System”
- w. DOD Information Management and Information Technology Strategic Plan 2008-2009
- x. Federal Information Security Management Act of 2002 (FISMA)
- y. DOD Directive 8500.01E, 24 October 2002 (certified current as of 23 April 2007), “Information Assurance (IA)”
- z. DOD Instruction 5000.2, 12 May 2003, “Operation of the Defense Acquisition System”
- aa. DoD Directive 1322.18, 13 January 2009, “Military Training”
- bb. Joint Requirements Oversight Council Admin Guide (http://www.interlink.sgov.gov/wiki/Joint_Requirements_Oversight_Council.Admin_Guide)

cc. Section 2222, title 10 U.S.C

dd. DOD 8320.02-G, 12 April 2006, "Guidance for Implementing Net-Centric Data Sharing"

ee. NCEC TechGuide (http://metadata.dod.mil/mdr/ns/ces/techguide/main_page.html)

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ACRONYMS

ASD(NII)/DOD CIO AV	Assistant Secretary Of Defense (Networks And Information Integration)/Department Of Defense Chief Information Officer All View
BA BIN	Battlespace Awareness Budget Initiative Number
CBA CIO CJCS COI CPA CPM CPR CRA	Capabilities Based Assessment Chief Information Officer Chairman Of The Joint Chiefs Of Staff Community Of Interest Chairman's Program Assessment Capability Portfolio Manager Chairman's Program Recommendations Chairman's Risk Assessment
DAS DAWG DBS DITPR	Defense Acquisition System Deputy's Advisory Working Group Defense Business Systems Department Of Defense Information Technology Portfolio Repository
DOD DODAF DOD CIO DOD IE DOD IEA DODI DSWG	Department Of Defense Department of Defense Architecture Framework Department Of Defense, Chief Information Officer Department of Defense Information Enterprise Department of Defense Information Enterprise Architecture Department Of Defense Instruction Data Sharing Working Group
EGB	Enterprise Governance Board
FCB	Functional Capabilities Board
GDF	Guidance For Development Of The Force

GIG	Global Information Grid
IRB	Investment Review Board
IT	Information Technology
JITAM	Joint Information Technology Analysis And Management
JCA	Joint Capability Area
JCB	Joint Capabilities Board
JCIDS	Joint Capabilities Integration And Development System
JCPAT-E	Joint C4i Program Assessment Tool -- Empowered
JPD	Joint Potential Designator
JROC	Joint Requirements Oversight Council
KM/DS	Knowledge Management/Decision Support
MDR	Meta Data Registry
MPMI	Most Pressing Military Issue
NCDS	Net-Centric Data Strategy
NCSS	Net-Centric Services Strategy
NSS	National Security System
OSD	Office Of The Secretary Of Defense
OSD DPA&E	Office Of The Secretary Of Defense, Director Of Programs, Analysis And Evaluation
OV	Operational View
PIM	Planning Input Memorandum
POAM	Plan Of Action And Milestones
POM	Program Objective Memorandum
PPBE	Planning, Programming, Budgeting, And Execution
SecDef	Secretary Of Defense
SIPRNET	DOD SECRET Internet Protocol Router Network
SNaP-IT	Select And Native Programming Data Input System - Information Technology
STP	System Tracking Program
SV	Systems View
TV	Technical View
USD(I)	Under Secretary Of Defense For Intelligence
WG	Working Group
WMA	Warfighting Mission Area

PART II -- DEFINITIONS

Acquisition Program. A directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need (DODD 5000.1, The Defense Acquisition Program).

Capability. The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. It is defined by an operational user and expressed in broad operational terms in the format of a joint or initial capabilities document or a joint doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) change recommendation. In the case of materiel proposals/documents, the definition will progressively evolve to DOTMLPF performance attributes identified in the capability development document and the capability production document. (CJCSI 3170.01F, Joint Capabilities Integration and Development System)

Capability Portfolio Managers. The civilian and military co-leads responsible for the execution of capability portfolio management activities for a defined portfolio. (DODD 7045.20, Capability Portfolio Management)

COI Forum. A series of quarterly sessions hosted by ASD(NII)/DOD CIO (Information Management Directorate). The purpose of these sessions is to share information, resources, and experiences as more COIs form to meet the goals of the net-centric Data Strategy codified by the DOD 8320.2 Directive, Data Sharing in a Department of Defense.

Combatant Command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02, DOD Dictionary of Military and Associated Terms).

Community of Interest. A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges.

Component. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Services, the Office of the Inspector General of the Department of Defense, the Defense agencies, the DOD field activities, and any other organizational entities in the Department of Defense (DODD 8115.01, Information Technology Portfolio Management).

Data Asset. Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or Web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a Web site that returns data in response to specific queries would be a data asset. A human, system, or application may create a data asset.

Defense Acquisition System. The management process by which the Department of Defense provides effective, affordable, and timely systems to the users. (DODD 5000.1, “The Defense Acquisition Program”).

Domain Portfolio Baseline. An IT investment is assigned to a portfolio using Joint Capability Areas (JCAs) for analysis, selection, control, and evaluation. The domain portfolio baseline will be coordinated with Services and combatant commands and approved by the FCB associated with the WMA IT domain.

Embedded Training. Training accomplished through the use of the trainee’s operational system within a live virtual constructive training environment.” (Reference DoDD 1322.18, 4 September 2004, “Military Training”).

Federated Architecture. A grouping of separately created architectures to form an architecture with larger scope. The Federated Joint Architecture Working Group, tasked by the Enterprise Architecture Summit, is currently defining the framework and business rules for federating and integrating disparate architectures. The Warfighting Enterprise Architecture consists of federated architectures produced by DOD components and includes JCIDS document architectures. As the WMA EA matures it will be located in the DOD Architecture Registry System.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (DODD 8000.1, “Management of DOD Information Resources and Information Technology”).

Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a DOD component directly or used by a contractor under a contract with the DOD component that requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

IT Domain. Subset of the warfighting mission area representing a common collection of related, or highly dependent, information capabilities and services. Managing these related information capabilities and services within domains improves coordination, collaboration, integration, and consistency of processes and interfaces for information sharing. IT domains are the basic organization established in WMA to conduct IT portfolio management and COI oversight. WMA IT domains are aligned to the JCIDS FCBs.

IT Investment. The development and sustainment resources needed in support of IT or IT-related initiatives. These resources include, but are not limited to: research, development, test, and evaluation appropriations; procurement appropriations; military personnel appropriations; operations and maintenance appropriations; and Defense Working Capital Fund (DODD 8115.01, "Information Technology Portfolio Management"). WMA IT investments recommendations will focus on whether acquisition programs, IT systems (as discussed in CJCSI 3170.01E), models and simulations, and budget initiatives should be initiated, modified, continued, or terminated. Specific financial and/or budget information will support program, system, and initiative recommendations.

IT Portfolio Management. The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based **scoring** criteria to achieve mission capability.

Initiative. All resources will be reported within initiatives. Initiatives can be systems, programs, projects, organizations, activities or family of systems. Each component will manage their initiatives through SNAP-IT. Initiatives are registered with key categories of data, GIG breakouts and other categorization requirements. To register a new initiative not previously reported in the IT exhibits and not yet assigned an initiative number, components access the on line registration capability of the SNAP-IT. An initiative number is associated with the initiative's name, functional area/communications and computing infrastructure category; system grouping; and other pertinent management information. The current and archived lists of initiatives are maintained on the SNAP-IT Web page. (FMR Vol 2B, Chapter 18 (180103)).

Mission Area. A defined area of responsibility with functions and processes that contribute to mission accomplishment.

National Security Systems. Telecommunications or information systems operated by the DOD, the functions, operation or use of which involves: intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons systems; or equipment that is critical to the direct fulfillment of military or intelligence missions. This does not include procurement of automatic data processing equipment or services to be used for routine, administrative, and

business applications (including payroll, finance, logistics, and personnel management applications). (See Title 44 USC, Section 3532)

Program Objective Memorandum. Recommendations from the Services and Defense agencies to the Secretary of Defense concerning how they plan to allocate resources to meet the SPG and JPG. (CJCSI 8501.1A, “Chairman of the Joint Chiefs of Staff, Combatant Commanders, and Joint Staff Participation in the Planning, Programming, Budgeting, and Execution System”).

Tagging. The process of associating pieces of information stored in a stream that are not the content itself, but describe the content.

Warfighting Mission Area. WMA’s objective is to enable Joint military operational effectiveness through effective warfighter IT. WMA was established to manage warfighter IT investments as portfolios focusing on improving joint capabilities and mission outcomes. WMA IT investments, to include NSS and automated information systems, models and simulations, support and enhance the Chairman's joint warfighting priorities. WMA IT investments also support actions to create a net-centric, distributed force capable of full spectrum dominance through decision and information superiority. WMA IT domains accomplish IT portfolio management processes in support of their associated Functional Capabilities Boards (FCB). Through the FCBs, WMA will provide input to the Planning, Programming, Budgeting, and Execution (PPBE) System and Defense Acquisition System (DAS) processes. Inputs will include life cycle (e.g., capabilities, resources, acquisition, development, operations, upgrades, deactivation, and retirement/reutilization or demilitarization) oversight.