Department of Defense Plan for Implementing the Federal Information Technology Acquisition Reform Act (FITARA)

Purpose

The purpose of this Plan is to describe the planned actions of the Department of Defense (DoD) to implement FITARA and the guidance contained in Management and Budget (OMB) Memo M-15-14, and describe the Department's processes and procedures for managing its Information Technology (IT) investments.

Background

FITARA was intended to improve Agency CIO involvement in, and improve management of IT investments across the government. Pursuant to FITARA, OMB issued M-15-14 to provide guidance to federal agencies regarding implementation of FITARA. That guidance recognized that FITARA, as enacted, included numerous provisions with exceptions or exclusions for the Department of Defense and Intelligence Community (IC), and directed DoD and the IC to clarify the applicability of OMB's FITARA guidance to their organizations, including alternative requirements or exceptions.

The enclosure describes how the Department will address FITARA provisions and OMB guidance related to:

- Increasing CIO stature and authorities;

- Managing high-risk IT investments;

- Managing agency-wide IT investments as a portfolio;

- Government-wide data center consolidation ;

- Developing an IT acquisition cadre, and

- Developing and maximizing use of government-wide strategic sourcing of IT services and supplies

Terry A. Halvorsen
DoD Chief Information Officer

Enclosure: as

October 15, 2015

Enclosure1: DoD Implementation Plan of Federal Information Technology Acquisition Reform Act (FITARA) P.L. 113-291 §§ 831-837

Federal Information Technology Acquisition Reform Act (FITARA)
P.L. 113-291 §§ 831-837

FITARA Provision	DoD Implementation
Management of IT w/in Federal Gov't *§831 "CIO Authority Enhancements"* • Head of each agency "to ensure that the Agency CIO has a significant role" in PPBE decision processes and management of IT within their agencies	*DoD is excluded from this subsection, with exception of 831(b)(1)(B) – as follows:* • *§831(b)(1)(B)(i)* requires DoD CIO to provide recommendations to SecDef on DoD IT investments. The DoD CIO is the Secretary of Defense's principal advisor for all IT matters for DoD, per DoD Directive 5144.02, which documents the responsibilities and authorities of the DoD CIO.
• CIO must approve all IT contracts and reprogramming of funds for IT programs; CIOs can use existing processes to accomplish the above IF CIO is part of those processes; CIO authority for the above can NOT be delegated • CIOs must approve appointment of other subordinate CIOs	• §831(b)(1)(B)(ii) Requires DoD CIO to certify that IT investments are adequately implementing incremental development. This requirement is met by DoD policy contained in DoD Directive 5000.01, "The Defense Acquisition System, " DoD Instruction 5000.02, "Operation of the Defense Acquisition System," which govern the Department's IT and all other acquisitions, and 10 USC 2223a.
§832 "Enhanced Transparency and Improved Risk Mgmt in IT Investments": • Requires CIOs to make publicly available cost, schedule, performance of major IT investments, and certify at least **semi-annually** that info is current, accurate 　• CIOs must categorize risk of each investment. 　• OMB may waive reporting for certain Agency information based on national security interests; and NSS are excluded • E-Gov and CIO must conduct a review of any moderately-high and high risk programs (rated that way > 1 year), and results reported to Congress 　• ***Provision allows DoD to use existing processes to assess any DoD high-risk investments***	*Management of DoD IT investments:* • DoD National Security Systems (NSS), MIP and NIP funded IT are excluded from FITARA §832. • Other (non-MIP, non-NSS) major DoD IT investments will continue to be reported to OMB's IT Dashboard, and complete Exhibit 300s • DoD risk assessments of these investments will be completed iaw DoD policy, "Revised Department of Defense Chief Information Officer Ratings Process for the Federal Information Technology Dashboard." • For DoD major IT programs that are rated moderately-high or high risk for more than one

FITARA Provision	DoD Implementation
• If investment (other than DoD IT) continues to be high risk, OMB shall deny request for additional development or enhancements for the investment	(1) year, DoD will use its acquisition process and 10 USC 2445(c) to address significant and critical changes, and report results to OMB
§833 "Portfolio Review" • Intended to establish govt-wide process to increase efficiency, effectiveness, consolidate, optimize, and better align IT investments in agencies • Requires OMB to develop standard metrics *in conjunction with Agency CIOs* for assessing IT investments • Requires annual review of agency IT portfolio – for DoD this only applies to business systems AND DoD can use existing acquisition and/or 2222 process to satisfy the review • Does not apply to Intel Community	**DoD Business System Portfolio** • This section only applies to DoD business systems and not to national security systems (NSS) • DoD will use the existing / established defense business system process under 10 USC 2222 and the Defense Business Council co-chaired by Deputy Chief Management Officer (DCMO) and CIO to review the non-NSS business systems portfolio

§834 "Federal Data Center Consolidation Initiative (FDCCI)"
 	
• Requires annual reporting of:
  • agency inventory of all data centers & multi-year strategy to consolidate & optimize data centers;
  • performance metrics for all data centers;
  • agency DCC timeline
 	
• Requires OMB to report government-wide progress on the FDCCI to Congress, including cost-savings; and GAO to do a review of FDCCI progress
 	
• Requires agencies to implement FDCCI consistent with NIST and FedRAMP cloud computing guidelines
	DoD Data Center Consolidation
	
	• DoD will submit the annual report required by §2867, P.L. 112-81 ("*Data Servers And Centers*,") (10 USC 2223a note) to satisfy this requirement to OMB and Congress
	
	• DoD complies with this requirement
	
	• DoD complies with this requirement.

§835 "Expansion of Training & Use of IT Cadres"
 	
• Requires OMB OFPP and E-Gov to work w/agencies (other than DoD) to update Human Capital plans for IT Acquisition workforce:
  • Consider creation of an "IT Acquisition. Cadre"
  • Specialized career paths, Direct Hire Authority, etc.,
	DoD IT Acquisition Workforce
	  • DoD is explicitly excluded from this provision
	  • DoD acquisition workforce is managed IAW chapter 87, Title 10 USC, and implemented through DoD Directive 5000.52, "Defense Acquisition,

FITARA Provision	DoD Implementation
	Technology, and Logistics Workforce Education, Training, and Career Development Program."
	• Additionally, the DoD's IT and cyberspace workforce is under the functional direction of the DoD CIO, and is managed IAW DoD Directive 8140.01, "Cyberspace Workforce Management." This directive establishes policies and responsibilities for managing the DoD cyberspace workforce – personnel who design, build, configure, operate, and maintain IT, networks, and capabilities.
§836 *"Maximizing Benefit of Federal Strategic Sourcing Initiative (FSSI)"* • Requires OFPP to develop regulations requiring Agencies to provide a business case for when they do **not** use FSSI	*DoD Strategic Sourcing* • DoD has had a standing Enterprise Sourcing Initiative for several years which manages strategic sourcing efforts. Additionally, DoD is executing a DOD-wide Better Buying Power utilizing Functional Domain Experts for Services Acquisition Management. The Deputy DoD CIO is the FDE for the Electronics and Communications Services portfolio.
§837 *"Government-wide Software Purchasing Program"* • Requires GSA to develop a strategic sourcing initiative for government-wide s/w and license agreements.	*DoD Enterprise Software* • DoD executes procurement of "Enterprise Software" across the Military Departments for the software with greatest requirement. This is being expanded to be now be more DoD-wide. DoD continues to work with GSA to provide such capabilities as part of its enterprise software initiative.