ISSN 2278-9723
DOI:10.31838/ijccts/08.01.04

Research Article

Examining DoD's Implementation of FITARA and the Implication for IT-Based Defense Systems: A U.S. Case Study

MURODOV S.S.
UTM Centre for Industrial and Applied Mathematics, Universiti Teknologi Malaysia, UTM, Johor Bahru, Johor, 81310, Malaysia
E-mail: Murodov@gmail.com
Received: 25.10.19, Revised: 27.11.19, Accepted: 15.01.20

ABSTRACT
FITARA provides that other than the DoD IT, situations, where investments are found to be high-risk, shall have the Office of Management and Budget (OMB) reject requests for investment enhancements or additional development. Regarding Section 833 "Portfolio Review," the main of FITARA is to develop government-wide processes through which agencies' IT investments could be better aligned, optimized, consolidated, and also ensure that they are effective and efficient. Additionally, Section 833 calls for OMB to collaborate with agency CIOs to establish standard metrics through which IT assessments can be assessed. It is also worth noting that through Section 833, FITARA calls for the agency IT portfolios' annual reviews. However, the case of the DoD holds that this provision or review can be satisfied via the use of the 222 process or the existing acquisition and that the review only applies to its (DoD's) business systems. It is further notable that for the Intel Community, Section 833 (Portfolio Review) does not apply. The main aim of this study was to examine analyze the effectiveness of DoD's FITARA implementation, as well as the implications for defense systems relying on the IT infrastructure in the U.S.
Keywords: Portfolio Review, better aligned, optimized, consolidated.

INTRODUCTION

In FITARA Section 833, communication technologies' requirements have been outlined. For instance, it is expected that agencies engage in a multi-year strategy that is updated and discussed towards the reduction and identification of waste and duplication in their respective IT portfolio; a provision projected to realize cost savings (McManus, 2012). Also, the section calls for agencies to develop or identify mechanisms through which the effectiveness and efficiency of their respective IT investments could be increased and also ensure that they stretch further and develop or identify opportunities that pave the way for increased utilization of shared-service delivery frameworks (Reid, Kaloydis, Sudduth& Greene-Sands, 2012). From these provisions, it can be inferred that Section 833 focuses on the identification of potential waste and duplication and also advocates for the development of action plans through which IT resources, programs, or portfolios could be optimized at the agency level. This study sought to examine analyze the effectiveness of DoD's FITARA implementation, as well as the implications for defense systems relying on the IT infrastructure in the U.S.

RESEARCH CONTEXT

Formerly referred to as the Defense Communications Agency (DCA), DISA refers to a combat support agency of the U.S. Department of Defense (DoD). DISA constitutes contractors, federal civilians, and the military (DISA, 2018). The organization was established with the aim of responding to communication issues that marred World War II (DISA, 2018; p. 1). Currently, the agency provides services to U.S. soldiers worldwide. From the observation by the Congressional Research Service (2018), DISA paves the way for the soldiers to gain access to services such as data services, multinational information sharing, information assurance, and computer hosting. In military force operations, information systems gained from DISA apply in full spectra; including humanitarian efforts, counterterrorism, defensive tactics, and offensive tactics. Therefore, the Congressional Research Service (2018) asserted that the ultimate goal embraced by DISA entails the realization of information dominance through the provision of

effective enterprise infrastructure that assures advantage on the part of users who are in combat.

Specific organizations and individuals to whom or to which DISA offers communication support and information technology (IT) support include systems or individuals contributing to the U.S. defense, the military services, the Secretary of Defense, the Vice President, and the President (McManus, 2012).Regarding specific services offered by DISA, one of the missions involves command and control. According to Nolan, LaTour and Klafehn (2014), this service allows DISA to provide the U.S. military commander with information through which effective decisions could be made and also pave the way for the provision of capability to the warfighter to access necessary information that supports the completion of missions (Reid, Kaloydis, Sudduth& Greene-Sands, 2012). Computing forms another service offered by DISA. Specific computing service portfolios entail server virtualization and hosting, application monitoring, and mainframe hosting. It (DISA) also manages partner labor, software, hardware components, and data (Sands, 2013). Contracting has also been documented as a service offered by DISA whereby the agency is responsible for the purchase of IT and telecommunication services and products, especially in situations where the U.S. military uses various contract vehicles. Regarding its role in enterprise engineering, DISA analyzes, constructs, designs and plans the effectiveness of the cyberspace used by the U.S. military before developing technological standards through which the Global Information Grid (GIG) could be made reliable and secure (Sands, 2013).

ANALYTIC RESULTS

This subsection focuses on the results regarding the analysis of DISA's IT CPIC. Indeed, DISA offers acquisition, telecommunications, and computing services to the military. Particularly, the Federal CIO Council Privacy Committee (2010) suggested that the agency offers these services in the form of a cost reimbursement basis. Recently, the agency's service reimbursements have exceeded $2.5 billion, and it has also engaged in related mission support command, as well as joint war fighting. Through direct appropriations, DISA has funded communication systems; with the appropriations exceeding $1 billion (McManus, 2012). Another notable step embraced by DISA involves the issuance of a 500 Day Action Plan through which the decision superiority of DoD could be supported. Indeed, the plan has been affirmed to constitute 140 planned or ongoing actions associated with resource investment. Relative to the development of this plan, the main focus has been on the understanding and satisfaction of the needs and concerns of customers (Nolan, LaTour & Klafehn, 2014). However, the agency has failed to address some elements of effective plan development. According to Reid, Kaloydis, Sudduth, and Greene-Sands (2012), some of these elements include the assurance of cost-effective planned investments. Whereas baseline commitments regarding the action plan's development have not been established, it is worth indicating that DISA has begun monitoring progress relative to these commitments. As mentioned above, the 500 Day Action Plan reflects a management action aimed at improving the performance of the agency's mission. Imperative to note is that the actions have only addressed some (rather than all) institutional management controls through which effective adjustment to changing strategic directions could be realized. As avowed by Sands (2013), some of these controls entail knowledge management, customer relations management, IT investment management, enterprise architecture management, organizational structure management, IT human capital management, and strategic planning. Overall, the analysis suggests that some of DISA's management controls have progressed much farther while others are in more formative stages. The eventuality is that unless the respective controls function fully, the agency will remain challenged regarding its maximization of accountability and performance, as well as strategic direction.

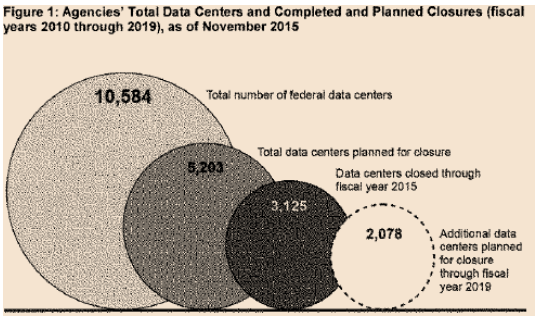

Fig:1

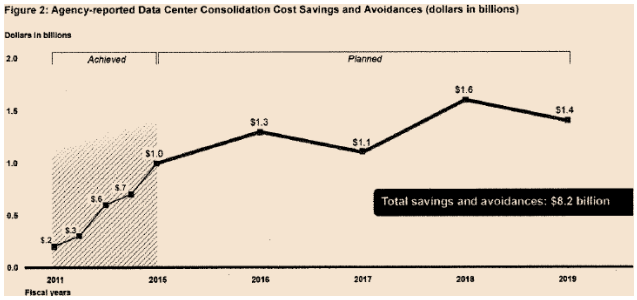

Fig:2

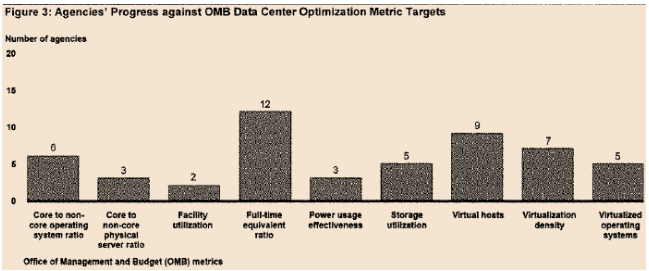

Fig:3

From the figures above, DISA has engaged in a mission of measuring its progress against other baselines in relation to its agency-based planned actions (and also ensured that it reports changes to customer bases that are affected). However, it has failed to measure the progress against some relevant baselines, including the expected benefits (because it has not established these baselines) (Sands, 2013). Additionally, the agency is yet to control changes to baselines in a manner that might justify the changes. It is also worth indicating that DISA has embraced annual benchmarking agency performances in relation to the industry standards (with the aim of measuring the success of action plan implementation), but the benchmarking fails to compensate for the lack of the plan actions' performance measurements (DeVisser & Sands, 2014). The latter outcome is informed by the affirmation that many actions fail to map to the benchmarked performance measures. The eventuality is that the agency cannot discern the economic justification of its continued investment in actions; neither does it discern the degree to which its changes to actions remain warranted (Endrass, Andre, Huang & Gratch, 2010).

CONCLUSION AND RECOMMENDATIONS FOR IMPROVING DISA IT CPIC PROCESS

To steer improvements in the manner in which DISA develops and executes its future and current action plans associated with IT investment, it is important that through the assistant secretary for intelligence, communications, control, and command, the DISA director is directed by the secretary of defense to embrace a disciplined and structured IT investment management procedure. This procedure should concern initiative evaluation, control, and selection in future and current action plans. To achieve

effective plan development, there is a need for the DISA director to ensure that preliminary life-cycle risk baselines for actions, benefit, schedule, and cost are established and the general scope of actions defined accordingly. Also, plan development needs to be conducted in such a way that a high-level and preliminary assessment regarding the proposed actions' return on investment is performed for purposes of gauging the cost-effectiveness of the proposed actions. In relation to plan implementation, there is a need for the DISA director to rely on approved baselines for establishing performance metrics that are results-oriented and also meaningful. Additionally, the DISA director needs to engage in the implementation of a formal process that seeks to inform stakeholders regarding some of the action baselines' significant deviations, as well as control the closure of actions and significant changes targeting action baselines. During the monitoring of DISA's planned actions, it is recommended that the DISA director updates risk baselines, benefit, schedule, cost, and scope of work for all actions as deemed necessary; a step that is poised to ensure that the chosen investment actions are cost-effective. Similarly, there is a need for the DISA director to develop a mechanism through which customer feedback could be tracked for resolving customer concerns that might have prompted the actions.

REFERENCES

1. Reid, P., Kaloydis, F. O., Sudduth, M. M., & Greene-Sands, A. (2012). *Executive summary: A framework for understanding cross-cultural competence in the Department of Defense.* (DEOMI Technical Report No. 15-12). Patrick Air Force Base, FL: Defense Equal Opportunity Management Institute.
2. Congressional Research Service (CRS) (2018). *FY2018 National Defense Authorization Act.* Author
3. DISA (2018). *Defense Information Systems Agency Annual Financial Report - GF Fiscal Year 2018.* Author
4. Nolan, R., LaTour, E., &Klafehn, J. L. (2014). *Framework for rapid situational awareness in the field* (Technical Report 1338). Fort Belvoir, VA: U.S. Army Research Institute for the Behavioral and Social Sciences
5. DeVisser, P., & Sands, R. G. (2014). Integrating culture general and cross-cultural competence & communication skills: Possibilities for the future of military language and culture programs. *The Journal of Culture, Language, and International Security, 1*(1), 34-63
6. Endrass, B., Andre, E., Huang, L., &Gratch, J. (2010). A data-driven approach to model culture-specific communication management styles for virtual agents. *Proceedings of the 9th International Conference on Autonomous Agents and Multi-agent Systems.* Toronto, Canada
7. McManus, D. (2012, April 22). McManus: A smaller, smarter military: The best-equipped Army in the world can still lose a war if it doesn't understand the people it's fighting. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2012/apr/22/opinion/la-oemcmanus-column-odierno-iraq-afghanistan-less-20120422
8. Sands, R. G. (2013, March 8). Language and culture in the department of defense: Synergizing complimentary instruction and building LREC competency. *Small Wars Journal.* Retrieved January 12, 2019 from http://smallwarsjournal.com/jrnl/art/languageandculture-in-the-department-of-defense-synergizing-complimentary-instruction-and
9. Sands, R. G. (2013, 20 August). Thinking Differently: Unlocking the Human Domain in Support of the 21st Century Intelligence Mission. *Small Wars Journal*. Retrieved Jan. 12, 2019 from: http://smallwarsjournal.com/jrnl/art/thinking-differently-unlocking-the-humandomain-in-support-of-the-21st-century-intelligence
10. Khode, V., Sindhur, J., Kanbur, D., Ruikar, K., Nallulwar, S. Mean platelet volume and other platelet volume indices in patients with stable coronary artery disease and acute myocardial infarction: A case control study(2012) Journal of Cardiovascular Disease Research, 3 (4), pp. 272-275.
DOI: 10.4103/0975-3583.102694