DOI: 10.15439/2020KM3
ISSN 2300-5963 ACSIS, Vol. 24

An Analysis and Discussion of the Defense Information Systems Agency's Level of Compliance and Integration of the U.S. Congress' Title Viii National Defense Authorization Act Fy 2015 Subtitle D—Federal Information Technology Acquisition Reform

S. Raschid Muller, Ph.D., MBA
Assistant Professor of Cybersecurity
Capitol Technology University
Laurel, MD, USA
Email - srmuller@captechu.edu
https://orcid.org/0000-0002-1742-7575

***Abstract*—This paper reflects a conducted assessment of the Defense Information Systems Agency's (Department of Defense) compliance with the Federal Information Technology Acquisition Reform Action (FITARA) Section 833: Portfolio Management and Section 834: Federal Data Center Consolidation Initiatives. The paper is organized by providing an overview of DISA leading into a brief history of FITARA (and its associated federal government implementation). For Section 833, the Government Accountability Office (GAO) Information Technology Investment Management (ITIM) assessment tool was applied to DISA's Information Technology Capital Planning and Investment Control (CPIC) process for evaluation, analysis, and recommendations for improvement. Following GAO ITIM, Section 834 was introduced, leading into a PEST and SWOT analyses relative to DISA's implementation of the framework concluding with the evaluation and recommendations. Summarily, Kotter's 8-step change model was applied in a proposed 12 – 36-month plan for implementation throughout the agency for senior leadership in addressing the various gaps of both sections 833 and 834.**

***IndexTerms*—FITARA, DISA, GAO, IT Capital Planning**

I. Introduction

THE PURPOSE of this paper is to conduct an assessment of DISA compliance with the Federal Information Technology Acquisition Reform Action (FITARA) Section 833: Portfolio Management and Section 834: Federal Data Center Consolidation Initiatives [1]. The paper is organized by providing an overview of DISA leading into a brief history of FITARA (and its associated federal government implementation). After providing background information on Section 833, the Government Accountability Office (GAO) Information Technology Investment Management (ITIM) assessment tool [2] will be applied to DISA's Information Technology Capital Planning Investment Control process for evaluation, analysis, and improvement recommendations. Following GAO ITIM, Section 834 will be introduced, leading into a PEST and SWOT analyses relative to DISA's implementation of the framework concluding with the evaluation and recommendations. Summarily, Kotter's 8-step change model [3] will be applied in a proposed 12 – 36-month plan for implementation throughout the agency for senior leadership in addressing the various gaps of both sections 833 and 834 [1].

The Defense Information Systems Agency (DISA) is headquartered at Fort Meade, Maryland, since 2011. According to the DISA website [4], the agency is charged with the mission of "provide, operate, and assure command control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations."

DISA receives funding through congressional appropriations and a Defense Working Capital Fund (DWCF) to meet the information technology requirements and needs of the entire Department of Defense (DoD). In 2018 DISA had a total budget of $9.4 billion (US), of which Congress budgeted $2.2 billion (US) through appropriations, and DWCF funding was estimated at approximately $6.9 billion (US). The agency's current mission priorities as per the DISA Strategic Plan [4] include: 1) improving responsiveness, agility, and collaboration with its various stakeholders and mission partners, 2) providing efficient, resilient, reliable, and assured infrastructure and services to its customers, and 3) defending the Department of Defense Information Networks (DODIN), securing its' data, and mitigating risks to the DoD holistically. Currently, DISA's Enterprise IT/IT Modernization efforts include the following:

- National Background Investigation System
- Cloud Computing
- Defense Information Systems Network (DISN) Tech Refresh
- CENTRIX
- The Global Command and Control System Joint Enterprise (GCCS-JE)
- Computing ecosystem

II. Literature Review

A. US Federal Government's Implementation of FITARA

Enacted on December 19, 2014, FITARA reflects US legislation to ensure that all federal Agency CIOs assume control of IT investments [5]. Indeed, the law requires that federal agencies in the US offer comprehensive inventories of data centers to the Office of Management and Budget (OMB) [6]. From recent reports by the Government Accountability Office (GAO), overall, $80 billion of the federal government budget is channeled to IT investments annually [7]. GAO has also estimated that this investment is likely to exceed $89 billion. Based on the historical context, most of these investments' projects have experienced years-long schedule delays and multi-million-dollar cost overruns [8].

Therefore, FITARA was established in response to the growing need for a long-term framework that would provide room for the management, assessment, and tracking of federal IT investments. Federal Chief Information Officers (CIOs) play active and crucial roles to achieve these requirements, and the GAO and Congress monitor their activities. FITARA focuses on seven major areas perceived to affect how federal agencies manage and purchase IT assets [1].

- Section 831 – Expanding the federal CIO authority
- Section 832 - Improvement of risk management and transparency in IT investments
- Section 833 – Portfolio reviews
- Section 834 – Federal data center consolidation
- Section 835 - Expansion of the use and training of IT Cadres
- Section 836 – The maximizing of federal strategic sourcing initiatives (SSI)
- Section 837 – Government-wide purchases of software

B. FITARA Section 833

Section 833, "Portfolio Review," holds that the main aim of FITARA is to develop government-wide processes through which agencies' IT investments could be better aligned, optimized, and consolidated [8]. Additionally, Section 833 calls for OMB to collaborate with Agency CIOs to establish standard metrics through which IT assessments can be achieved. It is also worth noting that through Section 833, FITARA calls for agencies to implement annual reviews of their IT portfolios [9]. It is also expected that agencies engage in a multi-year strategy that is updated and discussed to reduce and identify waste and duplication in their respective IT portfolios, a provision informed by the need to achieve cost savings [10]. Also, Section 833 calls for agencies to develop or identify mechanisms through which their respective IT investments' effectiveness and efficiency could be increased and ensure that they create or recognize opportunities through which increased utilization of shared-service delivery frameworks could be realized [11]. From these provisions, it can be inferred that Section 833 focuses on identifying potential waste and duplication and advocates for developing action plans through which IT resources, programs, or portfolios can be optimized at the agency level.

1) Federal IT Capital Planning and Investment Control (CPIC)

Established by the Government Accountability Office (GAO), the ITIM process reflects responsibilities and policy through which agencies' mission performance could be improved. ITIM process implementation involves selecting, controlling, and evaluating IT investments [12]. The central objective is to promote accountability among agencies. Furthermore, the legislation and its associated regulations aim to maximize the value with which IT investments are associated and eliminate inefficiencies, reducing duplicate spending [12]. FITARA strives to control the oversight, acquisition, and planning of IT resources by establishing specific responsibilities for agency Chief Executive Officers, the Chief Information Officer, and agency heads [5].

ITIM reflects a framework responsible for identifying and organizing critical processes through which IT investment could be successful. The CPIC process strives to plan, develop, and acquire capital assets and manage and operate those assets via usable life, having achieved the initial acquisition process [13]. Thus, GAO-ITIM's CPIC process reflects a decision-making mechanism striving to pave the way for IT investments' integration of effective strategic planning [14]. Three major phases have been documented about the CPIC process [2].

- PHASE 1 – Priorities are determined before making informed decisions regarding ongoing or new initiatives worth funding and necessary for inclusion in IT portfolios.
- PHASE 2 – Ongoing management procedures to monitor the nature of the selected initiatives' progress.
- PHASE 3 – Consistent evaluation of the process.

2) GAO-ITIM Framework for Improving the IT CPIC Process (Section 833)

As the IT CPIC process progresses to maturity, five major stages are embraced and operate so that each procedure builds on a preceding stage. The main aim is to ensure that an organization's IT investment is enhanced [14].

Stage 1 - Creating Investment Awareness

The first stage involves creating investment awareness, and the investment process is unpredictable, unstructured, and ad hoc. Indeed, this stage does not differentiate between the failure and success of different projects. Preferably, IT projects that are seen to reflect suitable investments or success are mostly attributed to the project team's exceptional actions, proving challenging to repeat [15].

Stage 2 - Building the Investment Foundation

The second stage implies that organizations strive to define and develop their IT investment boards and establish opportunities or business needs. The respective IT projects are likely to address and employ the knowledge gained towards new IT proposal selection [16].

Stage 3 - Developing a Complete Investment Portfolio

The third stage focuses on developing a well-defined and consistent perspective on IT investment portfolios while maintaining integrated and mature evaluation, control, and selection processes. Upon selecting an IT project and discerning that it meets the expected performance expectations (as defined during the second stage), organizations likely establish IT investment portfolios via investment procedures aimed at expanding the firm's focus from that of a primary project-oriented context to that which embraces broader portfolio perspectives [13].

Stage 4 - Improving the Investment Process

In the fourth stage, the main focus is on improving the IT investment portfolios and processes while ensuring that the selection and mature control processes are maintained. This stage requires organizations to analyze their respective investment portfolios regularly [13]. The main aim is to allow for the continuous alignment of investments with the most recent architectural versions.

Stage 5 - Leveraging IT for Strategic Outcomes

Lastly, the fifth stage and GAO-ITIM IT CPIC implementation involve leveraging IT towards strategic results. The mastering of the evaluation, control, and selection processes culminate in shaping the results [14].

C. FITARA Section 834

FITARA Section 834: Data Center Optimization Initiative (DCOI) is the continuation of the Office of Management and Budget's Data Center Consolidation Initiative (FDCCI) that began in 2010. Section 834 required the government to consolidate and optimize its data centers by 2018. It was still extended by the FITARA Enhancement Act of 2017, which extends the requirement to the end of the fiscal year 2020 [17]. As a result of these initiatives, the federal government has witnessed significant savings based upon improved efficiencies, newer technologies, and the emergence of cloud environments. Because DISA has several data centers worldwide, the agency must comply with the latest initiatives and report annual inventories, savings, and findings to OMB. In this study, the SWOT and PEST analytic methods are used to gain insight into the degree to which DISA has implemented FITARA Section 834.

1) PEST and SWOT Frameworks for Analysis for Section 834

The selected analytic frameworks (PEST and SWOT) are different in assessing institutional ideas. Whereas the appearance of similar factors in each framework point to the similarity between these frameworks, PEST evaluates a view from a particular position or business standpoint. Also, PEST can be incorporated into SWOT, or it can be presented before the SWOT analysis to achieve a similar effect.

2) Political, Economic, Social, and Technological (PEST)

The four aspects constituting the PEST framework include political, economic, social factors, and technological [18]. The political factors that have conflicts and wars, international pressure groups, pressure groups or home market lobbying, initiatives, grants and funding, and trading policies [6]. Others include government term and change, government policies, regulatory bodies and processes, international legislation, future legislation, current legislation home market, and environmental or ecological issues.

Economic issues that the analytic method (PEST) examines include international monetary or trade matters, exchange and interest rates, end-user or customer drivers, distribution trends and market routes, specific industry factors, and market and trade cycles. Others include seasonality issues, taxation specific to services or products, general taxation issues, overseas trends and economies, home economy trends, and the home country situation [7].

Social factors include ethical issues, advertising, publicity, religious or ethnic characteristics, buying access and trends, significant influences and events, fashion and role models, consumer buying patterns, technology institutions, and brand image [14]. Additional social factors analyzed through the PEST framework include law changes that affect social factors, media views, consumer opinions and attitudes, demographics, and lifestyle trends.

In the study by

The technological issues or factors that the framework considers include global communications, intellectual property issues, technology patents, licensing and access, innovation potential technology legislation, consumer buying technology or mechanisms, information and communications, manufacturing capacity and maturity, technology maturity, the replacement of solutions or technology, research funding, and competing for technology development [9].

3) Strengths, Weaknesses, Opportunities, and Threats (SWOT)

The SWOT analysis [19] refers to a useful tool through which an institution's position could be understood and reviewed. The framework's application is essential because it informs decision-making regarding future institutional direction and new ideas [7]. Additional scholarly studies assert that SWOT analysis assesses information subjectively, and its central motivation is to promote informed decision-making, discussion, and understanding of institutional concepts [8]. The SWOT framework is divided into four sections: strengths, weaknesses, opportunities, and threats of an institutional idea [19]. Some of the institutional aspects that the SWOT framework seeks to examine include organizational capabilities, customers, and business solutions.

Strengths observed some of the factors considered during the analysis or application of this analytic method include people, assets, resources, unique selling points, competitive advantage, institutional capabilities, and advantages of a proposition [20]. Other factors observed that need to be considered while analyzing an institutional idea's strengths include communications, IT, quality, value, the likely returns, and innovative aspects [10].

Other studies have documented factors that need to be considered while analyzing the weaknesses of an institutional idea. Some of these factors include gaps in capabilities, a proposition's disadvantages, poor leadership and commitment, compromised cash flow and continuity, own known vulnerabilities, and lack of competitive strength [21].

Some of the forces that are worth considering concerning the analysis of the opportunities at the disposal of an organization include market volume demand trends, agencies, partnerships, information and research, market response to tactics, niche target markets, new horizontal or vertical markets, and global influences [22]. Others include innovations and technological developments, lifestyle or industry trends, competitors' vulnerabilities, and market developments [22].

Regarding threats, the SWOT analytic framework focuses on issues such as credit and financial pressures, insurmountable weaknesses, obstacles, new ideas, services and technologies, market demand, competitor intentions, IT developments, environmental effects, legislative effects, and political effects [11]. Additional scholarly studies have examined and documented some of the factors that the selected analytic framework considers while analyzing opportunities at the disposal of an institution's operations. In contrast, threats and opportunities examine external factors, strengths, and opportunities to explore internal factors.

III. Results & Analysis of Applied Frameworks to Disa

A. Analytic Results of FITARA Compliance to Section 833

When deploying the PFM ITIM assessment tool to the Agency TTPs, DISA's compliance with section 833 can be viewed as subpar according to the processes in place, which directly align with the grades received from the DoD CIO Annual Scorecard. Subsequently, the agency remains at Stage 1: "Creating Investment Awareness" of the five stages. After conversing with several key personnel and stakeholders with duties related to compiling section 833 data, there is a consensus that FITARA compliance "to the letter" isn't an agency priority with aggregating data at the "enterprise level." However, it should be noted that the agency is compiling the data at the "component level" throughout the various DISA Commands around the world. The issue is that a mechanism or process at DISA Headquarters Fort Meade for reporting purposes doesn't exist. As a result, the DOD CIO's office summoned DISA leadership to the Pentagon for questioning in which the agency had to devise a plan for future grading and compliance then.

The communication lines were opened from the meeting between DISA's Office of the Chief Financial Officer and the DoD CIO to review DISA's methodology to capture savings and define acceptable metrics from both parties. Consequently, while DoD CIO's office looks for ways to capture and track savings at the component level, DISA HQ needs to consider doing the same for the enterprise level to meet the already standardized needs. Summarily, VADM Norton commissioned a FITARA Tiger Team led by Mr. Chris Catlin to understand DISA's compliance better and look for a way forward.

B. PEST Analysis of FITARA Compliance

Political

Political decisions affect how (and when) institutions such as the military will be employed, and employment effects DISA's operations. The US as a democracy exhibits credible and transparent elections whereby most of the elected representatives (including the President of the United States of America) tend to have considerable influence on global and national policymaking [11]. Despite this promising trend, the US continues to fall victim to terror group threats [22]. For DISA, the political situations characterizing the environment in which it operates imply that checks and balances are imperative to note. The law protects most of the rights of the minorities and other stakeholders served by the agency. Despite the mixed outcomes, it is evident that the agency operates in a supportive and positive region due to political stability. Sands [22] asserted that stability is informed by low-risk military invasion due to the United States' military might and power. Based on these favorable conditions, DISA has implemented FITARA Section 834 through technological dominance, advanced infrastructure, and a stable political environment.

Economic

Operating within the world's largest economy, DISA has enjoyed a well-developed IT system through partnerships with renowned economic organizations. However, labor has proved costly in this economy. As such, DISA has had to implement some of its FITARA-related IT strategies through outsourcing cheap labor from the rest of the global economies. What remains unaddressed is the extent to which the cheap labor has (or otherwise) promoted the agency's central mission and vision. Also, rapid changes in the global economy, a platform served by DISA, have proved challenging relative to the implementation of FITARA Section 834.

Social

Like most other developed regions, the dominance of an aging population marks the social environment in which DISA operates. As such, its implementation of FITARA faces the threat of labor shortage. However, as DeVisser and Sands [5] observed, labor stability is likely to be achieved through stable educational systems. The majority of the population supports liberal mindsets to change the security world to an IT-driven platform. What remains notable is that there is increasing illegal migration and racial intolerance in most of the regions served by DISA, trends that threaten the agency's implementation of FITARA. Specifically, these trends threaten operational stability at DISA because many individuals are keen to realize socio-economic mobility. Still, some of the means that they use (such as the state as mentioned above of illegal migration) imply that the security agencies served by DISA might be overwhelmed. The goals and objectives laid down by FITARA might experience stalled progress in implementation.

Technological

DISA's implementation of FITARA is dominated by an environment that proves to be one of the world's leaders in technology and science. Significantly, most of the individuals and organizations that the agency serves are characterized by a longstanding fascination for IT [6]. Thus, the institution has implemented FITARA while ensuring that it serves the people and the organization's technological needs. However, the environment served also faces stiff competition from rising economies. The dilemma is how DISA will satisfy its key stakeholders' technical requirements and implement FITARA while retaining technology supremacy.

C. SWOT Analysis of FITARA Compliance

Strengths

Regarding DISA's implementation of FITARA Section 834, the agency strongly emphasizes the military's general IT mission. This support implies that DISA can secure and maintain funding streams, especially when improved FITRA Section 834, implementation outcomes can be demonstrated [10]. Support for DISA's mission to serve other agencies and individuals is unlikely to wane soon [21]. Apart from political permission, it is observed that DISA operates in an adequate budget environment [11]. Additional strength lies in the decision by DISA to embrace new, responsive technology systems. DISA's ability to deploy modern IT systems is associated with high-level visibility and support [22].

Weaknesses

At DISA, one of the perceived weaknesses entails human capital. On the one hand, the IT staff adequacy reflects a notable strength. On the other hand, the staff is stretched thin and unlikely to attract dissatisfaction and turnover. Should the agency be forced to recruit new IT talent, several forms of challenges might prove significant. Some of these forms include the lack of a joint workforce document, challenges associated with contract resource procuring, and the general shortage of technically skilled talent [8]. Another weakness with which DISA is associated entails a lack of adequate enterprise controls and strategy. Due to the agency's restructuring, an apparent central decision authority might prove challenging to achieve. DISA's implementation of FITARA Section 834 is also marred by a weakness of the lack of adequate agency controls and strategy.

Opportunities

During DISA's implementation of FITARA Section 834, one of the disposal opportunities entails maximizing its move to another IT system. More analytics capabilities might be realized by accessing centralized data, especially when it ensures that infrastructure issues do not cause significant operations problems [12]. By maximizing the move to another IT system, it is projected that a new information superhighway will result in DISA. By establishing partnerships with similar organizations that serve identical agencies or individuals and offer related services, DISA might establish paths through which private options might be integrated into its current implementation of FITARA Section 834, upon which capacity concerns might be improved or offloaded [6].

Threats

Data breach forms one of the most significant threats facing DISA. Furthermore, the agency's morale and authority face the threat of goal and guidance imposition from "on high," a trend cautioned that is likely to reflect a lack of adequate control [9]. Given that the outside solutions are unlikely to fit in DISA's unique IT environment, the agency's systems rollout might be undermined significantly and end up blocking forward progress. The effectiveness and credibility of DISA's implementation of FITARA Section 834 also face the acquisition process's threat, primarily due to inadequate oversight.

D. Analytic Results of FITARA Compliance to Section 834

In summary, significant strengths characterizing DISA's implementation of FITARA Section 834 include improved data outcomes and analytics due to the ability to leverage new IT systems, the presence of funding streams, and the enjoyment of political support. Weaknesses include silo-based contract management, lack of adequate enterprise visibility and control concerning IT expenditure, the increasing demand for training and retention of the IT staff, and growing concern associated with human capital or staffing. Regarding opportunities, the SWOT analytic framework suggests that DISA's implementation of FITARA Section 834 could exploit mechanisms such as the development of public-private partnerships (that could, in turn, aid in addressing human capital or IT staffing issues) and maximizing benefits associated with IT rollout. It is also evident that several threats face DISA. Some of these threats include high visibility failures, IT rollout problems that might make the agencies or individuals served to lose trust, lack of adequate forward investments due to slow transition, and data breaches or cybersecurity issues that are likely to undermine the stakeholders of the stakeholders served; both at the individual and organizational or Agency levels.

IV. Recommendations

A. Compliance Section 833

To steer improvements in how DISA develops and executes its future and current action plans associated with IT investment, VADM Norton must embrace a structured IT investment process [16]. This procedure should concern initiative evaluation, control, and selection in future and current action plans. VADM Norton should ensure that life-cycle baselines are established and way-forwards are well defined for consistent effectiveness measured in metrics. Plan development is organized at a high-level to estimate the return on investment for proposed way-forwards' cost-effectiveness [2]. Senior stakeholders should be engaged about the prescribed process to include actionable transactions that directly affect metrics as varying from the baseline. 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 [14]. 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.

B. FITARA Compliance Section 834

To improve the degree of implementation of FITARA Section 834, one of the significant issues that DISA needs to embrace is understanding the baseline environment. DISA needs to collect input, define the vision from the SWOT and PEST analytic frameworks, establish transparency, and communicate accountability. Indeed, an achievement of this recommended mechanism requires that the agency identify an aggressive connection with significant stakeholders and ensure that partnerships, which form part of the opportunities at its disposal, are solidified. In so doing, it is projected that DISA will be better placed to discern what might be working and what might have failed, eventually ensuring that priorities are identified accordingly. Understanding the baseline environment is also projected to allow DISA to focus on the assurance of IT transition success while empowering its staff via adequate funding of strategies aimed at data protection. By implementing this mission, additional benefits might include continuous and resilient operations and prevention against possible data breaches that could, otherwise, compromise stakeholder confidence.

Further, it is recommended that DISA improves or consolidates its collaborative mechanisms by increasing its focus on staff training and continuing education. Success in improving collaborative tools in an agency such as DISA could be realized when big data analytics are used more effectively [7]. Thus, DISA needs to engage support organizations in garnering best practices that might shift from an oversight model to an operational model. It is also worth indicating that the recommended strategy of consolidating the agency's collaborative mechanisms might witness more success if the outsourcing model is considered and embraced more aggressively.

C. 8-Step Kotter Implementation Plan

This section applies Kotter's 8-step change model [23] to recommend a 12-36-month action implementation, especially about DISA's integration of FITARA. In this model, the first step concerns creating urgency.

Step 1 – Creating a Sense of Urgency

The change could happen if an entire organization embraces a sense of urgency regarding some needed change [23]. At DISA, this initial step calls for the sparking of initial motivation by prompting convincing and open dialogue regarding the extent to which FITARA Section 834 has been implemented, some of the threats ahead, significant milestones, or strengths that characterize the agency, and opportunities that are worth exploiting. Particularly, DISA needs to hold regular seminars and utilize relevant communication platforms to state potential threats to its current implementation of FITARA, establish scenarios depicting what is likely to characterize its future operations, and seek critical stakeholders' support towards the examination exploitation of opportunities at its disposal. To ensure successful change initiation, there is also a need for senior leaders and managers to sustain their long-term engagement and make it clear that the implemented strategies will be followed up and monitored continuously, which is likely to improve confidence among service users and key stakeholders.

Step 2 – Building Coalitions

From the change model, the second step involves the formation of a powerful coalition. This step requires change implementers or organizations to convince the targeted institutions, groups, and individuals that change is necessary [3]. For DISA, it becomes essential for the strategic personnel to stretch beyond change management and lead it. The selection of influential people, teams, or coalition needs to be determined by the IT personnel's political importance, expertise, status, and job titles. To ensure that team building and emotional commitment are realized and the right mix of team members from different levels and departments, DISA needs to share the assessments with Congress and the rest of the DoD sections to ensure that the proposed change is understood and supported accordingly.

Step 3 – Form a Strategic Vision

The third step requires creating a vision for change [24]. Notably, the recommended changes are likely to attract numerous solutions, approaches, or ideas regarding paths that need to be adopted during implementation. Therefore, DISA needs to ensure that the images generated by the team established are linked to the agency's overall vision while ensuring that they do not contravene FITARA's specifications. This linkage allows team members to quickly remember or grasp the change [23]. The vision paves the way for team members to understand the motivation and perceived benefits behind a given shift. For DISA, a summary capturing the projected future of the changed operations needs to be presented to the members.

Step 4 – Enlist a Volunteer Army

The process above needs to culminate in the communication of the stated vision. Specifically, DISA needs to stretch beyond special meetings and engage in regular discussions, ensuring that the team established for implementation purposes remembers and responds to the theme. By walking the talk, the selected team will demonstrate the behavior expected from other individuals and organizations. Also, visual communication will help address any anxieties and concerns raised by stakeholders such as Congress and the military personnel honestly and openly, having led by example.

Step 5 – Remove Barriers

The next step needs to constitute the removal of obstacles. Having built the people's buy-in and talked about the mission (which involves implementing the changes stated earlier), any resistance to change will have to be addressed. At DISA, removing obstacles or addressing any resistance change will have to be realized by establishing clear structures to empower team members towards vision execution, ensuring that the proposed changes move forward. Important to note is that addressing the barriers will require the selected team to identify specific groups that might oppose the proposed change (an example being the Congress) and sensitize them about some of the threats that DISA's implementation of FITARA faces currently, some of the opportunities at the agency's disposal, and the perceived benefits poised to accrue from the implementation of the proposed changes or the exploitation of any untapped potentials.

Step 6 – Generate Short-Term Wins

DISA's implementation of the proposed changes will need to be marked by creating short-term wins that seek to motivate team members towards further progress and attract support from otherwise negative thinkers and critics. Particularly, short-term wins will have to be realized by blending long-term goals with short-term targets. To reinforce the change implementation team, it is expected further that DISA will reward team members.

Step 7 – Sustain Acceleration

The seventh step will involve building on the change to ensure that improvements are made to the quick wins while keeping the long-term goals in mind. As each victory is realized, DISA's team will also be engaged in the analysis of issues that might have worked and those that require improvements, as well as approaches through which those improvements might be achieved. An example of an improved approach entails adding of new leaders and change agents to the initial change coalition or team [3].

Step 8 – Institute Change

Lastly, the change will have to be anchored in the rest of DISA's organizational culture. Making a change to be part of an organization's core ensures that it sticks and stretches into the far future for implementation by other workforce generations [24]. At DISA, making the change part of corporate culture will be informed by most of the scholarly affirmations documenting that an organization's corporate culture dictates what is likely to be supported by employee teams [24]. Thus, the continuous effort will be made to ensure that every aspect of DISA experiences or sees the change, a step projected to cement the agency's organizational culture's recommended strategies. Imperative to acknowledge that the success realized by the stepwise change and implementation of the recommended changes (aimed at strengthening DISA's implementation and integration of FITARA) will be determined by leadership support.

V. Conclusion

DISA needs to engage and manage the majority of key stakeholders' expectations more proactively. Notably, much time needs to be spent on input collection to ensure that the Agency's IT strategic plan is established quickly and communicated effectively. To ensure that the agency's priority projects are implemented timely, it is essential to act on and evaluate staff performance and measurable projects via the identification of the top talent and also directing the IT staff towards a transition to ensure that the organization achieves short maturity (via improved controls and governance, as well as assured consistent transparency to other individuals and organizations served). It is also evident that the degree to which DISA might integrate and comply with FITARA depends on the capacity to improve internal operations and its key stakeholders' experiences. Thus, there is a need for the organization to ensure that it poses a positive impact on the well-being of warfighters by establishing consensus and also demonstrating vision in the military IT community. In so doing, DISA's implementation of FITARA Section 834 might be more successful and ensure that it yields significant contributions to the IT rollout strategy.

Given the strengths and weaknesses revealed by the PEST and SWOT framework analyses, it is also essential for DISA to ensure that it maintains its stability while transforming the perceived weaknesses into opportunities for improvement. Indeed, these actions are poised to pave the way for the agency to steer dramatic improvements in the military IT environment, having advocated for an information-driven approach or model. Imperative to highlight is the extent to which DISA collaborates with significant stakeholders and achieves transparency. Accountability will play a moderating role in determining the successful implementation of FITARA Section 834 and the achievement of other internal and external goals with which it is associated.

References

[1] H.R.1232 - Federal Information Technology Acquisition Reform Act, 113th US Congress, September 2014. https://www.congress.gov/bill/113th-congress/house-bill/1232 [Accessed October 2, 2020]

[2] United States General Accounting Office (GAO), Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (pp. 1 - 138), 2014. [Accessed October 9, 2020]

[3] J. Auguste, Applying Kotter's 8-Step Process for Leading Change to the Digital Transformation of an Orthopedic Surgical Practice Group, Toronto, Canada. J Health Med Informant 4, 129, 2014. [Accessed September 9, 2020]

[4] DISA Strategic Plan, Strategic plan: 2015-2020, 2015. https://www.disa.mil/-/media/Files/DISA/About/Strategic-Plan.ashx [Accessed September 21, 2020]

[5] P. DeVisser, and R. Sands, "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), pp. 34-63, 2015. [Accessed September 3, 2020]

[6] B. Endrass, E. Andre, L. Huang, L., and J. Gratch, "A data-driven approach to model culture-specific communication management styles for virtual agents" Proceedings of the 9thInternational Conference on Autonomous Agents and Multi-agent Systems, Toronto, Canada, 2010. [Accessed September 3, 2020]

[7] V. Gezari, The tender soldier: A true story of war and sacrifice, New York: Simon & Schuster, 2013 [Accessed September 3, 2020]

[8] R. Hajjar, "Military warriors as peacekeeper-diplomats: Building productive relationships with foreign counterparts in the contemporary military advising mission', Armed Forces and Society, 40(4), 647-652, 2014. [Accessed September 1, 2020]

[9] P. Holmes-Eber, E. Tarzi, and B. Maki, B., "U.S. Marines' attitudes regarding cross-cultural capabilities in military operations: A research note", Armed Forces and Society, 42(4), 741-751, 2016. [Accessed September 10, 2020]

[10] D. McManus, "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, April 22, 2012. http://articles.latimes.com/2012/apr/22/opinion/la-oemcmanus-column-odierno-iraq-afghanistan-less-20120422 [Accessed September 5, 2020]

[11] P. Reid, F. Kaloydis, M. Sudduth, and A. Greene-Sands, "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, 2012 [Accessed September 5, 2020]

[12] R. Sands, "Thinking Differently: Unlocking the Human Domain in Support of the 21st Century Intelligence Mission", Small Wars Journal, 2013. http://smallwarsjournal.com/jrnl/art/thinking-differently-unlocking-the-humandomain-in-support-of-the-21st-century-intelligence [Accessed September 6, 2020]

[13] United States Government Accountability Office (GAO), Cost Estimating & Assessment Guide: GAO-09-3SP, 2009. http://www.gao.gov/products/GAO-09-3SP [Accessed September 6, 2020]

[14] United States General Accounting Office (GAO), "Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management", United States General Accounting Office Executive Guide: GAO-03-584G, 2013. [Accessed September 5, 2020]

[15] S. Fernandez, and H. Rainey, "Managing successful organizational change in the public sector", Public Administration Review, 66(2), 168-176 [Accessed September 5, 2020]

[16] United States General Accounting Office (GAO), "Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity", pp. 1 – 138, United States Government Accountability Office, Washington, D.C., 2004. [Accessed October 5, 2020]

[17] Data Center Optimization Initiative, New draft policy, 2016. https://datacenters.cio.gov/policy/ [Accessed September 5, 2020]

[18] T. Sammut-Bonnici, and D. Galea, D. (2015) PEST analysis, Wiley Encyclopedia of Management (eds C.L. Cooper, J. McGee and T. Sammut-Bonnici). doi:10.1002/9781118785317.weom120113. [Accessed September 15, 2020]

[19] D. Pickton, and S. Wright, S. (1998) "What's swot in strategic analysis?" Strategic Change, 7, pp.101-109. doi:10.1002/(SICI)1099-1697(199803/04)7:2<101::AID-JSC332>3.0.CO;2-6 [Accessed September 15, 2020]

[20] M. McCloskey, A. Grandjean, K. Behymer, and K. Ross, "Assessing the development of cross-cultural competence in Soldiers (Technical Report 1277)", U.S. Army Research Institute for the Behavioral and Social Sciences (DTIC No. ADA533959), 2010. [Accessed September 15, 2020]

[21] R. Nolan, E. LaTour, and J. Klafehn, "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, 2014. [Accessed September 15, 2020]

[22] R. Sands, "Language and culture in the department of defense: Synergizing complimentary instruction and building LREC competency, Small Wars Journal, 2013. https://smallwarsjournal.com/jrnl/art/language-and-culture-in-the-department-of-defense-synergizing-complimentary-instruction-and [Accessed September 15, 2020]

[23] J. Kotter, "Management is (still) not leadership", Harvard Business Review, 2013. [Accessed September 15, 2020]

[24] E. Cameron, and M. Green, Making Sense of Change Management: A Complete Guide to the Models Tools and Techniques of Organizational Change, (3rd Edition). London, GBR: Kogan Page, 2012. [Accessed September 15, 2020]

Dr. S. Raschid Muller is a Senior Cybersecurity SME with the Department of Defense (DoD) at Fort Meade, Maryland. He teaches Cybersecurity at the undergraduate and graduate levels at Arizona State University, University of Maryland Global Campus, and Capitol Technology University. Dr. Muller is a 2020 Brookings Institute Fellow (LEGIS) currently serving on the House Committee for Homeland Security assigned to the Cybersecurity, Infrastructure Protection, and Innovation subcommittee in the United States Congress. He will attend U.C. Berkeley's Executive Leadership Academy in 2021 as a Fellow in the Goldman School of Public Policy. He is a member of IEEE, ISACA, NDIA, and AFCEA.