



IT Acquisition Advisory Council (IT-AAC)

Recommendations for Implementing EO 13800 and Federal IT Modernization

Mr. Chris Liddell
 Director, American Technology Council
 The White House
 1600 Pennsylvania Ave
 Washington DC 20500

The Honorable John Michael Mulvaney
 Director
 Office of Management and Budget
 725 17th Street, NW
 Washington DC 20503

The Honorable Elaine Duke
 Acting Secretary
 Department of Homeland Security
 Nebraska Ave Complex
 Washington, DC 20407

The Honorable Wilbur Ross
 Secretary
 Department of Commerce
 1401 Constitution Ave
 Washington, DC 20230

The Honorable James Mattis, GEN (ret)
 Secretary of Defense
 Pentagon
 1400 Defense Pentagon
 Washington, DC 20301-1400

Mr. Tim Horne
 Acting Administrator
 General Services Administration
 1800 F St NW
 Washington, DC 20405

September 20, 2017

Dear Mr. Liddell, Secretary Duke, Honorable Mulvaney, Secretary Mattis, Secretary Ross, Mr Horne,

We at the IT-AAC are honored to provide our coordinated response to the forward thinking Report to the President on Federal IT Modernization, supporting EO 13800. As the nation's leading voice on Federal IT Reform, we applaud this effort to usher in commercial standards of practice and innovations emanating from the Global IT market.

The IT-Acquisition Advisory Council (IT-AAC), a federation of two dozen leading IT industry groups (NGO) and Standards Bodies (SDO), was chartered in late 2007 to provide Government leaders from Congress, White House and the Executive Branch alternative sources of expertise and insights that are more representative of the \$4T Global IT market, of which Federal IT sector is less than 2%. We believe this consolidated response will provide the White House, ATC with an evidenced based approach that can better inform the White House and Executive Branch how to modernize and security legacy IT systems that are consuming some 85% of all resources and represent our greatest cyber vulnerabilities.

We have reviewed your 2017 Report to the President on Federal IT Modernization and have found it to be comprehensive and very much aligned with past recommendations and findings gathered from our 9 year effort to address this long standing challenge that have frustrated previous well intended efforts to achieve these noble goals. A few observations are offered before getting into our responses to your five questions;

1. FFRDC/DIB over reliance: The goal of improving use of commercial IT innovations (COTS, Cloud, XaaS), is greatly appreciated, and a challenge recognized during the drafting of the Clinger Cohen Act. Unfortunately, most of government relies on an antiquated SDLC process and FFRDC/DIB resources that are "make biased" and drive costly custom development. The Free and Open S/W (FOSS) agile development approach that *should* be favored by major ISVs is not appropriate for major IT consumers, and undermining agency adoption of commercial innovations (COTS, Cloud, Shared Service). S/W development is the highest risk automation approach, especially when using unpatched open source code that creates new cyber vulnerabilities. The Economy Act, Clinger Cohen Act and Conflict of Interests rules need to be enforced better, including restrictions on FFRDC unfair competition. A partnership between GSA FAS and IT-AAC would address these needs while alleviating this frequent failure pattern that is costing the tax payer an estimated \$20Billion per year (DSB, OMB, GAO sourced).
2. IT Acquisition: Another major impediment called out in over 30 major IT reform studies, especially with Defense IT, is the mis-application of a "Weapon Systems, Waterfall Acquisition" framework and expertise that are "make biased". These "design to spec" frameworks undermine the adoption of commercial innovations and standards of practice (TBM, Cloud, SDN), and perpetuate a costly, 81 month delivery cycle, with a horrific success rate of only 16%. IT-AAC has sourced, piloted and standardized a robust Agile Acquisition Framework that has been fully vetted by both govt and





industry. Both OMB and GAO need to measure the cost and time of agency IT acquisition processes given the rapid pace of change. DOD frequently spends up to 100% premium on acquisition support cost, focusing on compliance vs measurable outcomes.

3. Benchmarked Standards of Practices: of Fortune 1000 companies thru their organic IT communities of practice reveal greater focus on measured outcomes and commercial IT adoption. This requires better metrics beginning with requirement stage. TBM provides a sound structure for measuring the COTS cost, but does not address the hidden "people cost" resulting from over specification and custom development. The Consortia for S/W Quality (CISQ), provides a DoD/SEI/NIST/DHS approved standard for automatically scanning for known cyber vulnerabilities, 1000x more efficient and effective than manual reviews. ICH's Acquisition Assurance Method (AAM), is one of the most mature Agile Acquisition Maturity Model in government for buying and assessing COTS (risk, cost, value) per SEI, ANSER and DOD reviewers. All of these should be encouraged to move Federal IT into the Digital World. On Risk Management, we appreciate the significant focus on the cyber front, and felt the sections addressing this were VERY well articulated and thorough. However, greater balance might be needed as the current RMF approach too narrowly focuses on s/w code that govt can access (GOTS, Open Source, Custom), and does not fully address COTS or implementation risk. Agencies will need better access to commercial standards of practice, expertise and innovations to achieve IT modernization goals.
5. We were delighted to see the emphasis on Shared Services, Cloud and XaaS, but felt it needed greater detail on the "how" issues. These require a completely different sourcing model and a detailed understanding of Service Level Management and Services Oriented Architectures. IT-AAC's SDO partners have already created frameworks that some agencies have successfully embraced to guide these investments, but most are failing miserably. DOD and the IC deserve no exceptions.

Please find our responses below to your specific questions:

ATC Q1) What are major attributes that are missing from the targeted vision? (Appendix A, Appendix B)

IT-AAC RSP1) Workforce, IT Acquisition Reform and Incentives. The vision articulated in the very well written document is spot on, and addresses nearly every conceivable issue we have documented. Continued embrace of commercial standards like TBM, AAM and CISQ frameworks are critical to improving how we measure cost, risk and mission value. We recommend greater emphasis on the non-technical issues, including Incentive and Federal IT workforce shortcomings; lack of trained or experienced staff in areas of requirements, tech assessment, risk management, service level management nor performance based contracting. Also important are new incentives that drive **risk based decision making** and **mission outcomes**. Public/private partnerships like IT-AAC, Center for Internet Security and P3 could help fill the knowledge gap by providing an elastic pool of just-in-time SMEs. GSA FAS is partnering with IT-AAC to provide these capabilities already on Schedule 70, but few have taken advantage.

ATC Q2) What are major attributes that should not be included in the targeted vision? (Appendix A, Appendix B)

IT-AAC RSP2) We felt all was well sourced and relevant. Proportionately, too much focus on cyber security and not enough on modernization and agile acquisition techniques that are today's Achilles heel. IT-AAC has identified 14 core shared services with associated performance metrics and use cases. This is missing in the discussion. Platform as a service has the lowest ROI.

ATC Q3) Are there any missing or extraneous tasks in the plan for implementing network modernization & consolidation?

IT-AAC RSP3) This was the best written, well thought out section of the document. We would suggest adding to the plan an alternative Agile Sourcing & Acquisition framework (vs development) that aligns with goals contained in FITARA, CCA and OMB A130. A template based approach that aligns with TBM Framework, but includes performance and risk metrics. Cost is only one part of the decision analytics process. An Agile Acquisition TechFar (currently targeting agile development) is needed agencies support sourcing of COTS, Shared Services and XaaS offerings would eliminate the costly "design to spec" and Integrator lock-in that government is currently struggling with.

ATC Q4) Are there any missing or extraneous tasks in the plan for implementing shared services to enable future network architectures?

IT-AAC RSP4) The network is very important, but the next four layers in the OSI model also need to be modernized and secured. IT-AAC has identified 14 service layers that should be considered for its Shared Service portfolio. GSA FAS should be the IT Modernization Center of Excellence to include support for drafting requirements, developing performance metrics, shared market research, and coordination point for industry outreach, including SDO cooperation. Embrace of Agile Acquisition, SOA and SDN are critical success factors.





ATC Q5) What is the feasibility of the proposed acquisition pilot?

IT-AAC RSP5) The thinking behind this pilot was very thorough. The recommendations that would help this pilot be most successful include; a) first identify and validate pilot/early adopters work already performed. We have done this and glad to share lessons learned, many dealing with the culture, processes and incentives. b) working in close coordination with established public/private partnerships (IT-AAC, TBM, CISQ, CSA) who have a deep portfolio of high tech members and affiliates. c) focus on mission outcomes and document what works. Include DOD and the IC as their systems are most at risk.

Again, we at the IT-AAC applaud this vision and action plan, and welcome the opportunity to remain part of the solution. Many of the past IT Reform failures typify quotes popularly attributed to Albert Einstein "continuing the same process over and over again, and expecting different results", and "trying to fix today's problems with the same thinking (resources) that got us there".

If you are interested in IT-AAC's related IT Reform Roadmaps, please visit the following hard hitting recommendations;

- 2009 Roadmap for Sustainable IT Reform Vol1; <http://www.it-aac.org/images/ITAACRoadmapCongSumv1.pdf>
- 2011 Roadmap Vol 2: http://www.it-aac.org/images/Dec2010Roadmap_Summary.pdf
- 2014 HASC/SASC Response leading to FITARA adoption: http://www.it-aac.org/images/IT-AAC_Defense_IT-Reform_Roadmapv2.0_SignedFinal9-24.pdf
- 2015 FITARA Implementation Roadmap; http://www.it-aac.org/images/IT-AAC_FITARA_Cyber_Roadmap_OMB_SUM.pdf

Very Respectfully,

MGEN Dale Meyerrose, PhD
Former DNI CIO

Honorable John G. Grimes
Former DOD CIO

Honorable Jacques Gansler Ph.D.
Former USD (AT&L)

Honorable David Oliver
Former PDUSD AT&L

Dr. Bill Curtis
CISQ Exec Director

Bill Greenwalt
Former SASC Staff

Honorable Dov Zakheim
Former USD (Comptroller)

Ted F. Bowlds, LTG, USAF Ret
Former AF ESC CMDR

Dave Deptula, LTG USAF Ret
Former AFA2 Deputy CoS

Dr. Marv Langston
Former Navy CIO & OSD DCIO

Chris Pick
TMB C Exec. Director

John A. Weiler
IT-AAC Exec. Director

Tony Scott
Former Federal CIO

Kevin Green, VADM (ret)
Former Deputy CNO

