IT Alliance for Public Sector
A Division of ITI

SUBMISSION OF THE IT ALLIANCE FOR PUBLIC SECTOR (ITAPS) ON IT MODERNIZATION

On behalf of the leading providers of ICT hardware, software, services, and solutions to the public sector that are members of the IT Alliance for Public Sector,[1] we appreciate the opportunity to provide comments to the American Technology Council's (ATC) IT Modernization Report. Our primary submissions regarding IT Modernization are to be found in the previously provided report, ITAPS Tech Industry's Recommendations for Federal IT Modernization. Those recommendations embrace the full agenda of issues and topics raised by the ATC and we look forward to working collaboratively on these and other issues in order to achieve broad, comprehensive IT Modernization in the federal government. These comments are intended to build and elaborate upon our submission.

#1. WHAT ARE MAJOR ATTRIBUTES THAT ARE MISSING FROM THE TARGETED VISION?

Network Consolidation and Security Vulnerabilities: The Report addresses the fundamentals of network modernizations and options, but does not acknowledge tying security requirements into the network modernization or the possibility that modernizing toward one IT Network creates new vulnerabilities for the Federal government. Many in the private sector security field are concerned that modernization and/or consolidation to one, modernized IT network for the Government will expose new and more vulnerable security holes. The recommendation for implementing security through enhanced application and data layer protection is the next logical step forward for security.

> **Recommendation**: The Report should be expanded to include a risk management approach to address how and when new vulnerabilities would surface and consideration of a security expert working group to advise the ATC on partitioning and rationalizing the IT Network across federal functions, agencies, or mission delivery areas and to lessen security vulnerabilities. Further, include a discussion on resilience and a proposed architecture that would be able to absorb a failure or intrusion and continue to operate or fail gracefully, without transiting the issue, further preventing additional consequence and propagation. Consider also adding requirements for agencies to improve on tracking breaches, alerting other agencies of threats, and developing reaction strategies at other agencies to prevent further damage. To improve security implementations, it should be strongly recommended that the Department of Homeland Security (DHS) Continuous Diagnostics and Monitoring (CDM) begin to get agencies closer to 100% Multifactor Authentication (MFA) for all users and get a better understanding of what hardware is on the network. Indeed, MFA implementation must be a priority.

> **Recommendation:** The Report should also contemplate a persistent layered approach by directly addressing endpoint security (including device, data, and identity management). No one disputes the value of migrating applications to the Cloud. The simultaneous security and cost benefits are no doubt compelling. The same benefits are true for the active management of access points to

[1] **About ITAPS.** ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies offering the latest innovations and solutions to public sector markets. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more. Follow us on Twitter @ITAllliancePS.

the Cloud. Client devices (e.g., PCs, laptops, tablets, smartphones, print devices, to name a few) are all part of an exponentially growing attack surface that must be proactively managed, as well. Cloud migrations will not eliminate this risk if the portals to access applications and data on the clouds are compromised. A similar approach of leveraging a security expert working group to advise the ATC on bringing endpoint security in line with established policies and best practices in cyber resilience – such as existing technologies that enable self-healing devices – should be included in scope.

IT Architecture and Legacy Systems: The Report addresses the fundamentals of network modernizations, but it does not address the next layer in IT architecture: legacy systems and portfolio rationalization. A natural next step is "what to do with all these legacy systems" and the need to rationalize and address development and management of new applications.

Recommendation: The Report should acknowledge that the Federal government must simultaneously engage in rationalizing spending on legacy systems and future application investments, and agencies should be actively engaging the IT industry to collaborate on market research of future managed services.

Recommendation: The Report focuses on network modernization and does not address application migration to the cloud. For specific recommendations on application migration, please see Tech Industry's Recommendations for Federal IT Modernization for additional guidance.

Architecture Frameworks: While the report mentions Reference Architectures, it does not mention what to do with the Federal Enterprise Architecture Framework (FEAF) or the Department of Defense Architecture Framework (DoDAF) or how it relates to the commercial The Open Group Architecture Framework (TOGAF).

Recommendation: Add references and guidance, at a minimum, on how and what agencies will do with the FEAF or DoDAF or how it relates to the commercial TOGAF. We believe that TOGAF should be used as it was originally donated to the open group when it was called The Architecture Framework and Information Model (TAFIM).

#2. WHAT ARE MAJOR ATTRIBUTES THAT SHOULD NOT BE INCLUDED IN THE TARGETED VISION?

Attributes Not to Include in Targeted Vision: The Executive Summary specifically points to ATC, the Office of Management and Budget (OMB), DHS, the Department of Commerce, and the General Services Administration (GSA) to adjudicate industry feedback, and the role of these entities is brought into the discussion later in the report. It also calls out certain companies as targets for engagement, to the exclusion of other companies providing services and IT to the federal community. Further, the Report proposes using "Manufacturer's Agreement" versus contracting officer/contractor negotiation (*see* page 42).

Recommendation: Consider expanding the aperture of this effort to ensure an all-inclusive scope and eliminate specific references using company names; instead note capabilities that the Government is seeking to use and/or expand on within the Vision. The use of manufacturing agreements would be a significant change in government procurement and may require further discussion with OMB's Office of Federal Procurement Policy (OFPP). Rather than identifying specific companies, the ATC should only identify attributes of services needed to ensure a competitive environment, efficiencies, and to allow for innovation.

#3. ARE THERE ANY MISSING OR EXTRANEOUS TASKS IN THE PLAN FOR IMPLEMENTING NETWORK MODERNIZATION & CONSOLIDATION?

Implementation Plan and Progress Reporting: Network modernization, cloud migration, security assessments, and more, are all core to the report. Although the Report lays out a set of time-bounded requirements for agency action on virtually every element, that approach does not address progress measures, metrics, or reporting.

Recommendation: Include requirement for agencies to measure and report on schedule, budget, deliverables, and performance metrics rooted in value to the agency mission. Performance metrics should be focused on desired outcomes (e.g., improved security, innovation, etc.) rather than completion of activities. Additionally, the ATC should consider submitting quarterly progress reports to the President's Management Council, OMB's Program Associate Directors and Deputy Associate Directors, the President's Cabinet meetings, and, where appropriate, publicly to send a coordinated message that the Administration will ensure a modern and secure Federal IT infrastructure and the appropriate use of shared services to enable future network architectures is accelerated and achieved. In this regard, the ATC should expressly acknowledge that the tools of acquisition, be they GWACs, Shared Services, or GSA Schedules, are a means to an end, not an end unto themselves.

Engaging IT Industry Early and Often: The Report notes the need for federal agencies and the IT industry to collaborate and share best practices. While the Report emphasizes the need to capture and use lessons learned from cloud migration efforts, it fails to recognize that the Government and industry have significant experience with past efforts that can be leveraged now._Many agencies do not engage the IT Industry on best practices, nor meet with industry *prior to* issuances of RFPs. Thus, federal program and IT managers may not be fully briefed nor open to new and innovative perspectives from industry, leaving many RFPs reflecting "old thinking" to acquiring network services, cloud services and managed services.

Recommendation: The Report and OMB must drive improving the engagement and learning of the federal
IT workforce and program managers by requiring market research, industry outreach, and collaboration sessions to drive the tenets of the ACT IT Modernization effort. ATC should consider requiring outreach and industry collaboration in General Services (GS) position descriptions and annual performance plans, as well.

Recommendation: As noted in the ITAPS recommendations, the Government can utilize existing lessons learned captured by GSA, the CIO Council, individual Government organizations, and industry to better educate the workforce.

Guidance Regarding Existing or Planned Contracts: The Report emphasizes use of the EIS contract vehicle, but does not provide guidance regarding existing contracts with similar scope. Similarly, the Report does not provide guidance regarding other contract vehicles with scope similar to EIS (e.g., GSA Alliant, NITAAC CIO-CS, CIO-SP3). Additionally, the Pilot does not reference the GSA Cloud SIN, the new GSA Cloud IDIQ, or the other existing contract vehicles that provide these services. While ATC recommends that "agencies should consider immediately pausing or halting upcoming procurement actions that further develop or enhance legacy IT systems identified that need modernization," it is not clear that there has been full consideration of the impact to agencies' systems and missions that such delays in procurement actions may have on day-to-day operations. Selectively halting upcoming procurement efforts can make sense as the prioritization of highly valuable assets is conducted. Halting progress, however, on all efforts can adversely impact important missions, increase the security exposure of the systems being modernized, and may negatively impact the continuity of services.

Recommendation: We believe that ATC must clarify the intent and provide guidance regarding existing contracts or alternative contract vehicles, as well as on planned procurements. ATC should communicate that agencies continue with key initiatives for cloud transformation strategy and planning, critical technology analysis and evaluation, and other related initiatives while prioritization efforts are performed.

#4. ARE THERE ANY MISSING OR EXTRANEOUS TASKS IN THE PLAN FOR IMPLEMENTING SHARED SERVICES TO ENABLE FUTURE NETWORK ARCHITECTURES?

Potential Impediment for Quick Win on CDM: For CDM, the report proposes Secure Shared Services to allow security centers of excellence to increase Agency's security. The recommendation suggests using Security Operations Center (SOC) as a Service (SOCaaS) to assist securing smaller agencies, especially non-CFO Act Agencies.

Recommendation: CDM can be implemented as a repeatable pattern for each cloud provider using existing implementations. To suggest that there should be one CDM implementation would unnecessarily constrain architectural decisions made by agencies to solve mission and business problems. The right approach to solving the convergence between CDM and cloud would be to require vendors to implement cloud versions that could run across all cloud provider platforms.

Recommendation: The ATC should address the biggest impediment to SOCaaS in federal agencies, which is not technical, but relates to data separation and visibility between Agencies. For example, in working with several department-level CIOs, it was determined that some agencies do not have

visibility into the components. For SOCaaS to work, consider requiring federal CIOs to ensure that the SOCaaS have full visibility into to the client agency and components.

ATOs and Moving to the Cloud: Before address the ATO, the ATC needs to have a discussion about the future of FedRAMP with stakeholders from the government and industry. The ATC should be aware that one of the biggest barriers of moving to a cloud environment is the Authority to Operate (ATO) process with Federal agencies. This process can delay achieving the benefits of cloud computing. We are encouraged that ATC, as stated on pg. 21 of your report, is directing OMB to focus efforts on "reducing the time and complexity of ATOs, including ATOs specific to cloud infrastructure and platforms."

Recommendation: Accelerate the ATO approval process and standardize its use across civilian agencies. The inconsistencies and rework inherent in the current process drives up costs and does not support "shared services" processes, standards, or compliance. Furthermore, the government can and should rely on commercial certification processes when possible, like ISO standards, rather than reinventing a government-specific standard.

Process Reengineering, Costs and Moving to the Cloud: Many agencies have not spent the time and requisite funding to conduct portfolio analyses of agency applications. Moving to the cloud will require both application portfolio analysis and determination as to which applications, if any, might need to be reengineered and/or eliminated before moving to a cloud. This can delay achieving the benefits of cloud computing and it could drive up the costs overall for the agency.

Recommendation: As part of the cloud shared services plan, agencies should be required to conduct an application portfolio analysis and determination on the viability and requirements for current applications. As noted in the ITAPS report, we believe such analyses should be required as part of the overall scheduled reporting.

Mandating Government-wide Operating Standards: The Report acknowledges the need for the CFOs and CIOs to work together to address funding requirements and challenges. Lack of standardization in systems operating requirements has led to the IT Industry to develop many one-off or "snowflake" applications, driving up operating and upgrade costs. Many agencies, however, lack the capabilities to effectively utilize today's vast amounts of data for use in analytics and to enable informed decision-making. Utilizing industry advances in this area will allow the government to address today's challenges and evolving threats.

Recommendation: The Administration should consider mandating government-wide operating standards, as it would make future upgrades and investments less costly and time consuming. Standards setting would also be a catalyst for industry investment (needed for real investment ROI). Further, the government should consider establishing clear outcome-based pricing with penalties and incentives for contracts, and require OMB's OFPP to implement, drive the use of and monitor agencies performance, and delivery in IT contracts. Mandating government-wide operating standards requires cultural change and strong leadership and impacts employee and

citizen experience, such that without some type of change management and adoption program accompanying these operating standards to be implemented, there is a greater risk of failure.

In doing so, the government can leverage artificial intelligences, business analytics, machine learning, and enhanced automation capabilities to improve agency decision-making, mitigate staffing and skills limitations, as well as budgetary challenges. For example, automation and cognitive enablement are needed to supplement the staffing and skills shortages in the critical area of cyber security. The government can also make better use of the vast amounts of data available today via advanced analytics solutions to improve cybersecurity by utilizing data aggregation, predictive analysis, pattern matching and the enhanced sharing of security relevant information across agencies.

#5. WHAT IS THE FEASIBILITY OF THE PROPOSED ACQUISITION PILOT?

Proposed Acquisition Pilot: The proposed pilot for a federal cloud email acquisition, for a commodity offering, is theoretically feasible. However, there are many concerns and questions that as to the implementation.

First, it is clear from the title of Appendix D that the Pilot title is not a buying strategy, but rather a process tactic that risks mission success. As found in the ITAPS report, we believe that the goal of the acquisition system is to facilitate an agency's mission at fair and reasonable prices. That goal is met by using the procurement approach that, based on agency-identified data, best fulfills the agency's mission-based needs, not by imposing a one-size-fits-all procurement process approach. It is unclear to ITAPS if the Pilot fulfills this goal for a variety of reason. For example, the reason for identifying "whether CSPs would be willing to participate in a pilot of the 'Manufacturer's Agreements'" as a goal is unclear. If the intent is for the government to use only company terms and conditions, it could pose risks to the agency if the mission requires additional protections. Also, in the past, the government had challenges in volume (discount) pricing for technology licenses or services as a result of the complexity involved in consolidating purchases for a volume commitment, including standardization, across agencies.

Furthermore, it appears that the economic premise used to justify the Pilot is inconsistent with the government's interests as buyer. The Pilot's equilibrium arises solely from limited competition among a limited number of sellers with limited product differentiation. Agencies, however, need continuing access to innovative IT at competitive prices, which comes from the dynamic market. Identifying "[s]uggested industry partners to target" is a highly unusual approach to a government acquisition pilot. Rather than allowing for a limited marketplace, the Pilot should leverage the free market competitive forces that reward participation by innovators and promote downward price pressure.

Additionally, it is unclear to industry how the success of the Pilot will be gauged as there is a lack of a meaningful analytic construct to measure Pilot performance. There is no identification of "before-state"

baseline data, and end-state metrics simply measure process completion, not value to the agency mission. The problems in the current system arose from just this kind of focus on processes, rather than on providing improved value to supporting agency missions. As such, modernization efforts should emphasize providing value to agencies and achieving the desired outcome rather than just checking a box.

Lastly, the relationship between the Pilot and existing programs is unclear and could impose requirements that conflict with the latter's contracts, leading to disputes. Open negotiation and reporting of services, configurations, and prices might be of little consequence where competition and innovation are limited to favored, pre-determined vendors, but they do risk discouraging market participation by new companies, who would not be as eager to expose proprietary date, thus limiting the government's access to innovation. Further, a mandate to report units and volume pricing compels new innovators to risk exposure of information that would allow reverse-engineering of their pricing methodology. ATC must also provide clarification regarding whether GSA will procure the services at a minimum guaranteed level and "resell" to other agencies or if the agencies themselves will procure the services.

> **Recommendation:** Based on the foregoing discussion, the construction and rationale for the Pilot must be re-assessed to ensure that it is structured in such a way that, first and foremost, facilitates agencies' missions and promotes government access to innovation and ease of acquisition. Moreover, it is incumbent upon the ATC to recognize that this Pilot can only be applied to commodity offerings like cloud service offerings and it should not be extrapolated to more complex shared service (e.g., financial management).