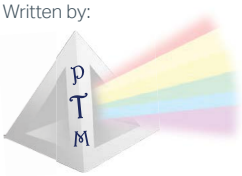
White Paper

IT Operations Management
Application Development Management
Security

The MGT Act: Stimulating Federal IT Innovation and Reducing Stagnation

Written by:



Prism Technology Marketing, LLC

MICRO FOCUS
Government Solutions

Table of Contents

With the passage of Modernizing Government Technology (MGT) Act at the beginning of the year and the American Council on Technology's (ATC) report to the President, the focus is squarely on IT modernization and Cyber Security.

Executive Summary

The clock is ticking, the hour glass is emptying, the game clock is running down, pick any colloquialism you want that highlights the sense of urgency Federal IT CIOs and IT program managers feel, and you would be accurately describing our current point in time. Over 30 years and a trillion dollars in IT spend and yet, here we are, facing debilitating Cyber Security threats. There is a need to digitally transform, or potentially face outsourcing at a scale and depth unseen in prior swings of the pendulum, from in-house to outsourced. However, change won't come easy. The Federal IT landscape is stagnant, with over 75% of the budget allocated to O&M and under 10% in genuine DME. Waves of Federal IT initiatives from Congress and OMB, admonishments by GAO, and successes here and there by the occasional outlier CIO or IT program manager have not produced pervasive world class Cyber Defenses or IT modernization.

Over the past few years, FITARA, DCIO, CDM, FedRAMP, and several other initiatives and scorecards tell IT what they need to do and grade them on it, but never how to go about improving or how making changes in culture or behavior will lead to better results for subsequent endeavors. Part of the problem is that virtually all new initiatives are targeting use of the small sliver of budget available to support innovation. With the passage of Modernizing Government Technology (MGT) Act at the beginning of the year and the American Council on Technology's (ATC) report to the President, the focus is squarely on IT modernization and Cyber Security.

MGT will focus on cost savings and improved outcomes (including cyber)—and rightfully so. The problem is that most agencies do not understand their baseline costs, and so their approach to IT modernization focuses on time to value and cost avoidance. But this does not always translate to cost savings, and worse, often bears little correlation to desired outcomes. Studies show that many Federal Agencies don't have situational awareness of the inventory of assets and applications on their networks, nor are they able to breakdown cost by IT capability within their own departments and agencies. It's no wonder there are countless examples of redundancy, shadow IT systems, and legacy systems. The problem is further exacerbated by contractual obligations, reprogramming limitations, annual artificial budget boundaries, and a lack of tools to support accurate and granular measurement of capabilities and their use, and therefore proper management. For instance, there are over a thousand vacation request systems scattered across the Federal Government, if even ten percent of these could be identified for consolidation in an MGT phase one program, significant headway could be achieved.

MGT takes an approach that focuses on pairing loans with an oversight board to entertain novel proof of concepts (PoCs) backed by best practices in program, contract, and technical management that can be reproduced at scale across multiple departments and agencies. As with any legislation, it must be translated into policy, and that policy into guidance—in the case of IT, with some from OMB—on the "what" needs to be done and proposal evaluation criteria. What is missing—yet again—is the "how" to successfully achieve the results desired on the other end.

The cost savings are the "what." The "how" is made up of best practices that should be developed as part of the PoCs. Shared Services are an obvious way to address cost savings, and consolidation is a core methodology for shared services delivery. How IT teams working on MGT projects approach existing programs, platforms, and contracts, and how they implement repeatable step-by-step processes to deliver value from shared services, is just as critical as the results they achieve. For example, information security and IT Operations should be addressed in an integrated fashion, leveraging standards and automation. World class organizations who've undertaken digital transformation employ a standard IT value chain applied to ensure reproducibility at each stage (plan, build, deploy, run). Proper cost accounting, project portfolio management, application delivery management, information security and IT management require the proper tools and enterprise-wide governance. Risk and compliance capabilities are required for this next generation IT Operating model.

This paper addresses the "how," rooted in a fundamental philosophy that IT should run like a business and align to open industry standards. In reading this paper we believe CIOs and IT program managers will realize they can achieve improved outcomes by changing their culture, contracting methodologies, consolidation priorities, and strategies for migration and cloud adoption. We describe the "how" in a prescriptive fashion, with careful attention on assessment of current IT capabilities and program portfolios, and how to correlate cost with outcomes to better understand the TCO for various options with a focus on consolidating common business processes to deliver digital transformation. It's the position of this paper's authors and Micro Focus® Government Solutions that MGT PoCs should be approached as a series of pragmatic and incrementally higher risk but higher yield projects, starting with "low hanging fruit" projects that deliver quick results with quantifiable and reproducible cost savings.

In March 2018 Micro Focus Government Solutions held its 8th annual Government Summit that included a panel on IT modernization. The panelists included Steven Grewal, former Deputy CIO for GSA, David Wray, Ops CTO for Micro Focus Government Solutions, and Robert Efrus, CEO/Founder for Efrus Federal Advisors. In total, all three panelist have roughly a century of Government IT experience. The panel was so well received that we felt compelled to put pen to paper and explore the topics covered and the points made in the panel discussion in more depth. Contributions were made by the above three panelists, as well as Rob Roy, Security CTO for Micro Focus Government Solutions. Based on their knowledge, willingness to have several follow-up conversations, contributions, and edits, we believe this paper will provide a practical view and prescriptive approach to project selection, teaming, submissions, planning, and implementation – not just for the MGT act, but in the context of your overall portfolio of Federal IT projects.

This paper addresses the "how" rooted in a fundamental philosophy that IT should run like a business and aligned to open industry standards. In reading this paper we believe CIOs and IT program managers will realize they can achieve improved outcomes by changing their culture, contracting methodologies, consolidation priorities, and strategies for migration and cloud adoption.

Companies like Facebook, Google, Netflix, and recent start-ups are digital by design. IT is built into every transaction they perform and interaction they have.

Modernization, Always over the Horizon

Contrary to popular public perception, Federal IT has an esteemed history dating back to the early stages of IT adoption in the 60s and 70s, from mammoth-sized mainframes comprised of vacuum tubes to the invention of the ARPANET by DARPA. The government, in partnership with academia, continues to pioneer in areas of basic research, such as funding for optical computing at NIST (Singer, 2014). However, over time, government's use of IT in support of internal- and external-facing operations, has fallen behind its commercial counterparts.

Like Federal IT organizations, large multinational corporations have been slower to change, burdened by several decades of legacy systems. Change is difficult when you have employee roles in the tens of thousands, customer bases that range from hundreds of thousands to millions, and countless external vendors and service providers. The result for large public and private enterprises has been the accumulation of several generations of different vendors' proprietary systems and business processes embedded into the systems. These investments create stagnation, yet are hard to eliminate without a clear cut,

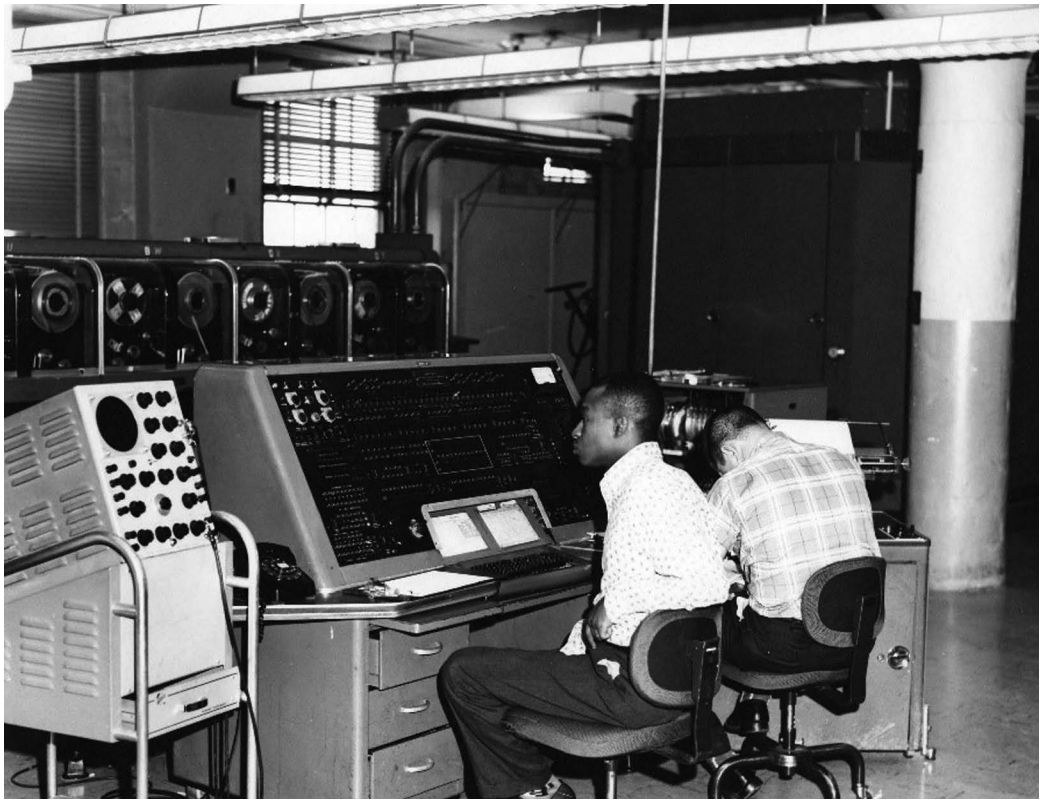


Figure 1. US Census Bureau, circa 1960 UNIVAC

compelling ROI justification. Digital transformation sounds terrific, but change is hard and often requires an external, existential threat met with a corresponding vision, and leadership committed to fundamental organizational and cultural change.

Companies like Facebook, Google, Netflix, and recent start-ups are digital by design. IT is built into every transaction they perform and interaction they have. Little is holding them back in the way of legacy infrastructure. Unfettered harnessing of digital business models, the ability to rapidly react to feedback by customers who appreciate the customization, and new approaches to business and personal needs, enables them to disrupt entire markets, and ultimately dislodge—and in many cases eliminate—large adversaries (Ex. Blockbuster, Toys-R-Us). Some large incumbents have already seen digital business strategies and tactics employed by their competition as change-or-die inflection points and have responded successfully, reducing or eliminating IT stagnation, transitioning to new digital business and consumption models.

The Federal Government now faces the same inflection points as large enterprises face. UPS can be replaced by FedEX, GSA with Amazon, and so forth, or alternatively, converted to private contracts one internal function at a time, from call centers to IT, outsourced wholesale. For Federal organizations to survive, they will need to become digital businesses, and this begins and ends with their IT organizations. But, as things stand, this is a tall order. Federal IT organizations are stagnated. This stagnation can be tracked as a combination of a high percentage of IT budget spent on Operations and Maintenance (O&M), 75%, and a very low percentage of the budget spent on innovation, measured as Development, Modernization, and Enhancement (DME), as reported by Federal IT accounting (Government Accountability Office (GAO), 2016). There is valid concern at all levels of government and from outside analysts monitoring Federal IT that stagnation is intractable and could place Federal IT into a death spiral (Goldstein, 2018) .

There are four core areas of IT stagnation:

1. Aging IT assets: Hardware (networks, servers, storage) and software (monolithic, lacking service-oriented nature, etc.)
2. Scarce yet outdated skillsets to support legacy systems, yet little in the way of top talent for latest in technology or program management
3. Siloed departments and fiefdoms which bespoke everything, from IT platforms to contracts
4. Contracting and partnering financial management, legislative guidance, and policy implementation complexity

Federal leadership, including Congress, would prefer federal agencies run IT like a modern business based on IT organizations akin to what we see inside of Facebook, Comcast, or other large global enterprises. In other words, replacing a moribund, stagnate Federal IT model with a fluid one based on agile development and cloud-based services, and supported by outcome-based contracting. As seen in Figure 2, there have been several waves of legislation and initiatives dating back to the Clinton administration to change organizational structures, contracting policies, and skill sets to modernize Federal IT.

Four Core Areas of IT Stagnation:

1. Aging IT assets: Hardware (networks, servers, storage) and software (monolithic, lacking service-oriented nature, etc.)
2. Scarce yet outdated skillsets to support legacy systems, yet little in the way of top talent for latest in technology or program management
3. Siloed departments and fiefdoms which bespoke everything, from IT platforms to contracts
4. Contracting and partnering financial management, legislative guidance, and policy implementation complexity

MGT is ambitious in that its goals are to fundamentally change the Federal IT technical and cultural models that have led to the high O&M and low DME figures through pragmatic, incremental, data-driven, proof-of-concept projects that are scaled-up in subsequent projects over multiple years.

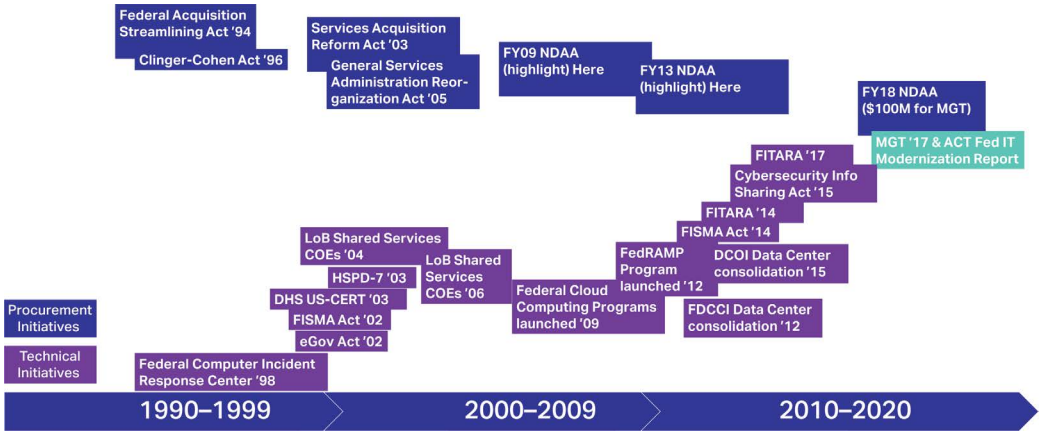


Figure 2. Convergence of Federal IT and Procurement Initiatives

MGT, Inflection Point or Blip on the Radar?

The MGT legislation passed with bi-partisan support at the end of last year as part of the National Defense Authorization Act (NDAA) (Gunter, 2017). MGT was spearheaded by Congressmen Will Hurd (R-TX) and Gerry Connolly (D-VA) and was a long time in the making. Unlike prior legislation, MGT does not provide an immediate large cash infusion, nor does it provide focus on a single innovation area like CloudFirst, MobileFirst, etc. Instead, MGT is ambitious in that its goals are to fundamentally change the Federal IT technical and cultural models that have led to the high O&M and low DME figures through pragmatic, incremental, data-driven, proof-of-concept projects that are scaled-up in subsequent projects over multiple years. Specifically, MGT does the following:

- Establish a federal government-wide working capital fund (WCF) that can act as seed money to invest in modernization
- Further strengthen the decision-making authority and accountability of Department and Agency CIOs over their budgets (in conjunction with their CFO partners)
- Direct federal departments and agencies to set up their own internal WCF funds
- Establish a Technology Modernization Board (TMB) that will oversee WCF-based project proposals
- Allow program dollars saved through WCF-based projects to be repurposed for other projects with latitude to expend those funds over a 3-year period
- Focus on projects that support modernization in the following areas:
  - Strengthening cyber security posture
  - Moving to cloud services
  - Supporting a 21st century Federal workforce

Projects will be graded higher if they can be shown to be best practices, can be delivered as shared services, or can be easily replicated by other departments and agencies.

To date, Congress has allocated $100 Million for MGT in FY18 and more funds are expected to be budgeted for FY19. The 7-member TMB has already been established (Chappellet-Lanier, 2018) with their first meeting completed in March 2018. The TMB has received nine requests for MGT funding from agency sponsors and already whittled them down to four projects (Byod, Technology Modernization Fund Board Picks First Projects to Advance, 2018). MGT, through the TMB, provides the seed funding (short term loans) and rule changes around how funds from annual budgets accrued through MGT and WCF related projects can be used for other projects over a 3-year period.

As with any set of policy recommendations from the White House, as well as the MGT act, it will be up to OMB to provide guidance. While some dates and directives have clearly been set forth by OMB [R] through the TMB, reprogramming approvals are still required.

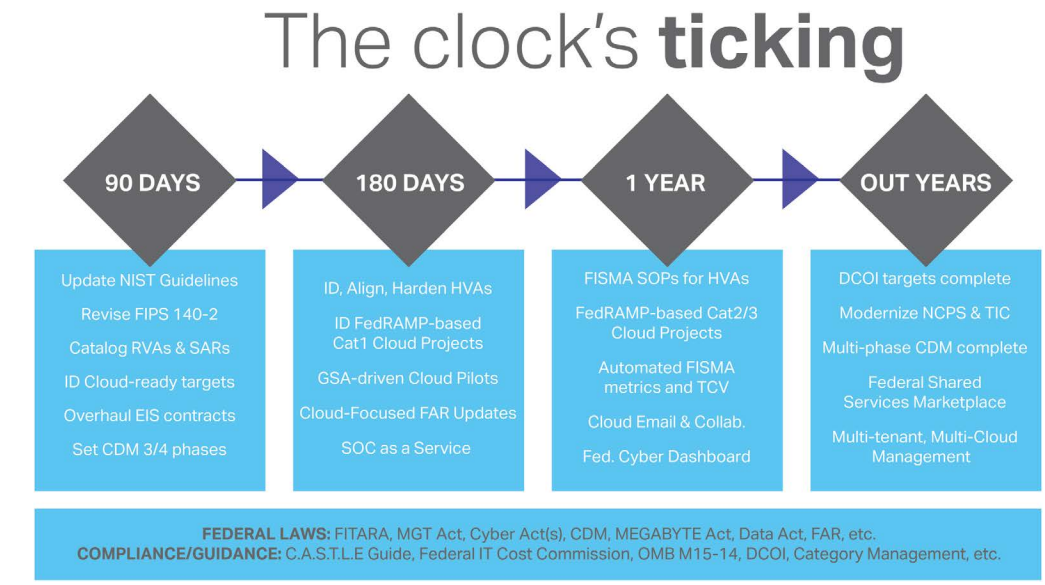


Figure 3. Summary of American Technology Council (ATC) recommendations noted in the White House publication

Figure 3 provides a collection of the recommendations issued by the American Technology Council at the end of 2017 in the Report to the President on IT Modernization (Council, 2017). As with any set of policy recommendations from the White House, as well as the MGT act, it will be up to OMB to provide guidance. While some dates and directives have clearly been set forth by OMB through the TMB, reprogramming approvals are still required (Mulvaney, 2018). Downstream Figure 3 delivery milestone dates are suggestive. Actual dates have not been determined across everything shown, and there may be delays or grace periods provided. Not all departments and agencies will progress at the same rate.

It is unclear the degree of interest individual Federal organizations will have in writing proposals against the current MGT TMF funds, given they are small loans, perhaps on average $500K to $1M, and must be repaid.

Getting the Most out of MGT

Many of the ATC recommendations are a natural evolution from mandates and initiatives undertaken by prior administrations. In aggregate, all prior guidance more than adequately defines "what" needs to be done and by "when," but often falls short on "how" it needs to get done. The "how" matters a great deal as it often makes or breaks implementation of strategy, uncovers dependencies, clarifies relationships, and generally determines success or failure.

It is unclear the degree of interest individual federal organizations will have in writing proposals against the current MGT TMF funds, given they are small loans, perhaps on average $500K to $1M, and must be repaid. For those that decide on submissions, it may make the most sense for them to focus on PoCs. For larger projects or PoCs, they may opt to transfer appropriated funds to their own departmental WCFs*, including O&M. No limit or approval is required, however you must report to OMB quarterly (increased compliance burden) on all plans (reprogramming, expenditures, project status etc.). The key question becomes, "How do departments and agencies get the most out of MGT?"

Grand Vision and Pragmatic Incrementalism Have the Same Starting Point

Proposals submitted for WCF consideration must address core modernization issues that produce predictable, quantifiable results within months. WCF funds cannot be allocated to projects that were previously requested but denied through the annual appropriations process, a restriction to avoid an end-around effort to work on projects explicitly denied by Congress. While the focus will be on PoCs, not just any PoC will do. It's necessary but insufficient for WCF proposals to solely address cloud migration, data center consolidation, cyber security improvements, or any other high-priority technical initiative. TMB will be looking for projects that drive cost savings and with a high probability of driving those savings faster than competing submissions. Over and above the technical and ROI considerations, CIOs and IT program managers must demonstrate that they have the program management skills, internal and external resources at their disposal, and track record of delivering high risk projects within cost constraints and project scope. It's not just a matter of collecting the "as-is" state from a technical perspective, or just to do a cost comparison on an individual asset comparison basis. It's a matter of looking at the topology, mapping the services, and developing a transition plan and a "blueprint" on what the end goal looks like, such that aggregate cost savings can be identified and submitted as part of PoC proposals. Prior track records and experience with this sort of analysis will weigh heavily in the decision-making process, as much as boldness of outcome for the least investment.

UNDERSTAND YOUR "AS-IS" STATE IN TERMS OF SERVICES DELIVERED, OUTCOMES, AND OPPORTUNITY COSTS

Some federal departments and agencies have made moderate progress over the last decade in understanding what assets they have and how those assets are associated with services delivered, but they still have significant ground to cover. Although a recent mandate required all departments and agencies to inventory and identify all high-value assets, the DHS CDM asset inventory exercise discovered that on

** Initially, agencies had until March 27th, 2018 to inform OMB how much they would be setting aside from their own WCFs*

average Federal IT organizations have 50% more IT assets than they knew about because they are unable to perform full, on-going, and comprehensive identification and classification of (Office, 2018):

- Compute platforms—not just those that reside in designated data centers, but end-user GFE compute platforms, systems outside of IT management control above the baseline infrastructure, and systems managed or identified as part of O&M contracts to any service provider or SI outside your organization.
- All software licenses owned and open source APIs (essentially all "In-Use" software covered by the Megabyte Act), including application development and IT operations management, as well as all API dependencies and proprietary code bases (often mislabeled as "free").
- Personal usage of cloud apps by employees for business purposes captured through user behavioral data.
- Data repositories, databases, and records management systems including their metadata and individual and enterprise-wide governance and compliance.
- All contracts and services that connect the assets together, IT staff supporting the assets, etc.

Once this more comprehensive accounting is performed, the next step is to determine which of these assets map to each service delivered, and that these services map to mission capability. If the "to-be" state is focused on shared services and migration to the cloud, a further required step is to assess the usage and cost of all your assets, tier them, understand their dependencies on each other, determine their utilization rates, and cost per increment of service delivered. Additionally, the "to-be" state must demonstrate an improved Cyber Security posture. You will also need to calculate High-value assets (HVAs) based on their mission importance and the impact an incapacitating cyber-attack would have on them, and the upfront cost to build remediation plans, governance policy implementation, and CDM versus the reduction in cost of a potential breach.

The culmination of this process places you in a position to rationalize in a top down fashion.

CLARIFY THE RELATIONSHIP BETWEEN CONTRACTING MODELS AND CONSUMPTION MODELS TO FULLY UNDERSTAND TCO AND ROI FOR CLOUD

Modernization exercises will need to be cross-functional, with inter-agency virtual teams performing comprehensive reviews of end-to-end cost, all contracts (including external networking contracts, for example TIC), and internal and external labor involved—not just systems and applications but development, operations management, and security (Government Accountability Office, 2018). For example, when making a cost comparison between an existing on-premise service deployed and what it would cost to move to Cloud, modernization teams will need to remember Cloud services require far more bandwidth in comparison to their existing, on-premise systems. Is there an existing network contract or cloud service already being procured by another Department or Agency? You'll need as much detail as possible about the cost of broadband associated with the service, outyear costs, costs of cancellation of existing contracts, and more. This total cost of ownership should even include the cost of shifting to a different cloud provider down the road, if necessary, avoiding the same vendor lock-in so common today. Vendor

Modernization exercises will need to be cross-functional, with inter-agency virtual teams performing comprehensive reviews of end-to-end cost, all contracts (including external networking contracts, for example TIC), and internal and external labor involved—not just systems and applications but development, operations management, and security.

Let's put this in practical terms. Just looking at services like email, network consumption, printing, and other very generic services represents 25—30% of budget spent on O&M contracts across the Federal government.

lock-in with Cloud services isn't just a contractual issue, SaaS offerings are often monolithic technology stacks. Subscription services may seem like a commodity, but shifting from one commodity stack to another isn't plug-n-play. There are costs associated with the replacement of the technology stack, which is usually financed overtime by the new SaaS contract, or required as an upfront setup fee. Leveraging IaaS and PaaS allows the government to select and own the technology stack and contract separately with vendors for services. This eliminates having to replace the technology stack and provides flexibility with future contracting alternatives.

This "As-is" state assessment will pinpoint where vendor lock-in exists, and when looked at across departments, how the cost of replacement may also be reduced by making the legacy to Cloud and Shared Services shift across organizations. Federal IT was amassed in fits and starts through cost-plus-fixed-fee (CPFF) contracts, and is now serviced through O&M contracts that are fixed-price contracts (FPC). The latter model being a response to issues around cost control and mission creep prevalent with the former. Unfortunately, a negative side effect is that many project managers tend to track contracts as cost, instead of actual cost mapped to outcome. In turn, if all their project costs are absolute rather than relative to outcome, it becomes difficult to incrementally scale down existing services. Some of these existing services and their related assets will remain "as-is" and contracts will need to be renegotiated and scaled-down (or replaced with another contractor). The goal should be to convert FPC to consumption-based O&M contracts, far more conducive to transferring savings to Cloud and IT Modernization.

From a technical standpoint this will require agencies to "Right-Size" the data center, often in two phases. The first is to quickly identify what can easily be consolidated, moved to VMs, automated, etc. and DCOI addresses this phase, emphasizing automation of datacenters and consolidation where appropriate (cost savings). The second phase is to perform application rationalization which gets to the heart of where and when you can combine services that may be on different technology stacks or code bases, focused on transforming outcomes. From a financial and contractual standpoint, far more could be saved if this exercise is performed across multiple departments with savings being reprogrammable across departments within the same year. This is currently not permitted.

Let's put this in practical terms. Just looking at services like email, network consumption, printing, and other very generic services represents 25—30% of budget spent on O&M contracts across the Federal Government (Mike Conger, 2017). These types of services and the redundancy in them is but the tip of the iceberg. CIOs and the program portfolio managers in their departments and agencies should also address large scale acquisition programs that are functionally the same, but may be on bespoke systems. For example, multiple HR, supply chain management, fleet management, records management, or development platforms as they are also ripe for consolidation, but require that second phase of consolidation, application rationalization to identify and address them properly. Often the programs and budgets associated with these functionally equivalent mission-related platforms are buried in department-level projects and not central IT. FITARA, however, provides the CIOs with the authority to consolidate these platforms into common service offerings and establish policies to force usage.

Cost Savings versus Risk Management versus Innovation

It's no secret that the TMB will be looking for quick wins. Many in the OMB have said so on the record. However, quick wins will still need to balance between the trinity of cost savings, risk management, and innovation. Further, the OMB has provided guidance for IT implementation projects under MGT (Mick Mulvaney, 2018). In this section we'll delve deeper into what's depicted in Figure 4 to determine where the "sweet spot" will reside on a balance of cost, risk, and innovation for proposed projects.

It's no secret that the TMB will be looking for quick wins. Many in the OMB have said so on the record. However, quick wins will still need to balance between the trinity of cost savings, risk management, and innovation.

UNDERSTAND THE GRADING CRITERIA FOR A SUCCESSFUL WCF PROPOSAL

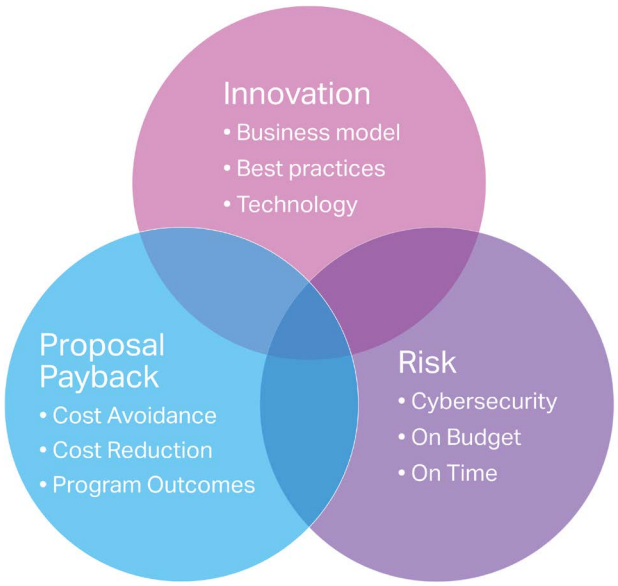


Figure 4. MGT/WCF Proposal Tradeoffs

There's no question that there will be countless projects for CIOs and program portfolio managers to choose from, a target rich environment, if you will. There will be some obvious projects that are called out as "no-brainers," like moving collaboration and productivity tools to Public Cloud.

We believe TMB proposal requirements will broadly fall into one or more of the areas in Table 1 on the following page. Clearly, there is overlap between these, and the submitter is more likely to be successful if they are achieving high marks in all five categories balancing across Proposal Payback, Risk, and Innovation as seen in Figure 4. Everyone will be competing for scarce dollars within their organizations and in requests to TMB which can easily result in overpromising and under delivering. Since many of the problems plaguing Federal IT organizations will be similar across organizations, it will be easy for proposals to look similar, addressing the same problems. With these potential scenarios in mind, it is important to do the following:

- Shore up any weakness—real or perceived—in your technical and managerial skills by partnering with other organizations in advance
- Balance aggressive proposals with near-term milestones you can easily hit
- If you're going to fail, then fail fast, and have a contingency plan that has already been broadcast to set expectations
- Ensure that those near-term milestones will return funds to your budget that are in your mission scope, such that you will be able to apply them for the 3-year period

Agencies are encouraged to review their existing agency-specific authorities to identify accounts with applicable transfer authority and submit the account names to their OMB RMO and OFCIO desk officer.

- Review your funding authorization and target areas where you have authority to transfer savings—sadly, this may exclude target rich program areas that can't be authorized for savings withdrawals
- Build a series of milestones in your program that continue to yield similar dividends and ultimately draw down your technical debt

In parallel with these more technical considerations, agencies will need to understand what is permissible under OMB guidance and their own Agency authorizations. The MGT Act does not confer transfer authority. Therefore, agencies may transfer funds to WCFs only if they have other authority that authorizes the transfer of such funds. Agencies are encouraged to review their existing agency-specific authorities to identify accounts with applicable transfer authority and submit the account names to their OMB RMO and OFCIO desk officer.

	Criteria	Example(s)	Impact(s)
Standardization	▪ Are you consolidating multiple services, tools, or infrastructure? ▪ Are you offering the service to IT groups outside your Department? ▪ Are you incorporating underlying programs into shared services?	▪ Move collaboration and productivity to Public Cloud ▪ Legacy ERP, Records Management, EDW retirement ▪ Cross agency consolidation in single Federal Agency or GSA ▪ Center of Excellence for Share Services	▪ Retires some systems ▪ Reduce software licenses ▪ Consolidate contracts ▪ Increases utilization of remaining systems ▪ Opportunity to move to Cloud ▪ Streamline process
Reusable	▪ Have you developed a best practice replicable outside your organization? ▪ Are you spurring innovation?	▪ Program and project management skills, reporting tools and methodology ▪ Using a rental car company to handle fleet management	▪ Better management and cost control ▪ Improved intra-agency collaboration
Payback	▪ Will the project yield incremental quantifiable outcomes? ▪ Will the project drawdown technical debt, reduce O&M?	▪ Eliminate old network (MPLS) contracts and replace with SDWAN-based contracts ▪ Reduce unused software licenses ▪ Increase VM use, re-orchestrate, automate	▪ Proper broadband for Cloud ▪ Additional budget for innovation ▪ Reduced compliance exposure for software licenses ▪ Reduce contract burden
Security	▪ Are you protecting your HVAs associated with your project proposal? ▪ Are you moving into subsequent CDM phases?	▪ Implementing a CDM program ▪ Developing a Security Operation Center as a Service	▪ Reduced security risk ▪ Improve time to respond and time to recover
Risk	▪ Do you have a track record of hitting your milestones on time within budget? ▪ Do you have modern project management staff/skills? ▪ Does you project have a long-term vision with incremental results that start within months?	▪ History of transparency and improvement over time in FITARA, PortfolioSTAT, TechSTAT, etc. ▪ Few cost overruns on projects ▪ Already on a trajectory to reduce O&M	▪ Increased likelihood of success ▪ Quick wins that can be reported back to congress ▪ Increased funding of MGT in the outyears ▪ Snowball effect on technical debt reduction

Table 1. TMB and WCF proposal prioritization and selection considerations

ACHIEVING AN "UNDER-PROMISE AND OVER-DELIVER" TRACK RECORD STARTS WITH QUICK WINS AGAINST A LONG-TERM PLAN

CIOs and IT program managers will need to perform a skills and resource assessment to ensure that through some combination of in-house and external resourcing they have the right skills and supporting toolset to quantify, track, and verify expected savings at each milestone gate. Projected work completion at each milestone, and savings associated, must be clearly defined. Not just in the near-term, but into the out-years as well. Part of this exercise will be for CIOs and IT program managers to work with their financial management counterparts to review their own track records and determine how successful they were in prior projects at generating savings. They will need to work with their line managers, down to individual contributors and their HR representatives, to understand what skills their teams have, and how these skillsets stack up against other Federal IT organizations, 3rd party contractors, and commercial industries where the type of work and project roles are equivalent.

For some CIOs and IT managers, the correlation of costs and outcomes may pose a challenge, as not all of them are tracking cost or cost savings today, instead, they track the cost towards major programs and contracts. Furthermore, many of them lack visibility into resources, since these are outsourced to contractors. Tracking time management in a granular fashion is another area ripe for improvement due to a dearth of Project Portfolio Management tools. The contractors mirror this deficit of granular tracking as they are required to report EVM expenditures in accordance with FAR requirements (FAR 15) at a contract level, but not at the program or project level. Acquiring the right tools will partially solve the problem, but the rest will require culture changes that, more than likely, will start as part of the PoCs funded by MGT, instituting new policies to track time, resources, and cost. Over time, all IT Modernization projects can adopt the new project management process that is focused on cost/risk and performance.

Increasingly, in accordance with new FITARA mandates, CIOs and IT managers will need to review their "as is" state assets in the context of each planned proposal to ensure that they can eliminate duplicate assets services. For example, in addition to a full accounting of what software an organization has (licenses and SaaS contracts), shadow IT must also be accounted for, ranging from improper use of VMs to end-user employees using informal tools, like Dropbox, for business purposes. As touched on earlier, Government asset management practices typically find 15—20% of software licenses are out of compliance (Government Accountability Office, 2016). IT management doesn't always know what's being run in their departments because they don't have continuous monitoring tools and are often relegated to performing periodic manual inspections.

One of the most common proposals will be consolidation initiatives, often including new hardware requests. New hardware acquisitions will increasingly trigger reviews of existing virtualization ratios. It is critical that CIOs and IT managers document the extent to which they are taking advantage of their existing resources. Typically, a 15:1 or 20:1 consolidation ratio, meaning 15 to 20 VMs running per CPU, is considered state-of-the-art in Federal IT Data Centers. For resources associated with a project that are below this average,

Increasingly, in accordance with new FITARA mandates, CIOs and IT managers will need to review their "as is" state assets in the context of each planned proposal to ensure that they can eliminate duplicate assets services.

It's not just a matter of your track record, but what the track record is for your proposed partners, Systems Integrators (SIs), Service Providers (SPs), core technology vendors, etc. TMB reviewers will not get directly involved in contracting decisions and most likely will only review proposal past performance based on PortfolioSTAT reviews of cost and schedule.

the first milestone should be improvements in virtualization ratios on your existing hardware. This can be accompanied by identification of shared service opportunities where additional instances of existing applications are moved into the targeted set of hardware. Additionally, automating provisioning, employing tools that improve monitoring, and measuring operations can also help to pinpoint and verify savings.

Broadly, there are several areas where quantifiable savings can be achieved by these types of projects including:

1. Hardware and Software Virtualization
2. Software Rationalization
3. Application Rationalization
4. Storage Optimization
5. IT Tool Consolidation/Automation
6. Business Process Rationalization within mission programs, provided the agency has authorization to transfer these funds to the WCF.

It's not just a matter of your track record, but what the track record is for your proposed partners, Systems Integrators (SIs), Service Providers (SPs), core technology vendors, etc. TMB reviewers will not get directly involved in contracting decisions and most likely will only review proposal past performance based on PortfolioSTAT reviews of cost and schedule. However, for large SI- or SP-driven programs, CIOs and IT program managers would be wise to assess how well these partners were managed, what skills and tools were used to manage them, how often budgets were maintained, and timelines were met. In some cases, even where departments or agencies have a great track record with an SI/SP on an existing project, the shift to Cloud, or new technologies like SDWAN may require using a new contractor (perhaps a different SI/SP or shift from one to another) and winding down existing contracts as a means of funding the new work. Federal IT groups making proposals will need both contractual expertise and technical expertise to determine who should receive the modernization contract. Contract experience will be needed to figure out how to cancel or renegotiate project scope and size to create funds to support a PoC. Let's say that PoC is to move away from low-bandwidth, expensive MPLS, to less expensive, higher-bandwidth SDWAN. In addition to contractual expertise, the Federal IT project management team (or a set of third party consultants—still managed by a technically savvy Federal IT group) will need to balance the tradeoffs between existing knowledge of network topology, security, and workloads that the incumbent contractor has against demonstrated success other contractors will provide as part of their bids.

Many agencies typically report cost and risk metrics through the IT Dashboard, but do not have real cost controls in place, and therefore, are not equipped to handle modeling these tradeoffs to evaluate where they can save costs. It may make sense for these agencies to propose an outsourced Project Management Office (PMO) with the right oversight experience.

In all the cases above, there is an opportunity to move to consumption-based models. However, moving to Cloud, SaaS, or any other OPEX vehicle requires a full analysis of the ROI and TCO to compare the existing

environment and the new proposed environment. This analysis must be used to determine what type of savings you have: cost reduction (immediate cost savings) or cost avoidance (longer-term reductions in fixed and expected expenditures)? OMB has provided some guidance on the difference between the two, but only the Agency IT managers can answer how to perform the cost estimation that will identify what type and how much of it will be generated. Initially, cost reduction is the preferred outcome, and therefore consumption-based projects must demonstrate lower cost, dollar for dollar, than the O&M on existing services delivered. It's not just that the Cloud is cheaper than replacing the systems in the near- to mid-term, but in the out years as well. Better yet if the aggregate positive difference in cost generates a cost avoidance. There is some chance this cost avoidance can be transferred into subsequent year budgets as savings. Keep in mind, though, cost avoidance will not free up funds for repayment of the WCF borrowed in the first year. Therefore, it is not a good first or second milestone project. If, on the other hand, the new SaaS, PaaS, or IaaS project is replacing existing systems within the reporting period, and reducing project spend, then it's a cost reduction that can be funneled back into payments for the WCF. This presupposes that the agency has provided a list of appropriated funds that are being targeted for potential savings and received confirmation from OMB that they have the authority to transfer funds between appropriated areas. If OMB has green-lighted the plan, agencies can use these additional funds to save on new projects or as seed money to further shift other legacy systems and O&M off the books. If this cycle is spun up and proven, there will be massive incentive to consolidate and build shared services.

The goal of MGT Act was to push for Cyber and IT Modernization projects that are "NOT" funded already via the normal appropriations channel. This is perfectly reasonable given that in comparison, new funds allocated for Cybersecurity work dwarf MGT allocations included in the same Omnibus bill.

CYBER SECURITY IS A MANDATE THAT ADDRESSES BOTH COST AND RISK

As mentioned above, the TMF has been allocated $100M for the current fiscal year (roughly 40% of an initially small request, but more is expected later in 2018 and 2019), and it's expected that the average project budget awarded will be $5M broken out in bitesize chunks. Cybersecurity is a key objective for the MGT act, as explicitly stated above and in recent statements in Congressional MGT reviews (Hurd, 2017). However, the goal of MGT Act was to push for Cyber and IT Modernization projects that are "NOT" funded already via the normal appropriations channel. This is perfectly reasonable given that in comparison, new funds allocated for Cybersecurity work dwarf MGT allocations (Miller, 5 ways the 2018 omnibus promotes IT modernization, cybersecurity, 2018), included in the same Omnibus bill:

- Homeland Security Department received $722 million with a separate $102M specifically for the next phases of the Continuous Diagnostics and Mitigation (CDM) program
- National Cybersecurity and Communications Integration Center received $244 million
- National Cybersecurity Protection System received $292 million

All three of these organizations, and the over $1B in this fiscal year under their auspices, will address government-wide cybersecurity deficiencies, spearheaded by US-CERT within DHS (United States Computer Emergency Readiness Team, 2018), with extension to commercial industry cyber threat protections under the critical infrastructure umbrella. With an order of magnitude more funds already being dedicated to direct Cybersecurity investments, how would $100M in MGT funds, or contributions at the Department level, make sense? Is there a relation between the two? Should CIOs and IT project managers propose Cybersecurity projects during the first year?

Most cybersecurity projects are perceived to be cost avoidance, not cost reduction. This perception is unfortunately misleading.

Far more substantial is the direct accountability for senior department and agency heads, including when, to whom, and how reporting will be handled. Guidance was laid out in last year's executive order on Cybersecurity (Mick Mulvaney, 2017) and complementary recommendations in the President's Report on Federal IT Modernization mandate innovations such as a shift to next-generation network protections, CDM, and end-point security, or changing to risk-based assessment of all operations and identification of HVAs with governance plans and remediation scenarios. The combination of funding for cybersecurity and guidance to exactly how it should be addressed is more than adequate. Thus, while the spirit of MGT should address Cybersecurity, the MGT funds allocated should directly address modernization of the systems and HVAs associated with Federal Networks and Critical Infrastructure, where possible, rather than bolstering antiquated systems. Also, given the number of expected proposals, the need to address all three areas—Proposal Payback, Innovation, and Program Risk—at the intersection point between the three, means that proposals that focused solely on Cybersecurity run the risk of missing the target on proposal payback as it pertains to cost savings in the form of real reductions.

There will be instances where direct cost reductions can be found when looking solely at IT Modernization from a Cyber Security vantage point. For example, if CIOs and IT managers can work with their CISOs and their subordinates to consolidate security operations centers, or support a smaller agency with a SOC as a service, and request funds used by that agency to be transferred to their budget, then there would be direct cost reductions. However, in many cases, the program for modernization would need to replace a legacy system or shift to Cloud, and in turn, as a byproduct of this effort, generate savings by removing the need for more costly, aging firewalls, or other perimeter defense systems. Similarly, the cases described above for IT Modernization involving Data Center operations would have parallel contractual consolidations and eliminations that should also be considered on the security front. Let's take the MPLS to SDWAN example above and look at it from a security perspective. There may have been a contract in place, direct hardware ownership of aging firewalls, or other intrusion detection systems with service and maintenance contracts tied to them. These systems, or that part of the existing contract, can now be replaced, leading to direct cost reductions.

Most cybersecurity projects are perceived to be cost avoidance, not cost reduction. This perception is unfortunately misleading. Unlike the examples provided above for IT Operations, in the case of cybersecurity, reducing cost avoidance can be cost reduction. Consider this: the bulk of Cybersecurity expenditures at the department and agency level are unplanned and reactive, often in response to compliance violations (or worse), identified attempts, and discovered breaches. Costs associated with cybersecurity expenditures are often out of project scope, accounted for in hindsight, and therefore hard to associate with annual budgets and associated classification as cost reductions. However, if CIOs, in conjunction with their CISOs, can shift focus to more proactive measures, then the cost associated with this approach can reduce the cost of incident response, mitigation, credit, and identity protection.

The good news is virtually every modernization project will indirectly lead to proactive cybersecurity improvements that can be clearly identified, and cost avoidance and reduction incurred. In some cases, cost reductions through the elimination of existing security measures associated with legacy systems and contracts can be achieved. Prior government studies (Alexander Heid, 2018) have found that a large swath of HVAs identified as having the highest risk of exploitation are aging systems with known vulnerabilities, many of which have patches, but many others are simply unknown. For example, if an ancient agency system is running assembly, it is extremely difficult, if not impossible, to fully identify every point of vulnerability. Part of the problem is lack of skilled resources that match the task. There is not exactly a glut of "white-hat" ethical hackers available to test for new attack vectors against many of these old systems running Cobol or interfacing through X.25 packet-based communications channels. In proposing legacy migration, data center consolidation, scope-reduction, or retirement of existing contracts, proposals should include the following with respect to indirect, but quantifiable Cybersecurity improvements:

- Identification of HVAs' location, operational process, remediation plans, and more for their "to be" state at each project milestone point
- Legacy modernization programs that remove aging systems and proprietary monolithic software stacks that are designated as, or related to critical infrastructure as defined by HSPD-7 (FAA, Electric Grid, etc.)
- In addition to the security risk assessments you make in your proposals for data center consolidation or legacy migration, look to calculate the per end-user, end-point security posture improvements inherited by the move to Cloud compounded by the number of uses.

It's worth mentioning that in parallel to the HVA identification exercise, many Federal IT practitioners are being asked to review and improve their disaster recovery plans with an emphasis on understanding how to reconstitute their environments, inclusive of any cybersecurity forensics that support estimation of the cost of an attack. For example, say a delivered service has a system with 50,000 users. If breached, the deleterious effects must be included in the DR plan. Likewise, a full accounting would also require cost estimation for incident response and handling, a cost to not just reconstitute the system but even the tools supporting it, all the labor involved, and essentially everything in the incident response lifecycle. Going forward, MGT modernization proposals should support reductions in the cost of incident response, another quantifiable cost avoidance line item.

It's worth mentioning that in parallel to the HVA identification exercise, many Federal IT practitioners are being asked to review and improve their disaster recovery plans with an emphasis on understanding how to reconstitute their environments, inclusive of any cybersecurity forensics that support estimation of the cost of an attack.

Fostering Durable Change

For the past two decades there has been a steady drum beat, growing louder with every IT advancement and digital transformation of every facet of business in our day-to-day lives. Federal IT should deliver services akin to those delivered by commercial entities. It's surprising to see that there's no guarantee that CIOs and key IT program managers responsible for the bulk of Federal IT budgets will apply for MGT

"All you can do is give the carpenter the tools"

RICH BEUTEL
Cyrrus Analytics Principal who helped draft the FITARA legislation as a senior staffer on the House Oversight and Government Reform committee

funds or take new directions. For instance, one former CIO said "The repayment thing, I think, is daunting to some CIOs whose plates may be full of lingering open oversight recommendations and pressure to improve Federal IT Acquisition Reform Act scores. Not because they don't understand it or can't figure it out. They're uncertain about how to figure out a project that would enable enough combination of savings" and efficiency that they can pay back within the three-year window." (Gunter, 2017)

Expectations for MGT cannot be set in isolation. MGT will only be successful in conjunction with other funding mechanisms and initiatives, improvements to transparency, accountability, and trust between Congress, OMB, department, and agency personnel. We conclude this paper by exploring what can be done to foster lasting change.

Transparency, Accountability, and Trust

Let's face the issue head on. Why is there a lack of transparency, accountability and trust? GAO reports issued over the past 30 years have unearthed many large cases of waste and abuse, internal to government organizations, by contractors, and as team activities (Office, G.A., 2017). Over time, layers of rules were put in place to curb these problems, and in turn, created some of their own.

During the 70s, 80s, and early 90s cost overruns were pandemic and, as a result, Federal acquisition policies were changed to emphasize fixed-price contracts (FPCs) over cost-plus-fixed-fee (CPFF) contracts. CPFFs facilitated too many changes with little oversight or consistency in process to support changes. FPCs were implemented to curb cost overruns by instituting very tight spending limits against SOWs and stringent oversight on how much of a project can be reprogrammed or rescoped—either as expansions or contractions. The intent behind boxing program managers into these financial limitations was to prevent cost overruns associated with scope expansion, as well as hording funds for other projects in out years through scope contractions. Further, rule changes were implemented that limited expenditures to the same year as appropriations. Generally, only 5% of annual funds can be reprogrammed on any given project without significant interaction and approvals with OMB or other oversight organizations.

The positive effects of these mandates and guidelines has been a steady reduction in overruns, mission creep, and banking of funds (shadow books) over successive years. The negative side effect is that without the ability to change scope and the majority of IT portfolio managers' funds tied up in these annual FPCs, there is little chance of finding cost savings that can be devoted to modernization and innovation. An agency has to obligate funds to a contract vehicle before the end of the year, rather than multi-year, an extra measure of fiscal prudence. This forces them to decide how to spend the money by year end (on a GWAC or IDIQ for example). The net effect has been the creation of a use-it-or-lose-it culture. In parallel, with little available for modernization or innovation, and most funds tied up in 3rd party vendor contracts, skill sets tend to self-select, matching the types of contracts and the level of technical sophistication necessary to run them.

With MGT, the TMB and Departmental WCF review structures erected and the programs selected, coupled with changes in program and contract management tools, internal IT culture and vendor relations, and contractual models should counterbalance the institutional emplacements and their side effects, enabling CIOs and IT portfolio managers to spend their budgets wisely, optimizing for cost reductions, and avoidance as well as innovation over multiple years. With more innovation and the development of CoEs, CIOs, and IT managers should also be able to find funds and attract the best and brightest from across the government, as well as from private industry. Adjusting contracts to be consumption based with funding caps would spur further chances of success. This may require that the government agrees to buying thresholds to achieve discount targets.

Savings in the form of cost reductions in programs associated with MGT can be reprogrammed over a three-year period. Additionally, if cost reductions in a given year lead to cost avoidance in one or more successive years, and those savings are still by and large deposited against expanded scope or scale, with existing projects or to new projects, then a "snowball effect" will commence. The key will be to start with quick wins as described above that lead to clear-cut cost reductions with follow-on multi-year cost avoidance as a by-product. The project management skills, reporting methodology, changes to internal operations, contract models, and tools necessary supporting these changes should deliver transparency and accountability that reduce risk and give the TMB confidence to recommend that Congress deposit more into the TMF. When OMB and department and agency executives then reward CIOs and IT program managers with budgetary support, career acknowledgement, and public praise, a bank of trust will be built. In other words, trust is bi-directional, earned over time, and no one should expect it to be blind and up front.

Trust may be a general feeling, but there are always specific lynchpins it rests upon. For example, there is often resistance to shared services, justified through a general push back of "my requirements, skills, contractor relationships, and related contracts are unique." These assertions must be taken head-on by better defining services and assets associated with them, building modularity and granularity into those services, and separating out what is unique to an organization and what can be incorporated into a shared service. Incrementally building and proving out this migration to shared services can build trust in a roadmap for moving the vast majority of functions to shared services over time. Programmatically turning that agreement into what each party is accountable for, and what and how both parties transparently view operations, requires a common operational picture (COP) which, in turn, requires a common set of skills, tools, and data (financial and technical) to both set up the COP, as well as define the metrics and populate them with data for agile, continuous decision making.

The TMB should incorporate the same COP into all their approved projects and publicize project success in dollars saved or risk averted. Additionally, success should be measured in what it delivers as best practices to downstream PoCs funded at subsequent milestones and new projects, including baseline grading, and methodology-used for on-going project and program management health. It's one thing to tell CIOs and IT portfolio managers to "fail fast." It's another to give them actionable advice on what that means. Quantitatively defining what missing your milestones means, with respect to the degree to which timelines are not met, cost overruns transpire, and at what point that should be considered within a

Trust may be a general feeling, but there are always specific lynchpins it rests upon. For example, there is often resistance to shared services, justified through a general push back of "my requirements, skills, contractor relationships, and related contracts are unique."

Micro Focus Government Solutions has spent decades working with both Federal IT and private sector large enterprise on their toughest legacy migrations and digital transformation projects.

margin of error and acceptable or unacceptable failure. The TMB will need to define what are acceptable and expected corrective actions for each project milestones, if not in advance, then during the reporting communications. What are acceptable Plan B approaches, how many strikes have they given other teams before replacing them, what's considered acceptable mitigating circumstances, etc. should all be transparent. Of course, it's easier over time building up a library of cases, but that compilation should be a predetermined goal of the TMB.

Shared Services Based on a Business-Driven Service-Brokering Model

In the one thousand Federal vacation tool application example, we suggested that if we could eliminate say 10% of the duplication through an MGT PoC, then we could declare victory—at least for initial PoC projects in the first year. What about the other 900? How do we go about reducing these? Most likely, these would be addressed in subsequent MGT programs as higher risk, but higher yield projects. Chances are some of these bespoke applications. The most archaic of them, for example—are monolithic, tightly integrated legacy architectures, not easily tackled by simply pooling existing or reduced licenses in a consolidated data center or highly virtualized machines. Many of these will need to undergo a more extensive application rationalization program, where business processes are decoupled from the code and examined against modern requirements and desired outcomes. This may lead to incremental changes to legacy HVA's that drive cost savings. For example, shifting DevOps off the mainframe to save money on MIPs. This does not retire the mainframe, just makes it more cost effective, and could lead to potential for consolidation of remaining applications on to fewer remaining mainframes—directly leading to cost reductions. For even higher yield, the Ops side of the DevOps would be placed in the Cloud on modern platforms, a longer term and heavier investment.

Micro Focus Government Solutions has spent decades working with both Federal IT and private sector large enterprises on their toughest legacy migrations and digital transformation projects. Based on this experience in both environments, there are clear parallels in terms of lessons learned as well as blue prints for success. In this section we look at a basic model that can ensure MGT project selection, management, and expected outcomes are stimulating innovation and reducing stagnation.

STEP ONE: INJECT MISSION OBJECTIVES INTO THE IT OPERATING MODEL

Injecting mission objectives would start with a managed and metered Service Model approach against a set of duplicative services, taking a Project Portfolio Management approach where the following steps would be executed:

- Start with the HVA's and define all inter-dependencies, services and data relationships, and again, look for redundancy and consolidation opportunities
- Breakdown redundant service offerings, map what is common across them and bespoke by department and contract associated, consolidate the common services, and eliminate the underlying components where possible
- Re-evaluate what's bespoke against mission objectives and what is required for enterprise cross cutting services that all can share

- When cost effective (based on cloud 1st guidance), build out new infrastructure
- The positive impact of this approach is to deliver a standards-based operating model that shifts IT from factory design to value delivery. With the proper cost estimation and cost control tools integrated into your Application Delivery Management, IT Operations Management, and Security Operations Centers you can erect ERP-like functional flow, improve financial control and enable fine-grained, usage-based chargeback, an essential part of creating an apples-to-apples comparison of your "as-is" state and your "to-be" state. This is mandatory, regardless of whether it's on-premise, private cloud, public, or—more than likely—Hybrid cloud.

STEP TWO: ESTABLISH YOUR IT OPERATING MODEL ON TOP OF A STANDARDS-BASED IT VALUE CHAIN

Once you've established your value to cost measurements and laid out your project plan, you will need to adopt a Value Chain for IT to ensure alignment throughout the project lifecycle, and across a project portfolio against business requirements and a reference architecture. An example of an IT Value chain is shown in Figure 5 (Mark Smalley, 2018). It should leverage an open standard RA that has cross industry use to open Federal IT to cross pollination of ideas and talent. Building agile, repeatable PoCs requires a repeatable process, and this is achieved through repeatable "Value Streams" as seen in Figure 5. The Value Streams describe the core life cycle phases of the IT value chain as:

- **Plan**
  - Ensure business strategy and desired outcomes lead to the optimal IT portfolio
  - Capitalize on quick cost savings (ITAM/SAM, App Rationalization)
- **Build**
  - Streamline requirements to build and deploy new services, and focus on composable microservices instead of larger, slow moving services
  - Implement Robust Discovery and establish a full topology CMDB
- **Deliver**
  - Accelerate requests to streamlining the supply-chain to fulfill them
  - Integrate security into core IT Operational processes for change/incident management
- **Run**
  - Avoid failure by detecting and correcting issues proactively through improved root cause analysis that addresses both MTTR & Cyber security

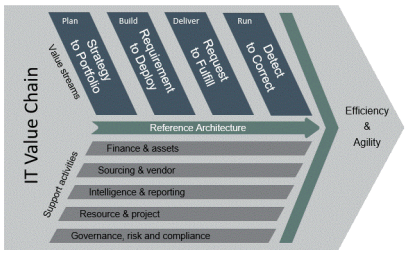


Figure 5. IT Value Chain for Program Portfolio Management

The Value Streams and the RA are applied by project with a set of supporting activities listed in Figure 5. This set of supporting activities facilitate business case creation and execution, but rely on a set of tools. Without the right set of tools, it's very difficult to measure progress or to collaborate and communicate successfully.

Once you've established your value to cost measurements and laid out your project plan, you will need to adopt a Value Chain for IT to ensure alignment throughout the project lifecycle and across a project portfolio against business requirements and a reference architecture.

The oversight necessary to institute top-down risk management, enterprise-wide GRC, and shift to a continuous improvement model will require CIOs to increasingly have the power and resources to drive top down change. MGT can serve as a rallying point, but change will not happen overnight. Prioritization and waves of PoCs, increasing in scale and risk, but also in positive returns, will be the best approach.

STEP THREE: MAKE IT RUN LIKE A BUSINESS

Steps one and two provide a standard taxonomy, model, and management system for IT costs, resources, and services so that IT leaders, CFOs, and other stakeholders use the same language and methodology to evaluate and improve cost for performance, paving the way for IT run like a business. But there are fundamental shifts needed in how IT operates as a business including the following:

- Implement a top down risk management and fix what matters first
  - Identify the critical risks that impact mission effectiveness
  - Define what services/controls are required for the mission
  - Identify and fix issues with critical controls and HVA's and services first
  - Implement new controls and services as required for real-time situational awareness
- Establish Department, Agency, and Government-wide, transparent governance, risk management, and compliance
  - Establish enterprise governance and compliance standards
  - Evangelize change management, asset management, and Release Control gates for all types of change
  - Integrate security processes into release management (DevOpsSec)
  - Publicly celebrate success stories—wall of fame but also expose bad actors—wall of shame
- Measure and continuously improve
  - Use data analytics to measure what matters to the mission (at the point of action where possible)
  - Measure and continuously improve IT development, security, and operational processes overtime
  - Rationalize, automate, and shift to shared services when cost effective
  - Communicate success and collaborate

The oversight necessary to institute top-down risk management, enterprise-wide GRC, and shift to a continuous improvement model will require CIOs to increasingly have the power and resources to drive top down change. MGT can serve as a rallying point, but change will not happen overnight. Prioritization and waves of PoCs, increasing in scale and risk, but also in positive returns, will be the best approach.

Glossary

Acronym	Term
ATC	American Technology Council
CAPEX	Capital Expenditure(s)
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CMDB	Configuration Management DataBase
CoE	Center of Excellence
CPFF	Cost Plus Fixed Fee
DARPA	Defense Advanced Research Projects Agency
DCIO	Data Center Infrastructure Optimization
DME	Development Modernization and Enhancement
ERP	Enterprise Resource Planning
FAR	Federal Acquisition Regulations
FedRAMP	Federal Risk Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FITARA	Federal IT Acquisition Reform Act
FPC	Fixed-price contract
GAO	General Accounting Office
HVA	High-Value Asset
IaaS	Infrastructure As A Service
MGT	Modernizing Government Technology
MPLS	Multi-Protocol Label Switching
MTTR	Mean Time To Repair
NCPS	National Cybersecurity Protection System
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OMB	Office of Management and Budget
OPEX	Operations Expenditure(s)
PaaS	Platform as a Service
PoC(s)	Proof of Concept(s)
RA	Reference Architecture
ROI	Return on Investment
RVA	Risk Vulnerability Assessment
SaaS	Software as a Service

SAR	Security Architecture Review
SDWAN	Software Defined Wide Area Network
SI(s)	Systems Integrator(s)
SOC	Security Operations Center
SOPs	Standard Operating Procedures
SP(s)	Service Provider(s)
TCO	Total Cost of Ownership
TCV	TIC Compliance Validation
TIC	Trusted Internet Connections
TMB	Technology Modernization Board
TMF	Technology Modernization Fund
VM(s)	Virtual Machine(s)
WCF	Working Capital Fund

References

Bur, J. (2018, February 27). *How agencies can request funds to replace legacy IT systems*. Retrieved from Federal Times: **www.federaltimes.com/it-networks/2018/02/27/agencies-to-begin-submitting-mgt-funding-proposals/**

Byod, A. (2018, April 19). *IRS' 60-Year-Old IT System Failed on Tax Day Due to New Hardware*. Retrieved from NextGov.Com: **www.nextgov.com/it-modernization/2018/04/irs-60-year-old-it-system-failed-tax-day-due-new-hardware/147598/**

Byod, A. (2018, April 22). *Technology Modernization Fund Board Picks First Projects to Advance.* Retrieved from NextGov: **www.nextgov.com/it-modernization/2018/04/technology-modernization-fund-board-picks-first-projects/147624/**

Chappellet-Lanier, T. (2018, March 1st). *Here's who's on the Technology Modernization Fund*. Retrieved from FedScoop: **www.fedscoop.com/omb-technology-modernization-fund-board-members/**

Council, A. T. (2017, December 13). *Report to the President on Federal IT Modernization*. Retrieved from CIO.GOV: **https://itmodernization.cio.gov/**

Donald J. Trump, POTUS. (2017, May 11). **Whitehouse.Gov**. Retrieved from **Whitehouse.Gov**: **www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/**

Goldstein, P. (2018, March 20). *USDA's Sheridan: Cloud Is the Way Out of Infrastructure 'Death Spiral'*. Retrieved from FedTech: **https://fedtechmagazine.com/article/2018/03/usdas-sheridan-cloud-way-out-infrastructure-death-spiral**

Government Accountability Office (GAO). (2016). *Federal Agencies Need to Address Aging Legacy Systems*. Washington DC: GAO. Retrieved from **www.gao.gov/assets/680/677574.pdf**

Gunter, C. (2017, December 12). *The MGT Act is law. Now what?* Retrieved from Federal Computer Week (FCW): **https://fcw.com/articles/2017/12/13/modernization-whats-next-gunter.aspx**

Mark Smalley, A. B. (2018, January). *IT4IT™ Business Value, Delivering Business Value with IT*. Retrieved from OpenGroup.Org: **https://publications.opengroup.org/white-papers/w183**

Mick Mulvaney. (2017, May 25). *Reporting Guidance on Executive Order for the Strengthening of Cybersecurity for Federal Networks and Critical Infrastructure*. Retrieved from **Whitehouse.Gov**: **www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf**

Mick Mulvaney. (2018, February 27). *M-18-12 Implementation of the Modernizing Government Technology Act*. Retrieved from **Whitehouse.Gov**: **www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf**

Miller, J. (2018, March 26). *5 ways the 2018 omnibus promotes IT modernization, cybersecurity*. Retrieved from Federal News Radio (KTOP): **https://federalnewsradio.com/reporters-notebook-jason-miller/2018/03/5-ways-the-2018-omnibus-promotes-it-modernization-cybersecurity/**

Miller, J. (2018, March 5). *Advice to CIOs: 'Don't pooh-pooh the IT modernization guidance'*. Retrieved from Federal News Radio (KTOP): **https://federalnewsradio.com/reporters-notebook-jason-miller/2018/03/advice-to-cios-dont-pooh-pooh-the-it-modernization-guidance/**

Singer, P. (2014, January). *Federally Supported Innovations, 22 Examples of Major Technology Advances that Stem from Federal Research Support*. Retrieved from **www.sciencecoalition.org/downloads/1390490336mitpetersingerfederallysupportedinnovationswhitepaperjan2014-21.pdf**

United States Computer Emergency Readiness Team. (2018, April 20). **www.us-cert.gov**. Retrieved from DHS US-CERT: **www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf**

Learn More At
www.microfocusgov.com/

www.microfocusgov.com/

MICRO FOCUS
Government Solutions