Testimony of:
Alfred Grasso
President and CEO, The MITRE Corporation
to the
US SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
on the subject of
"Examining the President's Plan for Eliminating Wasteful Spending in Information Technology"
APRIL 12, 2011

Chairman Carper, Senator Brown, and honorable members of the Subcommittee, thank you for the opportunity to appear before you on this important topic. My name is Alfred Grasso, and I am the President and Chief Executive Officer of The MITRE Corporation. Our company's 50 plus years of experience, contributions, and accomplishments have given us a perspective that I believe is highly relevant to today's topic of information technology planning and management. From the early days of the SAGE air defense system to present day deployment of advanced command and control and business systems, MITRE has been witness to great successes and significant disappointments in the acquisition and deployment of advanced information technology (IT) systems. We are honored to be asked to share our thoughts on the direction of IT reform in the federal government with your subcommittee.

You may know that MITRE is a not-for-profit corporation, managing five federally funded research and development centers sponsored by the U.S. government. Our organizational structure demands that we remain conflict free, do not manufacture products, and do not compete with industry. In this way, MITRE is able to provide objective assistance to the government and work on programs for our government sponsors with the primary motives of achieving established program outcomes, and being good stewards of public funds. It is these motives that bring me here before you today.

Information technology-intensive programs operate in an environment of rapid technology evolution where new generations of technology are introduced in months rather than years. Unfortunately, current federal acquisition processes and budget cycles are not well matched to these timelines, thereby causing some technology components to become obsolete while the program is still in development. To compound matters further, IT investment decisions are often made against a backdrop of rapidly evolving policy decisions, mission priorities and business needs. This pace of change challenges federal IT programs to keep their technical skill base current. All of these factors conspire to undermine the transformative potential IT holds for our government and the public. The answers to these problems are not easily found, but it is essential that steps be taken to begin turning the tide.

OMB's 25-point plan is a positive step in the IT reform process. In addition to OMB's activities, others across the federal civilian and defense sectors are also striving to find solutions to these challenges. As a personal example, I had the privilege to co-chair the Defense Science Board Summer Study on enhancing military adaptability last year. It should not be surprising that the observations and recommendations made in that study align closely with those expressed here. Adaptable systems, processes and people are critically important in an environment that is rapidly changing.

As I observe the state of IT management in the federal government, I am struck by the amount of attention paid to failures versus time spent analyzing successes for critically important lessons to be learned. I observe a strong tendency to impose new policies, processes and reporting requirements in an effort to avoid future failure. These requirements introduce an ever increasing burden that reduces agility, imposes costs, and delays the delivery of much needed capability. In an interesting study conducted at the Defense Acquisition University, students determined that a "null program"–one that delivers nothing but satisfies mandatory reporting and process requirements–would take three years to complete under the current rules. A system that requires three years to deliver nothing is fundamentally flawed.

As we consider how to reform IT management in the federal government and this Committee considers potential legislation, I suggest policy, process and model decisions be based on what is known to work in government and the private sector, not on reactions to problems. We must build our systems upon successful practices and avoid focusing solely on correcting past failure. My comments today will be based on this premise–that the experiences and attributes of organizations that develop and deploy IT successfully should be the models on which new legislation, policy, and process decisions are based.

The *"25-Point Implementation Plan to Reform Federal Information Technology Management"* is based on practices that work. It establishes a good direction and addresses an important set of issues. We applaud OMB, Mr. Kundra, and the Federal CIO Council's leadership on this topic. It is a national imperative, and it is our collective obligation to deliver information technology more effectively and rapidly to better meet the needs of the public. However, experience leads us to observe that additional steps can be taken both to enable successful implementation of the plan and to expand on some of the important goals defined in it. With that in mind, I will address the following three important topics and provide specific recommendations that build on the intent and direction in the plan:

1) Establishing a governance model which incorporates a comprehensive portfolio management and budgeting approach with close coupling to the end user
2) Establishing strong Program Management Offices (PMOs) by incentivizing and professionalizing the key roles required to successfully deliver IT programs
3) Building secure and resilient IT intensive systems

IT Governance and Portfolio-based Management and Budget Model

Succeeding in a rapidly changing environment requires a balance between discipline and flexibility. The planning-centric investment and acquisition environment of today is built upon a strong discipline, but management must have the tools and authorities to shift resources as conditions change, opportunities arise, and risks are identified and present themselves. This balance is important in an effective IT governance model. Several points in the 25-point plan address aspects of this challenge.

Aligning the budget process with the technology cycle offers the flexibility to shift resources to address changing needs and increase agility. Furthermore, streamlining governance and ensuring accountability strengthens the role and authorities of the CIO to execute important Clinger-Cohen responsibilities. However, these actions will fall short if the link and timing between the investment decision process and the budget formulation process is not addressed to afford increased flexibility.

Fundamentally, the problem is this: the investment decision process occurs 12–24 months before the budget is actually made available, but the steps necessary to make a sound investment decision cannot be taken that far in advance and without some limited budget authorization. More specifically, the details required in the supporting documentation (the E300) cannot be accurately provided without performing some degree of up-front systems engineering to evaluate alternatives, establish initial requirements, and develop an architecture that is needed to estimate schedule and cost–all tasks that currently require the initial budget allocation (which, unfortunately currently requires a completed and approved E300). The net result is an investment decision, based on little real analysis, made two years in advance to support a budget request. By the time the budget is authorized, technology has likely changed, the business environment has been altered, and key personnel have moved to other pursuits, all of which results in significant risk to the successful delivery of the desired results on time and on budget.

This is occurring now, in FY11, as agencies are developing their FY13 budgets. They are currently making major assumptions about future investments and IT expenditures, without the resources or authority to do the ground work required to properly scope the investment, evaluate alternatives, and estimate the cost of delivery based on an evidence-based analysis. By FY13, the assumptions used today to build the budget will be irrelevant.

Moreover, organizations that budgeted to refresh their aging infrastructure using procurement funds may not have the budgetary flexibility to move to the more efficient services model proposed in the 25-point plan. We are already seeing some organizations making suboptimal decisions because the "color of money" does not support provisioning for services. The 25-point plan proposes to work with Congress to realign this process, and we agree. The near term solution is for Congress to provide greater reprogramming authority for IT investments to all department and agency CIOs until a single IT appropriation can be enacted. This is especially critical for IT infrastructure investments that shape the foundation for future mission and business investments. Increasing transparency into these reprogramming actions can satisfy

Congress' oversight function with limited risk and without imposing on the CIOs authority to make trade-off decisions.

This model is very common in private industry and not a new concept. In 2005, the Corporate Executive Board performed a benchmarking study of Key Attributes of World-Class, High Performing IT Organizations. Among the eight attributes identified, IT governance was one of the three most important priorities, based on the nearly 1000 private and public sector organizations involved in the study. Within IT governance, Portfolio Management ranked as one of the activities of greatest importance.[1] Within the federal government, the CIOs of DHS, VA, and IRS have all adopted, or are moving to, a portfolio approach. The DoD, in its IT acquisition task force effort, has also determined that changes to the resourcing process, including portfolio management and a single IT appropriation, are critical enablers for IT acquisition reform.

Unfortunately, the budget process and oversight approach does not align well with this management model and does not allow these CIOs to treat their budgets as a complete IT investment portfolio, thereby diluting the degree of trade-offs that can be made and the spending efficiencies that can be realized. Portfolio flexibility is a long-standing best practice in the private sector where corporate boards of directors rarely engage in line-item oversight of specific IT investments or spending priorities. Instead, they hold the Corporate Officers and the CIO accountable for investing wisely to meet the needs of the business and their customers and for demonstrating strong fiscal and fiduciary responsibility. I strongly encourage Congress to take the additional steps necessary to provide this flexibility by realigning the budgeting model and allowing CIOs and portfolio managers to exercise the strategic decision-making that their peers in the private sector have had for years.

I think that a fundamental reshaping of the role of the CIOs and the implementation of a version of this model, along with the alignment of the budget and technology cycle already defined in the 25-point plan, will transform IT management in ways that will result in more efficient and effective use of IT budgets and greater agility to react to a changing environment.

In addition to the improvements described above, we agree that aligning the delivery cycle with the technology cycle through incremental delivery is another clear step in the right direction. These increments represent a disaggregation of large-scale capability into a number of smaller integrated projects that can be executed in a more accelerated manner. The increments must be built on a sound foundation of up-front architecture and systems engineering, where the architect works to understand the user's operational needs and translates them into technical requirements, and the systems engineer translates those technical requirements into a system design. Sound systems engineering performed early in a program's life cycle has a strong correlation with improved project cost and schedule planning. The use of modular open-system enterprise solutions based upon established standards sets the environment for seamlessly and rapidly delivering incremental performance improvements while enabling the environment for continuous competition. These elements provide for an enduring foundation that will reduce risk

---

[1] CIO Executive Board of the Corporate Executive Board, "Key Attributes of World-Class IT Organizations: A Competency Diagnostic"; January, 2005

and deliver capabilities in a timeframe during which the technology is current and skills are relevant. This is also a common approach in the private sector.

Equally important is the need to couple the IT investments and the acquisition process more closely with operations. Speed is important, but it must be well matched to the operational tempo. This coupling ensures that technology drops have clear business value, and increments build on an enduring, underlying IT infrastructure that supports future investment and capability delivery in a cost effective fashion.

At the enterprise level, current processes tend to focus more on compliance than on outcomes. This means they often fall short of meeting business needs. Aligning all stakeholders to a set of shared mission outcomes creates clarity of purpose and will drive dynamic trade space analysis to assess alternative architectures; concepts of operation; and tactics, techniques, and procedures. Aligned teams can guide decisions through short development cycles and can motivate their home organizations to support the outcomes most effectively. These teams provide a venue for the enterprise to engage directly with the operator and gather important feedback from the field. This "Integrated Product Team" (IPT) program management office approach, highlighted in the 25-point plan, is a most effective way to manage an incremental development program. It is critically important that this concept extend to include the development team and be inclusive of the technical management roles (e.g., Chief Architect and Chief Engineer) to set the technical direction for the program, guide the technical decomposition of the solution from concept to field, and enable the government to be a technical peer to the contractors and other supplier organizations. Without this broad set of operator and technology perspectives, the risk of missing critical issues, or taking advantage of opportunities to lead to better outcomes.

With these thoughts in mind, my recommendations can be summarized as follows:

1) Adopt an IT governance model that that features a consolidated, portfolio-based IT budgeting model to allow the flexibility of CIOs and agency leaders to adapt funding during the year to react to changes in technology and mission requirements. This should include multi-year authority and the authority to fund the up-front systems engineering and alternatives analysis necessary to evaluate and estimate the scope, cost, and schedule for their proposed investments without prior approval.
2) Eliminate the investment line-item oversight and the practice of differentiating or "fencing" budget by investment type. Instead, allow CIOs to trade-off investments between New Development, Operations and Maintenance and Infrastructure.
3) Enhance and expand accountability methods and metrics akin to the TechStat reviews and the evolving dashboards to hold the CIO, business leader, and other stakeholders collectively accountable for outcomes. Act upon these results by rewarding performance and addressing areas needing improvement.
4) Match incremental delivery with the operational cadence of the organization or function the IT program supports, with timeframes no later than those identified in the 25-point plan, but not requiring an increment every six months.

Establishing Strong, Enduring PMOs by Incentivizing and Professionalizing IT Program Management

In my past testimony to this subcommittee, I emphasized the importance of maintaining strong technical and management capabilities within program management offices (PMO). It continues to be my experience that successful programs are characterized by a strong government PMO capable of acting as a strong "technical peer" with contractor counterparts on systems engineering. The individuals assigned to these program offices must view their position as a career and not simply a job. Incentives play a key role in attracting and retaining competent program office personnel. Establishing a career progression gives individuals the opportunity to secure greater responsibility and pay based commensurate with increased degrees of proficiency.

Incentives for individuals need to become more mission-focused and designed so that top performance leads to career growth. Incentives should motivate individuals to leave assignments better than they found them. Toward that end, the performance of the organization and individual leads should influence those individuals' future performance reviews. Too often individual leads are so concerned with ensuring that nothing "happens on my watch" that problems are not recognized in a timely fashion. Individual incentives should also be designed to retain individuals with knowledge and skills of value to the organization and make allowances for a reasonable amount of courageous risk taking, recognizing that that the occasional failures that are a natural outcome of that behavior are far outweighed by the potential benefits.

Contractor incentives also must be considered, as they play an important role in the organization's ability to achieve its objectives. Current contract management practices create some incentives that run counter to government objectives for these companies, which today are motivated largely by profit, opportunities for change orders, and maintaining barriers to entry. In other cases, the excessive bureaucratic and regulatory environment produces disincentives that lead many commercial companies to refuse to do business with the government. While it is clear that the contractors must operate in ways that satisfy their stakeholders and employees, it should also be possible to establish incentives that serve both the government and contractor community well—incentives that are mission-focused, allow for reasonable profit, reward successful contract performance, lower the barrier to entry for commercial firms, and promote continuous innovation and competition.

1) Establish career paths for these IPT PMO team. Many are identified in the 25-point plan, but I would include the technical management roles such as Chief Architect and Chief Engineer since they set technical direction and act as the technical peer with the contractor.
2) Establish incentives for program leaders and technical leaders by aligning their performance with mission outcomes, not just program outcomes. Reward prudent risk taking and results.
3) Allow contracting flexibilities to incentivize contractors in accordance with mission outcomes, not just with contract delivery.

Building Secure IT Systems

A final area of extreme importance is securing information systems. This should be a critical aspect of any investment, and it warrants major investments in its own right. All too often, however, security is regarded as an afterthought, an option. And all too frequently, concerns about system vulnerabilities are used to justify making less transformational investments and adhering closely to the status quo–making marginal improvements instead of fundamental changes. This reluctance is justified as a concern about the "new technology."

I believe that security concerns should not be the reason for not doing something new, but rather should be a major consideration in how to do it successfully. This process starts with the architecture and initial investment plan. Defining resilient architectures that not only address vulnerabilities but also include the capabilities required to withstand a breach should be a key element of any investment. Factoring in security considerations should be, for instance, important in determining the type of cloud environment to adopt and how to architect and operationalize it. It should not be a deterrent.

An example of this case can be found in the 25-point plan's "cloud-first" policy. Cloud-based strategies provide opportunities for efficiencies through virtualization, commoditization, and provisioning of services. However, security issues should be a major consideration in the process of determining the type of cloud. From my experience, it is important to weigh the security issues as a key element in the decision about which applications are moved to the cloud and which cloud strategy is best leveraged to meet the functional needs, deliver efficiencies, and protect the data and applications. We developed, and have shared with many agencies and OMB, MITRE's *Cloud Computing Decision Process*[2]—our recommended guidance on how to measure and evaluate the trade-offs to make the best cloud decision. Inherent in this framework, and the intent behind it, is the belief that decisions of this nature should recognize and weigh both risk and benefit.

As an illustration, deploying data and applications to a cloud environment changes an organization's IT security posture. New technologies are introduced into the IT infrastructure and responsibility for securing systems is shared between the organization and the cloud service provider. These changes create both challenges and opportunities. Risks introduced by the new technologies are challenges that must be understood and addressed. The cloud service provider, however, is an ally who has both expertise and resources to help address these challenges. Working together, these partners have the opportunity to achieve more secure systems. The cloud service provider can address IT infrastructure security, thereby allowing the organization to focus on protecting information.

This is a topic on which the Federal CIO, the CIO Council, and the Congress can provide more leadership. They should send a clear message that government information technology investments must not only be aligned with business needs, deployed incrementally, and managed

---

[2] Presented in *"A Decision Process for Applying Cloud Computing in Federal Environments"*; www.mitre.org/work/tech_papers/2010/10_1070/cloud_federal_environments.pdf

properly within budget and schedule, but must also be architected, developed, and operated with a clear eye on protecting public and private data and continuing the critical services government performs for the public. A major thrust of this nature will also represent a transformation in the way information technology is adopted, deployed, and operated by the federal government.

Summary and Closing

Achieving the results expected of the 25-point plan requires a major transformation that spans many aspects of the federal government's operations. Transformation succeeds when culture, strategy, vision, processes, incentives, and accountability are aligned and reinforce one another. Moving away from core rigidities that prevent the enterprise from being as effective as possible can only be achieved by changing the way individuals think about their roles and how they help achieve the overarching goal of the organization.

John Kotter's *Harvard Business Review* article "Why Transformation Efforts Fail"[3] lists the mistakes companies make when attempting to reengineer themselves. One of the most common errors is not anchoring changes in the organization's culture. Change sticks when it becomes "the way we do things around here," when it seeps into the bloodstream of the corporate body. Until new behaviors are rooted in social norms and shared values, they are subject to degradation as soon as the pressure for change is removed. Cultures can change when leaders make a compelling case for change, there is a clear roadmap of explicit steps, the roadmap is consistently communicated to all stakeholders, and expectations and accountability are unambiguous. The 25-point plan presents this roadmap.

One of the key attributes of successful commercial organizations is the willingness to examine how the firm does its work and to abandon processes that consume resources but don't create value for the mission. The federal government, conversely, has a long history of repeatedly layering new initiatives on existing processes with a goal of minimizing risk. As a result, achieving IT objectives in the federal government is more difficult, takes longer, and requires too many reviews and approvals. To compound this process-heavy environment, the culture of risk aversion means that "no" is much more likely to be encountered than "yes." Successful organizations will routinely abandon less valuable activities to increase speed and reduce cost. We must not be reluctant to do the same.

The many elements of the 25-point plan reflects two sets of related priorities – adopting new technology that enables greater efficiency, and establishing an enduring foundation of capabilities to plan, manage, and execute IT programs more successfully. I believe the latter represents both the greatest challenge and the true imperative. From my vantage point, enduring change will require the following:

---

[3]. John P. Kotter, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review on Change*, Harvard Business School Press, 1998.

1) Establishing IT governance that includes authorities and flexibilities where they best contribute to the success or failure of these programs without losing transparency into how these portfolios are performing
2) Building and empowering Program Management Offices (PMOs) by incentivizing and professionalizing the key management and technical roles to motivate people to adopt these roles as careers
3) Defining and building IT capabilities that are secure and resilient

Without the opportunity, authority, and resources to accomplish these goals, the success rate in adopting new technology will continue to suffer. I am supportive of the direction of the 25-point plan, as well as other similar action plans developed and being implemented across many agencies today. I am encouraged by the clear interest of this subcommittee in taking steps to codify methods and operating models that we know to be successful and on the increased emphasis on developing the foundation capabilities that endure beyond contemporary solutions. I believe if these steps are taken, the promise of the 25-point plan can be realized, and the priorities it lays out will endure.

I respectfully request that my prepared statement be included in the record, and I would be pleased to answer any questions.