STATEMENT OF
KAREN S. EVANS
FORMER ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
May 8, 2014

Good morning Chairman Carper, Ranking Member Coburn, and Members of the Committee. I am pleased to be invited back to share my views on, "Identifying Critical Factors for Success in Information Technology Acquisitions." My remarks today will describe best practices and success factors for managing information technology (IT) systems that the government can learn from industry.

The federal government will spend over $80 billion on information technology (IT) this year. Despite guidance and oversight by Congress, General Accountability Office (GAO), and Office of Management and Budget (OMB), Federal IT projects too frequently incur cost overruns and schedule delays, and end-up contributing little to agency mission outcomes. Frequently these failures resulted from well know hazards that experienced practitioners have learned to avoid by adopting specific procedures – best practices – that circumnavigate these pitfalls. Other times the project failure could be traced to someone not doing what they were supposed to do. The technology did not play a trick on them. There was not an unforeseen outside force dooming the project. No, in every case, someone missed their block and let a defender sack the quarterback. The reflexive response is to add another layer of rules to prevent someone from making that bad decision again. This is the wrong way to go, as it adds layer upon layer of bureaucracy that eventually grinds the process to a halt.

One cannot mandate good outcomes, nor can Congress legislate to preclude failure. Rather, the IT acquisition system must foster a culture that allows and tolerates a continuing learning cycle to improve overall performance. Results, whether they are good or bad, provide important feedback that needs to be integrated into the overall management framework. The goal must be to enable success, not to preclude failure.

Government and Industry – Similar Challenges

Government and industry face many similar challenges in planning, acquiring, and deploying IT systems. While today's hearing is focused on improving the Federal Government's management of IT by learning best practices from industry, it is worth noting that the private sector does not have a perfect batting average. A 2012 report [1]from the Standish Group International found that 18 percent of private sector IT projects failed. That is, they were either canceled prior to completion, or delivered and never used.

The causes of such failures are not unique to the private sector. Government IT and acquisition professionals face similar issues. This is not meant to excuse the Government's failures, but rather to demonstrate why industry best practices are applicable to the Government. The Standish Group also

[1]The Standish Group International, Incorporated. Chaos Manifesto. 2013.

reported that the number of software development projects that were completed successfully on time and on budget, with all features and functions as originally specified, rose from 29 percent in 2004 to 39 percent in 2012, a significant improvement. Government should adopt these practices that enabled this success.

Government and Industry – Different goals lead to different challenges

The very obvious differences between the goals and priorities of Government and the private sector create different challenges for each. Government and industry have very different time horizons. Businesses focus on short-term results even as they pursue long-term strategies for their organizations; quarterly earnings, next season's fashions, or the new model year. Their long-term strategies are not to develop IT systems – IT is a means to an end, not the end itself. Government, on the other hand, will tolerate a very long time to fruition for a project and chooses to be measured by their level of effort to pursue their mission/program goals – to end homelessness, to cure cancer, to fight poverty. And whereas businesses seek low turn-over in their executive ranks, Government senior leaders are inherently transitory. The Executive Branch compensates for this characteristic with the career Senior Executive Service (SES) managers providing stability and long-term perspective, while supporting short-term objectives for their political leadership's priorities and policy initiatives.

The clear performance indicator of profit and loss makes some aspects of IT management easier in the commercial world. A business only spends money to make more money. So, if an IT project will increases profits, then it gets a green light, and if the project begins to overrun its budget so much that it won't make money, then it is cancelled.

Whereas a business earns money to meet its goals, Government spends money to meet its goals. If an IT system will help accomplish the goal, then money is spent on that IT system. Government employees are often passionate about their agency's mission, and perhaps a little less sensitive to cost overruns than the private sector. As such, OMB and Congress have instituted a regimen of compensating controls – indicators, alarm bells, and processes to alert management if a project is in trouble.

Finally, business has little tolerance for failure – mismanaging a project or selecting the wrong vendor can bring serious financial consequences or even cost a job. Established metrics are closely monitored, especially for high risk, high visibility IT projects.

Conversely, Government leaders pursue very long-term goals, with sometimes ill-defined performance measures, and it is difficult to hold people accountable for their performance. IT Project Managers should be different. These roles have clearly defined competency requirements, and projects have standardized metrics, frequent performance evaluations and feedback. Yet, when a project fails and tens of millions of dollars are wasted, the person who was supposed to prevent that is not held accountable appropriately. Many times, they go on to manage (or mismanage) subsequent projects.

Conversely, PMs viewed as competent are often pulled midstream from a major project to go manage another project midstream. The result is now old project goes of schedule and performance under inferior management.

The Committee should consider whether it would be appropriate for providing incentives for the quality PMs to stay with their major project through successful completion and ensuring PMs

demonstrated from training completed and/or successfully delivering results on smaller scaled projects before managing major large scale IT projects.

Yet, accountability cannot be implemented in a way that creates a culture of fear. If such a culture takes root, IT managers and acquisition professionals will adopt strategies that stifle innovation and become less responsive. They will take steps to try to eliminate risk altogether. Risk cannot be eliminated in any project that has meaning. Rather, risks have to be *reasonably* mitigated and balanced with goals related to cost, timeliness, and effectiveness.

This is a delicate balance. Managers who routinely make bad decisions must be held accountable. But by the same token, they also need to have the ability and authority to exercise good judgment. Only by doing so can IT managers actually achieve positive results.

Lessons Learned

Oversight – Surveillance, not Inspection

While I was at OMB, one of the statutory roles assigned was oversight and leadership of the Department and AgnecyChief Information Officers (CIOs). I can appreciate the balance the Committee must strike in assessing without inhibiting, and the enormous amount time that adequate and appropriate oversight can absorb.

Like the Committee, we had a small staff, so we needed to be efficient while being effective. I gave my staff an analogy -- they had to be like a teacher -- grading papers but not correcting errors. To do this, we required agencies to submit evidence of having completed a task than rather than documentation of the task results – allowing the staff to perform surveillance rather than inspection. For example, agencies are required to perform a cost-benefit analysis when proposing a new IT system. Rather than having the agency submit the documentation of the cost-benefit analysis, the requirement was for the CIO to affirm that they had performed the analysis and the date. Therefore, during review meetings, questions were posed regarding the decisions made based on the analysis.

In reviewing the House-passed *Federal Information Technology Acquisition Reform Act*[2] (FITARA), I saw several oversight provisions that could create unintended consequences – burdening the Congress with inspection rather than oversight. For example, requiring the Agencies to submit a report to the House and Senate Oversight Committees is intended to provide information to the Committees, and to force the agency to look at their own data periodically and subsequently manage their projects in the course of preparing that report. Unfortunately, Peter Drucker was right when he said, “What gets measured gets managed.” If you ask for reports, you'll get reports – not necessarily better management. For example, the Federal Information Security Management Act (FISMA) was intended to improve the security of IT systems. The annual reporting process of FISMA created the emergence of a cottage industry to generate these reports but the result was not reduction of risk or improved risk management and security of IT systems. If you ask for a report, the agencies will dutifully comply and provide the reports. And having received the report, if a Committee’s prescribed report format does not contain a piece of data necessary to diagnose a problem, the risk has now shifted because the Committee did not identify appropriate data necessary to ensure successful implementation.

[2]H.R.1232 - Federal Information Technology Acquisition Reform Act

Similarly, requiring meetings will yield meetings and not necessarily the outcome you're after. Ideally, you really want agencies to manage themselves to agreed-upon outcomes for programs and projects where oversight as in this Committee can provide a red-light or green-light.

Oversight - Focus Management Attention

In addition to verifying compliance with statute and policy, the E-Government Act[3] directs the Administrator to help improve the management of IT in the agencies. During my tenure, we published a quarterly list of projects that warranted extra management attention. The Management Watch List included projects which were either not well planned or not being well managed and projects which exhibited unusual risks because of their size or complexity. By distilling volumes of data down to a simple list, agency senior executives, who might not have expertise leveraging IT management tools (*e.g.*, earned value management), would readily know the status of projects in their agency, and could, call our office if they had questions. And we were able to flag suspicious or obviously incorrect data for further investigation of those projects such as no variance in the data – where planned data exactly matched actual data.

As a result of this approach, we saw a 62% improvement in the planning and management of major IT capital investment projects over the six year period during which I served.[4] The oversight has continued in this Administration through their process of TechStat Accountability Sessions (TechStats) and now PortfolioStats. I would note that we released the Management Watch List on a quarterly basis, and I would strongly encourage the Administration to do the same. In particular, relevant data should be updated regularly and that which is related to the Portfolio Stats meetings should be posted on the IT Dashboard.

Oversight – Collaboration

While we used the Management Watch List to help direct the attention of agency senior executives, that same list of projects informed both GAO and the Agencies' Inspectors General (IGs) of what projects they should focus their attention on as well. Now, with the alignment of high priority goals, cross-agency priority goals, strategic plans, and budgets as required by Government Results and Performance Modernization Act, the GAO and IGs audits and evaluations are focused on the agencies' performance in achieving these aligned goals.

Critical Success Factors

Numerous books and articles have been written on to improve the management of IT acquisition projects. For example, the Software Engineering Institute has developed their highly regarded Capability Maturity Model Integration (CMMI) program, and GAO has issued numerous reports on IT management practices. Interestingly, most of these reports agree on the essence, if not the details, of requirements for project success. And my experience confirms their conclusions. Below is not a complete list of critical success factors as there are factors ingrained into the agency culture affecting success, but rather the factors that the Committee could easily influence, should it choose to do so.

---

[3] E-Government Act of 2002, PL107-347

[4] Executive Office of the President. Budget of the United States Government: Analytical Perspectives. Budget Year 2009. Washington, DC. U.S. Government Printing Office, 2008.(Table 9-7).

1. Qualified Project Manager

A good Project Manager (PM) is absolutely essential for project success. Indeed, a strong PM can compensate for shortcomings elsewhere, but nothing can compensate for a weak PM. The PM has a multi-faceted job. The PM leads the technical staff, manages financial resources, oversees contracts, and makes hundreds of decisions on priorities and trade-offs.

Industry best practice assigns the CIO the responsibility for supplying trained, certified PM's. The CIO establishes the policies and procedures for managing IT projects, and establishes the standards for certifying PM's as being qualified to manage projects of a certain size or complexity. These certifications attest that the PM has demonstrated a designate scope of knowledge, and had demonstrated success managing programs of a specified size or complexity.

An example is the Project Management Professional (PMP) certification from the Project Management Institute (PMI). Major consulting firms commonly establish their own certifications which build upon the PMP program, adding knowledge of their proprietary tools or methodologies.

The Federal Government followed this industry best practice in establishing the FAC-P/PM certification. This certification was recently updated on December 16, 2013, by Office of Federal Procurement Policy[5]. The FAC-P/PM combines IT project management and Federal contracting to yield an individual with knowledge and experience necessary to manage the entire acquisition life cycle. The FAC-P/PM can be certified at three levels, affirming knowledge and experience at progressively higher levels of accomplishment.

The strength of the FAC-P/PM certification significantly reduces the risk of a project. Conversely, knowing that the PM is not qualified would be reason for concern and extra management attention. Because this information is essential to assess the risks of an IT project, OMB requires Agencies to submit the name and qualifications of the PM for every major project. Unfortunately, this information is not made available on the IT Dashboard, preventing users from assessing the project risk.

2. Shortage of Qualified Program Managers

While OMB requires a qualified PM, agencies sometimes do not follow this guidance – assigning instead an unqualified PM. Either the CIO was not consulted on the selection, or they simply couldn't find a qualified PM. The E-Government Act assigns Agency CIOs the responsibility for planning and training their Agency's IT workforce. The Clinger-Cohen Act and the E-Government Act (Section 209) both require an Annual IT Workforce Assessment by the Federal CIO Council under the leadership of OMB and the Office of Personnel Management (OPM). This report has consistently stressed the need for additional training to develop more qualified PMs[6].

The Committee should consider whether it would be appropriate for Agency CIOs to have additional flexibility to help alleviate the chronic shortage of qualified PMs. Although there are human resources tools available such as direct hiring authority and transfers or details, additionally flexibility may be useful in adjusting existing policies to allow hiring a contractor to be the PM with the authority to direct other contractors.

[5] http://www.fai.gov/drupal/sites/default/files/FAC%20PPM%20Policy_121613.pdf
[6] https://cio.gov/wp-content/uploads/downloads/2012/09/2011_ITWCA_Results_Report_Final_5.31.11.pdf

3. **Actively Engaged Project Executive**

The other person essential for the success of an IT project is the Project Executive (PE). Assigning a PE to an IT project is an Industry best practice. While the CIO is responsible for providing a qualified PM, the PE represents the organization that will pay for and use the IT system. The PE has two roles: overseeing the PM in all aspects of managing the project, and supporting the PM in interacting with the PE's organization by securing the cooperation and support of the organization.

The government frequently disregards this model because of the appropriations process. The scenario is as follows: The CIO has the responsibility to manage the IT projects. An Assistant Secretary will request funding for a new program which includes the supporting IT systems. The Assistant Secretary wants to ensure "control and accountability" and therefore, appoints a PM, which is usually a member of the program team without the appropriate qualifications or PM certification for the scope and complexity of the project.

The result is certain failure. Not only does the project not have a qualified PM, it also has an ineffective PE who is neither independent nor able to manage the PM. Because the Assistant Secretary has selected the PM – he is conflicted. Congress should consider the requirement that PMs work for the CIO of the organization versus taking all the budget/appropriations authority and giving it to the CIO. In this manner, the Assistant Secretary is still responsible for their portfolio and program outcomes but gains the experience and expertise of the CIO organization for implementation of IT systems.

4. Mature Enterprise Architecture (EA)

In the E-Government Act, Congress sought to enable agencies to align internally with the development of their enterprise architecture. Additionally, OMB sought to align the government as whole with the efforts surrounding the development of the Federal Enterprise Architecture (FEA). These initiatives are not to just standardize hardware and software but to share and re-use investments. The issuance of the "Common Approach to Federal Enterprise Architecture," seeks to address the use of EA to "include principles to help agencies eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among government, industry, and citizens."[7]

By having a mature process involving the development of EA artifacts, the CIO sees the world "as it is" and "how it could be" and should establish the necessary transition plans to accomplish the outcomes necessary to support the agency mission. These artifacts should be used by OMB and Congress in order to ensure the outcomes are understood and adequately resourced. Therefore, departments and agencies should be required to submit as part of the Congressional Budget Justifications the appropriate artifacts to illustrate adequate planning for the "to be" architecture and transition plans that are reflected in their request.

5. **Requirements Management**

From an IT implementation standpoint, IT project failure happens all too frequently. Many speculate after the fact that the failure was due to complexity in the procurement, lack of testing, or lack of

[7] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf

requirements definition. However, most federal government IT project failures are due to inadequate management decisions.

In private industry, all levels of management are engaged reviewing data such as "earned value management" (EVM) in order to assess the project's progress. By using such as tool, all levels of management become sensitive to the variances produced by early warning signs of impending schedule delays and cost overruns. This approach also allows individuals outside the project to see a standardized metric describing the cost and schedule performance of that particular project and compare it consistently with other projects. IT projects are particularly good at highlighting management failings because they require coordination between many different parts of the organization.

EVM has evolved from an industrial engineering tool to a government and industry best practice, providing improved information to conduct oversight of acquisition programs. As such, it is guided by industry best practices and standard, and is required by regulations and requirements at the federal government as demonstrated by the TechStats and now the Portfolio Stats sessions with OMB.

6. Public-Private Partnerships

In order to address actual procurement issues and potential reform, the federal acquisition model needs to truly have a process which allows for shared risk between the government and the contractors supporting them. All too often, when an IT project fails, the contractor states the government failed to provide adequate requirements and the 'finger pointing' begins. All levels of both organizations need to be willing to be involved and understand the intricate aspects of management and implementation.

Instead of revisiting the Federal Acquisitions Regulations (FAR) as whole, the public-private model should be re-evaluated allowing new models to be deployed within the federal government. Taking an example from the state governments which is more of a "no-cost model," it is possible to significantly reduces the risk of the project by having the service provider invest in the large up-front costs of building an IT system and manage the project through the entire life cycle.

In states such as Oklahoma, Arkansas and Montana, online services are delivered at no cost to government agencies through a transaction-based, self-funding model. In this model, the contractor assumes the cost of building and managing services, and then the contractor recoups its investment through modest fees paid by citizens or businesses electing to use the service. This type of performance-based contracting approach ensures the contractor is motivated to quickly deploy service that citizens and businesses want to use. It also shifts financial risks from the government to the private sector.

Currently, the Department of Transportation (DOT) is using this model to provide trucking companies with access to important driver safety data. Since 2009, over 2.5 million driver records have been accessed through a secure online service that costs DOT nothing to build, operate or maintain. It may be possible to apply this model across other federal government agencies.

Similarly, the "share-in-savings" model has the contractor pay for the capital costs of things like energy efficiency projects. After negotiating a baseline, the contractor recoups its investments by sharing in the savings attributable to the reduced energy consumed. Not only does this reduce capital outlays otherwise borne by the taxpayer, it shifts the risk of project failure to the contractor.

Congress has granted certain agencies specific authorities to develop similar public-private partnerships and these should be expanded. The Committee should consider whether to encourage wider use by eliminating hurdles such as cost scoring and budget treatment of such collaborations.

7. Need for Leadership at the Departments and Agencies

The CIO is the person in the C-Suite who should have the capacity to translate technology issues into business-speak for the other business leaders. The CIO position is currently under scrutiny as the original purpose of the position is not necessarily working as envisioned both in private sector and government. Whether this person is the CIO or the Chief Risk Officer, Chief Innovation Officer, Chief Strategist, or some other "chief," it is necessary to have a leader who can speak to senior executives in terms that are relevant to them, and can state the potential consequences in terms of political and policy values (*e.g.*, public opinion, impact on promised level of service, unfavorable news stories, decline in earnings per share, etc.). Right now, the CIO is in the unique position to ensure that this happens and needs to provide the leadership in order to avoid the mistakes of the past.

Overall federal CIOs and commercial CIOs are similar---with the same job description: to be the technology savvy member of the executive team, to provide value through innovation, to manage data as a strategic asset, and to lead a team of technologists and enables organizational greatness.

There is a widespread perception that the government is inherently incompetent at implementing IT systems – not just because of the recent high-profile failure, but because that follows a string of high profile failures. However, I've also seen lots of IT projects that were tremendously successful – that delivered on time and within budget – that are helping the American Government to serve the American people, and that did not get newspaper stories written about them. So rather than trying to prevent failure, we should promote success by implementing best practices, assigning qualified program managers, and monitoring with accurate metrics. IT is a neutral enabler for program delivery. Good management is nonpartisan, and can support all policies.

Thank you for this opportunity to testify today. I look forward to answering the Committee's questions.