

Editorial: Obama's Information Technology Priority

by Roger Sessions

Editor-in-Chief

Perspectives of the International Association of Software Architects

Reprinted from the Perspectives of the International Association of Software Architects, Issue #7, January, 2009

Copyright 2009, IASA, Reprinted with Permission.

Introduction

As a presidential candidate, Barack Obama recognized the potential of Information Technology (IT) to play a transformative role in our government and in our lives. In a major position paper, his campaign said:

Barack Obama understands that we must use all available technologies and methods to open up the federal government, creating a new level of transparency to change the way business is conducted in Washington and giving Americans the chance to participate in government deliberations and decision making in ways that were not possible only a few years ago. To achieve this vision, Barack Obama will encourage the deployment of the most modern communications infrastructure. In turn, that infrastructure can be used by government and business to reduce the costs of health care, help solve our energy crisis, create new jobs, and fuel our economic growth.¹

This is a compelling vision, but given the current state of IT in the federal government, it will be a very difficult one to deliver. In this editorial, I am going to examine the challenges that President Obama will have delivering on his promise. I will also make some specific suggestions on how his administration should proceed. However, before I discuss how federal IT needs to change, I need to look at the current state of federal IT.

The State of Federal IT

The challenge of creating large complex mission critical federal IT systems has proved intractable. While the total number of major IT projects in the U.S. Government has remained relatively constant over the last three fiscal years, the number of these projects that are considered troubled (that is, either not "well planned" or not "well managed" or both) has risen at an alarming rate. These trends can be seen in Figure 1, with data taken from the 2009 U.S. Budget².

Comparison of Major Federal IT Projects and Troubled IT Projects

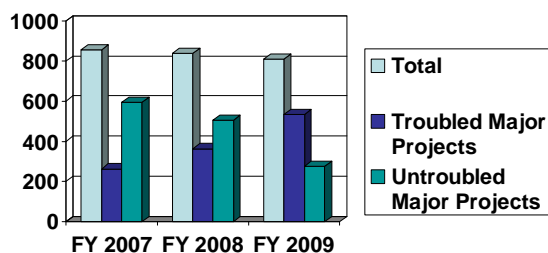


Figure 1. Troubled Major Federal IT Projects

As shown in Figure 1, the total number of major federal IT projects has remained at a relatively constant 800 projects over the last three fiscal years. However the number of these that are troubled has risen from 30% in FY 2007 to 43% in FY 2008 to 66% in FY 2009. In absolute dollars, this means that of the \$71 billion in federal IT investments, someplace around \$47 billion is invested in projects that are at risk.

This analysis most likely underestimates the problem because it only considers projects that are officially over-budget or behind schedule. A large number of federal projects manage to stay on budget and on schedule by a process known as rebaselining, that is, redefining targets and schedules after a project has missed previously defined targets and schedules.

The rebaselining process is surprisingly common in the federal government. According to a recent General Accounting Organization (GAO) report:

...we project that 48 percent of the federal government’s major IT projects have been rebaselined for several reasons, including changes in project goals and changes in funding. Of those rebaselined projects, 51 percent were rebaselined at least twice, and about 11 percent were rebaselined 4 times or more.³

In other words, of the \$71 billion in federal IT investments, the estimate of \$47 billion landing in troubled investments is almost certainly too low. If one includes projects that escaped the “troubled” label through rebaselining, the troubled investments could total \$60 billion or more.

Indirect Costs of Challenged Federal IT Projects

The direct costs of challenged federal IT projects are clearly high, but the indirect costs are much higher.

As an example, consider the IRS mission critical information system, the Electronic Fraud Detection System (EFDS). Between 1994 and 2005, the IRS spent \$185 million on EFDS. This system had multiple problems and was abandoned in 2006⁴.

Approximately \$185 million was lost on this project in direct costs. However the indirect cost to the U.S. taxpayer was much higher. In September 2008 the Treasury Inspector General for Tax Administration estimated that the federal government lost approximately \$894 million in fraudulent refunds during 2006 because the EFDS was not operational⁵.

In other words, the IRS lost \$185 million in direct costs and \$895 million in indirect costs. This is a ratio of indirect cost to direct cost of 4.8:1. If this ratio holds true for the rest of the challenged federal IT projects, then the \$60 billion costs mushrooms to \$289 billion.

This ratio may seem high, but it is, in fact, typical. In the private sector, this is known as “lost opportunity costs”, and these costs usually far outweigh the direct cost of the IT failure.

Of course, not all of this indirect cost will be because of lost tax revenue. Some of it will come from criminals entering the United States illegally because of failures in the Department of Homeland Security’s U.S. Visitor and Immigrant Status Indicator Technology program⁷. Some of it will come from identity theft because of widespread failures to encrypt sensitive information⁸. Some of it will come from troubled financial markets because of failures in the information systems of the Securities and Exchange Commission⁹. The list is frighteningly long.

The bottom line is that while we will never know for certain how much these challenged federal IT systems are costing, we can be sure that this cost is very, very high.

Efforts to Improve Federal IT

The challenges of creating effective federal IT systems is not news. The General Accounting Office issues a new report highlighting some challenged area of federal IT approximately every ten days. Very few governmental agencies escape GAO scrutiny.

There have been two major initiatives to help the federal government improve its ability to manage IT. The first is accounting. The second is architectural.

The accounting approach to IT management goes under the name of Earned Value Management (EVM). When a project begins, it creates a time line. At regular intervals, predictions are made about how much money will be spent and what deliverables are expected. The ratio of expenditure to deliverables is called “earned value.”

A project that reaches a given time point spending the expected budget and receiving the expected deliverables has a good EVM index. A project that reaches a given time point and exceeds its expected budget or receives less than its expected deliverables is in danger of falling behind schedule. A project that reaches a given time point both overspending its budget *and* not receiving expected deliverables (the all too common case) is in serious trouble. Close monitoring of the EVM is used to spotlight troubled projects.

There are three problems with the use of EVM metrics in the federal system. The first problem with EVM is that the use of rebaselining, discussed earlier, makes this metric unreliable. The second problem with EVM is that while it might help us better understand the direct cost of the challenged projects, it does not help us understand the much higher indirect costs. The third problem with EVM is that while it can theoretically do a good job of pointing out projects in trouble, it does nothing to keep the project from getting in trouble in the first place. Building IT systems that do not get in trouble should be our first priority.

The architectural approach to addressing federal IT challenges goes under the name of Federal Enterprise Architecture (FEA). I have discussed the FEA in depth in a white paper¹⁰, so I will not repeat that here. I will simply point out two salient points.

The first is that FEA is an expensive project. Its requirements extend to every federal agency. While I have never seen cost estimates for the entire FEA, based on the scope it must be in the hundreds of millions of dollars.

The second is that most of the pieces of FEA were put in place by 2006 and the use of FEA throughout the federal government has been steadily expanding since then. If FEA was going to be successful, we would expect to see a reduction in troubled projects beginning in 2006. We have not seen this. As I discussed earlier, the number of troubled projects has been increasing, not decreasing, since 2006.

So we see that to date the government has taken a two-pronged approach to dealing with troubled IT. The first, EVM, is an accounting approach. The second, FEA, is an architectural approach. And while both of these seem to be useful, the cost of troubled IT projects continues to increase. Something more is needed.

President Obama's Challenge

Against this backdrop, President Obama has specifically highlighted two areas for his new technology initiatives. The first is healthcare. The second is better integration between the Veteran's Administration and the Department of Defense. Both of these areas have cautionary tales to which the new administration is advised to pay heed.

Let's start with health care. According to candidate Obama's position paper,

A key feature of Barack Obama's health care plan is the use of technology to lower the cost of health care. Most medical records are still stored on paper, which makes them difficult to use to coordinate care, measure quality, or reduce medical errors. Processing paper claims also costs twice as much as processing electronic claims. Barack Obama will invest \$10 billion a year over the next five years to move the U.S. health care system to broad adoption of standards-based electronic health information systems, including electronic health records¹³.

This plan is strikingly similar, both in intent, scope and cost, to a British plan known as National Programme for Information Technology (NPfIT). NPfIT is run by the United Kingdom's National Health Service (NHS). As the NHS describes NPfIT systems,

A key aim of the National Programme [NPfIT] is to give healthcare professionals access to patient information safely, securely and easily, whenever and wherever it is needed. The National Programme is an essential element in delivering The NHS Plan. It is creating a multi-billion pound infrastructure which will improve patient care by enabling clinicians and other NHS staff to increase their efficiency and effectiveness¹⁴.

To date, NPfIT has been a case study in IT failure and this shows no sign of changing. I have written about NPfIT extensively in my recent book¹⁵ and I will not rehash it here. Suffice it to say that it will probably cost somewhere between \$40-100 billion and earn the dubious distinction of being the world's most costly IT failure. The Obama administration is well advised to study what went wrong with NPfIT before embarking on a similar venture.

The other initiative candidate Obama mentioned is better integration between the Veteran's Administration and the Department of Defense. His position paper said,

Obama will make the Veterans Health Administration, the nation's largest integrated Paid health system, a model in the use of technology to modernize and improve health care delivery. To ensure that veterans get the best care possible, he will improve electronic records interoperability between the Pentagon and VA, expand effectiveness research, promote wellness programs, and use technology to improve the accountability for performance and quality.¹⁶

The National Defense Authorization Act for Fiscal Year 2008 already requires the Department of Defense and Department of Veterans Affairs to accelerate the exchange of health information and develop interoperability between their systems. However, this effort has been troubled from the beginning. The General Accounting Office (GAO) has repeatedly highlighted problems in this effort, most recently in September, 2008¹⁷.

In addition, both the Department of Defense and the Veteran's Administration have historically been two of the most challenged federal agencies in terms of their ability to deliver *any* successful IT project, never mind one requiring interoperability between the two agencies. Of the 60 major IT projects currently underway at the Department of Defense and of the 40 major IT projects currently underway at the Veteran's Administration, every one has been placed on the GAO's Management Watch List for high risk¹⁸.

If the Obama administration is going to make the Veteran's Administration "a model in the use of technology to modernize and improve health care delivery" it will need to start by looking carefully at why recent efforts have been so troubled.

The Federal Chief Technology Officer

The Obama position paper promised to appoint a Chief Technology Officer (CTO) for the federal government. This person will work “with chief technology and chief information officers of each of the federal agencies, to ensure that they use best-in-class technologies and share best practices¹⁹”.

Having a single CTO for the federal government is a good idea. Clearly, the difficulties of delivering successful IT projects extend far beyond any one agency. The CTO’s position could address this problem across the entire federal government.

The first thing the CTO needs to do is try to understand why we see the same problem occurring repeatedly across a highly diverse collection of federal agencies. The Department of Homeland Security has 28 major projects on the Management Watch List. The Department of Education has 11. It is hard to imagine two agencies that have less in common, yet they both seem to be struggling with the same basic issue. In total, 352 major federal IT projects are on the Management Watch List. Could there be some factor that they all have in common?

Factor X

Let’s assume that there is a single factor that is causing all of these problems across all of these agencies. Let’s call this factor *Factor X*. Here is what we know about Factor X:

- Factor X is costing the U.S. taxpayers many tens of billions of dollars in direct costs and many times that in indirect costs.
- Factor X is reducing our ability to respond to terrorist threats (28 projects of the Department of Homeland Security are on the Watch List.)
- Factor X is reducing the effectiveness of our military forces (63 projects of the Department of Defense are on the Watch List.)
- Factor X is threatening the health of our citizens (29 projects of the Department of Health and Human Services are on the Watch List.)
- Factor X is reducing our ability to monitor volatile financial institutions (e.g. major failures in the Securities and Exchange Commission.)
- No branch of the U.S. Government is safe from the debilitating effects of Factor X.
- None of the tools or methodologies in use today by the federal government have been able to protect us against Factor X.

If all of these assertions about Factor X are true, does it not make sense that the identification and elimination of Factor X should be one of our highest national priorities? And if Factor X turns out to be within the purview of the Chief Technology Officer of the United States Government, does it not make sense that Factor X should demand this person’s complete and undivided attention?

I believe that Factor X does exist. Its name is *complexity*.

Complexity is the single factor that unites all of these troubled IT systems. It is the one IT issue that cuts across every federal agency from State to Treasury. It is the common enemy that attacks our health systems with the same relentlessness as it attacks our financial systems. If we could find an antidote to federal IT complexity, we could simultaneously reduce our tax burden, increase our security, and improve the effectiveness of our government in almost every area.

Critical Questions

There are then two critical questions. First, is it really true that complexity is the elusive Factor X? And second, is there a reasonable possibility that we could find an effective way to address complexity? If the answer to both of these questions is *yes*, then we need to give this issue a very high priority

The answer to the first question is clearly *yes*. Complexity is an increasingly serious problem in both private and public sector. A recent article in CIO magazine described the problem:

Within IT, factors that increase complexity include outsourcing management, the adoption of Web and consumer technologies, support for mobile workforces, developing and managing technology architectures and governance for those workforces, and ensuring security in a distributed environment.

Outside of IT's direct control, complexity is increased by the requirements of compliance, the need to support global business, and the speed and depth of access to information demanded by your customers and your partners.

CIOs can -- with difficulty -- handle these challenges individually, one at a time. But in the real world CIOs face many, if not all, of these challenges, all at once, over and over²⁰.

These factors all contribute to federal IT complexity. In addition, federal programs must cope with increasingly complex situations such as financial regulation, tax laws, and defense. There is little doubt that complexity is a factor that is shared by all of the troubled federal IT systems. In fact, it is the *only* factor I can think of that is common to all of these systems. Therefore complexity looks like our best candidate for Factor X.

The next question is, does a potential solution exist?

The current federal approaches have shown some promise. FEA is identifying potential areas for consolidation. EVM is giving us a way to identify problems earlier on in their delivery cycle. And the GAO is doing an excellent job of helping us understand where problems exist. But it is clear that something else is needed. If there is an antidote for complexity, we need to find it. There is far too much at stake to ignore this issue.

Let me start by suggesting some basic requirements for any hypothetical antidote for federal IT complexity.

- The antidote must be fully focused on the issue of complexity. We have other antidotes to deal with other issues. We need something to solve the complexity problem.
- The antidote must be testable. We must be able to ask the question, have we eliminated as much of the complexity from this system as possible? Could we do a better job?
- The antidote must be reproducible. It must not be based on the experience or proclivities of a given individual or group.
- The antidote must be technology neutral. It must not be based on any particular platform, language, infrastructure, toolset, or solution architecture.
- The antidote must be quickly scalable. It must be an approach that can be rolled out over the entire federal government.

One Possible Antidote

I believe there is a potential antidote for federal IT complexity. Before I describe this antidote, I need to offer a disclosure. I have been focusing on the problem of IT complexity for most of the last decade. I have been refining a methodology that I believe offers unparalleled ability to reduce IT complexity, both in the private and public sector. This methodology is called *Simple Iterative Partitions*, or SIP²¹. My suggestions in this section are taken directly from SIP. So understand that while I advocate SIP or some variant of SIP as a solution to federal IT complexity, I am not an impartial observer of the SIP methodology.

Most large federal IT projects can be loosely broken down into four stages: requirements gathering, architectural development, coding, and deployment. The larger the project, the more likely it is that errors will be made in each of these stages. And to make matters worse, these errors are cumulative (errors in requirements re-manifest themselves as errors in architecture which re-manifest themselves as errors in coding, and so on.) It is the accumulation of these errors that puts large projects in jeopardy. It is critical, therefore, to keep this error rate as low as possible.

The main factor determining the error rate is the complexity of the project. And the complexity of the project is largely determined by the amount of functionality in the project. The greater the amount of functionality in the project, the greater the complexity and the greater the error rate. The lower the amount of functionality in the project, the lower the complexity and the lower the error rate.

The trick, then, is not to do large projects. Instead, do small projects. By partitioning a large project into a number of small projects, you reduce the complexity of the project as a whole.

The problem is that when you partition one large project into a number of smaller projects, you introduce two new types of complexity.

The first type of complexity introduced is the complexity of managing multiple small projects rather than a single large one. I'll call this *management complexity*.

The second type of complexity introduced is the complexity of having the multiple pieces work together in some type of coordinated workflow. I'll call this *workflow complexity*.

Both management and workflow complexity are highly dependent on exactly how you have partitioned the project. If you partition the project correctly, you introduce a minimum of both management and workflow complexity while greatly reducing your project complexity. If you partition incorrectly, you introduce more management and workflow complexity than you save in project complexity.

To ensure that you achieve the best possible partitioning, SIP introduces a new stage into the project lifecycle. It is the *partitioning stage*. This stage occurs even before the requirements gathering stage. In this stage, we partition the project into optimal, smaller autonomous projects based on business function synergies and we then identify the workflow relationships between them.

We can demonstrate mathematically that when a project is partitioned correctly, we achieve the best possible balance between reducing project complexity and increasing management/workflow complexity. We can also use a mathematically based validation methodology to ensure that the partitioning we have proposed is the best possible partitioning from a complexity reduction perspective.

Once we have completed the partitioning stage, we move onto the requirements gathering stage, the architecting stage, the implementation stage, and the deployment stage. But each of these is done only within the context of one of the smaller projects. Since each of these smaller projects is a fraction of the size of the pre-partitioned project the complexity and error rates are much lower.

Can SIP effectively address federal IT complexity? It is too early to know for sure, but it is certainly a candidate methodology that deserves close examination.

The Recommendation

There is overwhelming evidence that complexity is a major problem for federal IT projects, costing us astronomically in both dollars and in governmental efficiency. If any foreign country threatened the U.S. national security as much as complexity does, the U.S. government would respond immediately. The fact that complexity comes from within makes it no less of a national threat.

The absolute highest priority for the new federal CTO is to declare a War on Complexity.

Specifically, I recommend the following steps:

- Drive a consensus on the need to control complexity.

- Identify candidate methodologies that show promise in helping control complexity.
- Test the candidate methodologies in real life scenarios.
- Choose the one that does the best job of controlling complexity.
- Train project managers throughout the federal government in the use of that methodology.
- Require the use of that methodology on all new IT projects.
- Continuously reevaluate and refine the methodology.

Complexity is a huge problem, but it is a solvable problem. President Obama has made an excellent start by promising to name a Chief Technology Officer for the federal government. If that CTO can wage an effective War on Complexity, that person will have made an incalculable contribution to the United States of America, and perhaps, to the world as a whole.

Bio



Roger Sessions is the CTO of ObjectWatch, a company he founded thirteen years ago. He has written seven books including *Simple Architectures for Complex Enterprises* and dozens of articles. His specialty is IT Complexity Analysis and he consults with private and public sector clients around the world. He holds multiple patents in software and architectural methodology. He is a Fellow of the International Association of Software Architects, Editor-in-Chief of the Perspectives of the International Association of Software Architects, and a Microsoft recognized MVP in Enterprise Architecture. He has given talks in more than 30 countries, 70 cities and 100 conferences on the topic of IT Complexity and Enterprise Architecture. He lives in Chappell Hill, Texas. He can be reached at roger (at) objectwatch.com.

References

(1) Position Paper: *Barack Obama: Connecting And Empowering All Americans Through Technology And Innovation*

- (2) Budget of the United States Government, Fiscal Year 2009, Analytical Perspective, published by the Office of the President of the United States, page 169.
- (3) Information Technology: Agencies Need to Establish Comprehensive Policies to Address Changes to Projects' Cost, Schedule, and Performance Goals. GAO Report GAO-08-925.
- (4) GAO Testimony before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate, July 31, 2008.
- (5) The Electronic Fraud Detection System Redesign Failure Resulted in Fraudulent Returns and Refunds Not Being Identified, Office of the Treasury Inspector General for Tax Administration, August 9, 2006, Reference Number: 2006-20-108.
- (6) Report 2008-10-172 to the Internal Revenue Service Deputy Commissioner for Services and Enforcement by the Treasury Inspector General for Tax Administration.
- (7) Homeland Security: U.S. Visitor and Immigrant Status Indicator Technology Program Planning and Execution Improvements Needed. Report by the General Accounting Office (GAO-09-06)
- (8) Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. Report by the General Accounting Office (GAO-08-525).
- (9) Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program, Report by the General Accounting Office (GAO-08-280).
- (10) Comparison of the Top Four Enterprise Architecture Methodologies by Roger Sessions. Available at [www.objectwatch.com / White Papers](http://www.objectwatch.com/WhitePapers).
- (11) Budget of the United States Government, Fiscal Year 2009, Analytical Perspective, published by the Office of the President of the United States, page 158
- (12) *ibid*, page 159.
- (13) Position Paper: *Barack Obama: Connecting And Empowering All Americans Through Technology And Innovation*, page 6.
- (14) The National Programme for IT Implementation Guide, December 2006.
- (15) *Simple Architectures for Complex Enterprises* (2008) by Roger Sessions, Microsoft Press.
- (16) Position Paper: *Barack Obama: Connecting And Empowering All Americans*

Through Technology And Innovation, page 6,7.

(17) DOD and VA Have Increased Their Sharing of Health Information, but Further Actions Are Needed. GAO Report 08-1158T

(18) OMG and Agencies Need to Improve Planning, Management, and Oversight of Projects Totaling Billions of Dollars, GAO Report 08-105IT.

(19) Position Paper: *Barack Obama: Connecting And Empowering All Americans Through Technology And Innovation*, page 5.

(20) Strategies for Dealing With IT Complexity, CIO Magazine, December, 2007

(21) *Simple Architectures for Complex Enterprises* (2008) by Roger Sessions, Microsoft Press.