TESTIMONY OF
Richard A. Spires
Independent Consultant
Before the
House Committee on Oversight and Government Reform
November 13, 2013

Chairman Issa, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to testify on issues with the development and deployment of HealthCare.gov as well as the Administration's plan to address the problems associated with the website. I bring more than 30 years of experience working on the delivery of information technology (IT) programs. In the private sector, I helped deliver large, complex IT systems to clients in the financial services and telecommunications industries. I spent 4 ½ years at the Internal Revenue Service (IRS), with 2 ½ of those years serving directly as the Program Manager of the Business Systems Modernization Program, a multi-billion effort to modernize tax processing systems in the IRS. Most recently, I spent nearly four years as the Chief Information Officer (CIO) at the Department of Homeland Security (DHS), where I had oversight responsibility for more than 90 major IT programs. Hence for more than eight years I had the privilege of serving the Federal Government in a number of senior-level IT positions, in both the President Bush and President Obama Administrations. I have seen the same set of IT management issues in both Administrations, so I ask that my remarks be viewed as highlighting systemic weaknesses in our ability to effectively manage IT, not as a criticism of either Administration.

In regards to the rollout of HealthCare.gov, my observations are based solely on public information I have gleaned through the media and listening to the various Congressional hearings. I was never close to the planning or development of the HealthCare.gov website and supporting back-end systems. In full disclosure, however, I did participate in one HealthCare.gov planning session a couple of years ago when I was DHS CIO. The session was to ensure various agencies (including DHS) identified the individuals to work with the Centers for Medicare and Medicaid Services (CMS) on the required data-sharing to support the enrollment process.

The troubled launch of HealthCare.gov pains me – as someone who has great passion for wanting to make government IT more effective, this public spectacle once again casts federal IT in a very negative light. As a federal IT community we appear unempowered, and worse, incompetent. I hope through this testimony to make a case for serious change that is much needed in how the government manages IT. To set context for my recommendations for change, I first outline the key elements that are required to successfully deliver a large-scale complex IT program in government. Based on what I do know of the HealthCare.gov launch, I will touch upon issues related to those key elements. In particular, I will focus on the importance of organizations' roles and the governance model to ensure proper transparency and decision

making to maximize a program's chances for success. Lastly, I will make general recommendations on how to significantly improve IT management in government; recommendations that would not only help government operate more effectively and efficiently, but would help avoid the types of problems that we see all too often in large IT programs, like what has happened with HealthCare.gov.

Key Elements for IT Program Success

When I am involved in establishing a new large-scale complex IT program or assessing the health of an on-going program, I address five key elements. Each of these elements is critically important, and if any one of them is not being addressed appropriately, it raises risk significantly and can lead to outright program failure. Further, while it is critical to have constant vigilance regarding each element throughout a system's design, development, and implementation, I have found that most troubled programs make major mistakes right out of the starting blocks. Hence, I place tremendous importance on ensuring the program properly addresses all five areas as it launches. Below I give high-level descriptions of each of these five key elements.

The first key element is ensuring that there are a ***set of mature management processes*** used in running the program. There must be an appropriate system development life cycle, which lays out the approach(es) that will be used to design, develop, test, and deploy the system. For complex systems such as HealthCare.gov, there may be different approaches for the various subsystems. Modern development approaches, in particular modular approaches, can help simplify and lower development risk. For instance, an agile development methodology is appropriate for developing the user interface and business logic for customers to interact with the website. A more traditional development approach might be used for the data hub, in which requirements and data specifications could be defined prior to development.

In addition to establishing the proper development life cycle(s), the program must establish a robust set of project management disciplines, which include, for example, schedule, estimation, requirements, configuration, and risk management processes. In a program as complex as HealthCare.gov, which contains multiple subsystems, I would be particularly interested in the integration management processes that would be used throughout the life-cycle of the program, again to lower overall delivery risk.

The second element is ensuring there is a ***solid business architecture that is supported by a solid technical architecture***. Simply, the business architecture describes the overall process of what the system must do to support the business or mission outcomes desired. There are many failure mechanisms for programs, but I am surprised how often there is not a solid high-level business architecture in place early in the program's life – if not it typically leads to major requirements changes during system development, testing, and deployment. Further, there should be an effort to simplify, to the degree possible, the business processes and determine the minimum required capabilities for an initial system launch. This can greatly reduce program risk.

Having a solid technical architecture in place, especially for a complex system with a number of subsystems, is absolutely critical. First, if there are subsystems that can be "bought" or repurposed from other systems the meet requirements, the government ought to do so – it lowers risk substantially to buy rather than build. There should be the proper use of off-the-shelf software components, whether they are offered by traditional software vendors, or appropriate use of open source capabilities. Yet there should also be overall simplicity in technical architecture – integration of dozens of off-the-shelf components creates its own set of technical complexities. Problems with the technical architecture tend to show up late in the development life cycle during integration and end-to-end testing, typically resulting in performance and scalability problems.

The third element focuses on organizations' roles, commitment, and governance. There must be a ***program governance model in place that recognizes the proper roles and authorities of the important stakeholders***, to include the business (or mission) organization, IT, procurement, privacy, etc. In particular, for IT programs, the business organization must be intimately involved in helping define requirements, making hard functionality trade-offs, and being a champion for the program with stakeholders both inside and outside the Agency. The IT organization must ensure there is a capable program management office (PMO) using management best practices to deliver large IT programs (delivering on the first key element above). There also should be a formal program governance board in which executives from all the key stakeholder organizations meet regularly to support the program manager (PM) in running a program. Transparency and good communications amongst the stakeholders are critical for success. So many programs falter because the stakeholders are pulling the program in differing directions; an effective governance structure will drive stakeholder alignment and provide clear and informed decisions for a PM to rely upon.

Executing elements one through three well is not possible without ***a set of skilled and experienced personnel that are leading the program***. This goes beyond the Program Manager, but also includes a Requirements Manager, Systems Architecture Lead, Test Manager, Deployment Manager, etc. For Federal Government programs, my experience is that having government personal fill most of these leadership roles is necessary. While contractor personnel can support a PMO, it is difficult to have them in leadership roles in the PMO, given the need to build strong and trusted partnerships with other stakeholder government staff. The most common reason large IT programs fail is the lack of properly skilled and experienced leadership in the PMO.

The fifth and last key element is developing the ***proper relationships with the contractor(s) that are supporting the program***. Government cannot execute large IT programs without outside support. These proper relationships have both formal and informal aspects. The formal aspect is the contract, in which the scope of work, terms, and incentives are codified. This is where the procurement organization, with the contracting officer(s) being part of the team, need to work closely with or even be embedded as part of the PMO to make sure contracts are structured in

such a way to best support what the program is working to achieve. The informal aspect is the management of the contractors via the PMO. I always look for a program in which the contractors are well integrated into the program, well understand their roles, others' roles, and there is open and candid communications amongst the parties. This type of environment will enable issues to be identified early, innovative ideas to be surfaced and discussed, and informed decisions made.

These are the five key elements for large IT program success, and they lead to some insights that are not well understood by people who have not been in the business of managing large complex IT programs. First, ***the proper management of the program is paramount (elements one through four) and is more important than the procurement process to choose the contractors supporting the program.*** You can have highly competent contractors, solid contracts, and will have a fiasco of a program without a solid PMO. But if you start with a competent set of leaders running a PMO, they will quickly deal with non-performing contractors either through working to get their performance up to par or replacing them if warranted. Some Federal Government agencies are putting more emphasis on working to address procurement issues. We hear terms like "fix how we buy IT". Certainly we need to address procurement issues, but the government did not "buy" HealthCare.gov, it had to create it. There is commodity IT (I put much of IT infrastructure in that category) that can be bought. But HealthCare.gov is an example of the government creating a unique system to meet the public's needs as part of the rollout of the Affordable Care Act (ACA) and using a cadre of contractors to support that creation. In such systems, it is the capability of the PMO that will determine the ultimate success of the system.

Many people observe the problems with HealthCare.gov and believe that government cannot properly manage such complex programs so the government should outsource the program management completely to a contractor. Yet my own experience and looking at many other major government programs leads to the insight that the ***government outsourcing the program management of its large, complex IT programs is even more risky***. A number of Agencies, to include the IRS and Coast Guard, have tried to outsource the program management to contractors in the past, with very poor results. When I came on board with IRS in 2004 to take over the Business Systems Modernization (BSM) program, the model was an outsourced PMO. It took me only a couple of weeks to conclude that model was not working and could never work. The Prime contractor for the BSM program could not build the necessary trusted relationships with the key stakeholders across IRS to be successful. That had to be handled by government employees. As a team we worked hard over the next few years to build the talent base to take on the functions of IRS becoming its own integrator and running the BSM program. That shift, ongoing maturing of the IRS program management processes, and subsequent successes of the BSM program led to GAO removing IRS modernization from its high-risk list earlier this year.

Observations on HealthCare.gov Development and Launch

My knowledge of the HealthCare.gov program is based strictly on testimony of others and the media reports. Even so, there is pattern recognition for those of us who have been involved in many large IT programs, and in regards to the rollout of HealthCare.gov, it is clear that:

1. There are fundamental weaknesses in the program management processes (element one). For a system as complex as HealthCare.gov, best practice would have led to a plan that included: completion and testing of all subsystems six months prior to public launch; three months of end-to-end functional integration testing; concurrent performance testing that would have simulated loads up to 10 times greater than expected (especially since it was difficult to model expected peak loads); and a subsequent three month pilot phase in which selected group of users were using the system to identify problems not caught in testing. It was reported that the program did not start end-to-end functional testing till two weeks prior to launch, the performance testing did not anticipate the volumes seen on day 1, and there was no formal pilot program prior to rollout. All of these are evidence of a lack of mature program management processes.

2. Regarding role assignment and authorities (element three), the evidence on the launch of HealthCare.gov shows the balance between the business and IT organizations was not correct. Two examples clearly show this. As reported by the media, a change in a requirement that disabled the ability for users to browse insurance policies without first enrolling was made just two weeks before launch. This was much too late -- requirements should have been locked down months before then. Second, the launch date of October 1 was deemed immovable. As development schedules slipped, as integration challenges mounted, there were clearly compromises made so as not to delay the launch. I suspect little functionality could be deferred (the site must enable the full enrollment process), so what was compromised is good practice. It is simply bad practice to launch a complex system with very little end-to-end testing. There is no excuse for this, and given the complexity of systems CMS operates, there are clearly individuals in the PMO who knew this launch would not go well because of inadequate testing. This clearly indicates the business organization had the ability to make changes that led to bad program management practice.

3. Based on contractors' testimony and the media reports regarding warnings to the government regarding issues with HealthCare.gov, there were not the proper informal relationships with the contractors (element five). Ample warnings and recommendations were given by contractors responsible for the development of the subsystems. Perhaps there was serious consideration given to those warnings and recommendations, but in the end, it did not alter the government's decision to go live with a system that was not ready.

Further, regarding the decision to go live on October 1st, there must have been internal discussions as to whether it was best to go live with a system that had not been adequately tested, or delay the go-live date and receive criticism for having such a delay. I have been part of the PMO on a number of programs in which we had to make a decision regarding delaying a go-live date. My experience has been that it is always better to delay launch of system that is not ready, for two reasons. First, you only get one chance to make a first impression with users, and that is a lasting impression. But second, and more importantly, once you put a system into production you must operate and maintain it. This adds considerable burden to the program team at the very time it is under the most pressure to fix known problems. This extra burden lengthens the time to get the system stable and fully functional.

Lastly, the Administration is claiming that HealthCare.gov will work well for the vast majority of the users by the end of this month. They are making this prediction based on the punch list of items they are working off. I hope they are right on the timing, but my prior experience suggests that is still an aggressive schedule. Again, I have two reasons. It is always surprising to me during integration testing how many new problems (software "bugs") are uncovered as you correct known problems. In addition, sometimes there are technical architectural issues that are only uncovered during the integration testing period. If any such issues exist, it may require significant rework that could elongate the schedule.

Recommendations to Improve IT Management

The issues with the rollout of HealthCare.gov are emblematic of the IT management problems in the Federal Government. But addressing IT management is not just about having a smoother launch of a system such as HealthCare.gov or even the ability to save ten to twenty percent of the $80 billion IT budget, though both of those are quite important. Leading corporations in almost all industries harness and manage IT to transform the way they conduct business and give them distinct competitive advantage. Our government, if it more effectively manages IT, can likewise harness such transformational capability, significantly improving government's effectiveness and efficiency in both its mission and business operations.

I recommend that three actions be taken to improve Federal Government IT. First, it is important for Congress to pass legislation to update how this government manages IT. I appreciate the leadership of Chairman Issa and Representative Connolly in co-sponsoring the Federal Information Technology Acquisition Reform Act (FITARA) legislation. While legislation alone will not fix all issues with IT management, it will elevate the standing of Agency CIOs and put in place mechanisms for development of "Centers of Excellence" in which best practices in program management and acquisition can be developed and leveraged across the Federal Government. These changes could have helped to address some of the critical failings of the program management of HealthCare.gov, giving the IT organization more authority to ensure best practices were used, and a means by which the program could have tapped experts, both during the start-up phase of the program, and as it began to have execution problems.

Second, Agency CIOs need to have control over implementation, operations, and the budget of all commodity IT in their Agency, which includes the data centers, cloud services, servers, networks, standard collaboration tools like e-mail, as well as back-office systems supporting functions to include finance and human resources. A couple of years ago, I was fortunate to be in a session that included a number of the CIOs for Fortune 50 companies, organizations in which IT has been a true competitive discriminator. In the course of the discussion, it became clear that one the key elements in effectively leveraging IT for an enterprise is the modernization, standardization and appropriate consolidation of the underlying IT infrastructure. All the CIOs concurred that while one objective was to be more efficient and save money in IT infrastructure, such consolidation enabled more effective and timely delivery of new capabilities for their business customers, and improved the overall IT security posture of their organizations. I urge Congress to address this recommendation through the IT Reform legislation and the Administration to address this recommendation through the PortfolioStat process.

Lastly, the current Administration should make IT management a centerpiece of its overall management reform agenda. This entails the recognition and focus at the most senior levels of government of the importance of IT and improving IT management, and the empowerment and elevation of Agency CIOs. It includes a serious commitment to improving program management practices, and ensuring the Agency CIOs own the commodity IT for their Agency. Yet it also includes ensuring those Agency CIOs have the requisite skills and experience to carry out a larger and more expansive role. Just elevating and empowering CIOs is not enough; we need a cadre of experienced and capable individuals that can lead this government in making effective use of IT.

Conclusion

The troubled launch of HealthCare.gov has put a spotlight once again on the issues of Federal Government IT program management in particular, and IT management in general. I hope the government can use this episode as a catalyst to drive positive change in the way we manage IT. This is about making government more effective and efficient, which is a bi-partisan issue. The best practices exist and are proven. We need leadership in Congress to pass reform legislation and leadership in the Administration to recognize the importance of IT management as part of its management reform agenda. Thank you.

Richard A. Spires

Richard A. Spires currently serves as an independent consultant specializing in senior-level operations and information technology issues for large-scale corporations, IT product companies, and US Federal Government entities.

Mr. Spires was appointed and served as the Department of Homeland Security's (DHS) Chief Information Officer (CIO) from August 2009 till May 2013. In this capacity, Mr. Spires was responsible for the strategy and operations of the department's annual $5.6 billion investment in Information Technology (IT). Mr. Spires was the chairman of the DHS Chief Information Officer Council and the Enterprise Architecture Board. Mr. Spires also served as the Vice-Chairman of the Federal Government CIO Council and the Co-Chairman of the Committee for National Security Systems (CNSS), the committee that sets standards for the US Government's classified systems.

Mr. Spires held a number of positions at the Internal Revenue Service (IRS) from 2004 through 2008. He served as the Deputy Commissioner for Operations Support, having overall responsibility for the key support and administrative functions for the IRS, to include Information Technology, Human Capital, Finance, Shared Services, Real Estate, and Security functions. Prior to becoming Deputy Commissioner, Mr. Spires served as the IRS' CIO, with overall strategic and operational responsibility for a $2 billion budget and a 7,000-person Modernization and Information Technology Services organization. Mr. Spires led the IRS's Business Systems Modernization program for two and half years, which is one of the largest and most complex information technology modernization efforts undertaken to date.

From 2000 through 2003, Mr. Spires served as President, Chief Operating Officer, and Director of Mantas, Inc., a software company that provides business intelligence solutions to the financial services industry. In helping to establish Mantas, Mr. Spires successfully led efforts to raise $29 million in venture funding. Prior to Mantas, Mr. Spires spent more than 16 years serving in a number of technical and managerial positions at SRA International.

Mr. Spires received a B.S. in Electrical Engineering and a B.A. in Mathematical Sciences from the University of Cincinnati. He also holds a M.S. in Electrical Engineering from the George Washington University. Mr. Spires has won a number of awards for his leadership in IT, to include the 2012 Fed 100 Government Executive Eagle Award, TechAmerica's 2012 Government Executive of the Year, Government Computer News 2011 Civilian Government Executive of the Year and was named a Distinguished Alumnus of the University of Cincinnati's College of Engineering in 2006.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: Richard A. Spires

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2010. Include the source and amount of each grant or contract.
Subcontract from Nester Consulting, LLC (dba GovernmentCIO) to Richard A. Spires Consulting in support of a competitively won solicitation (No: ED-FSA-13-R-0033) to provide Virtual Data Center (VDC) Strategy Consulting Services to support the CIO Organization at Federal Student Aid, U.S. Department of Education. Date of subcontract was August 28, 2013 with a ceiling of $13,000.

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with those entities.
I am not representing any entity other than myself. I currently operate as an independent consultant under a sole proprietorship of Richard A. Spires Consulting.

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2010, by the entity(ies) you listed above. Include the source and amount of each grant or contract.
Not applicable.

I certify that the above information is true and correct.

November 11, 2013