STATEMENT OF
KAREN S. EVANS
FORMER ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
November 13, 2013

Good morning Chairman Issa, Ranking Member Cummings, and Members of the Committee. I am pleased to be invited back to share my views on "ObamaCare Implementation: The Rollout of HealthCare.gov" My remarks today will discuss best practices for major Information Technology (IT) systems implementation, how policy decisions drive the technical specifications for IT systems, and the role of the CIO in elevating these decisions to policy officials.

Typical IT Major Project Failure

From an IT implementation standpoint, Healthcare.gov was a classic IT project failure that happens in the Federal Government too frequently. As the executive leadership of Federal departments and agencies, the President's political appointees are at the top of the management chain for Federal employees and contractors. In looking for the cause of this failure, some point to the lack of testing. Others, including the President, cite the challenges of the IT procurement process. And still others note the complexity of the program and the interfaces with private insurance company systems. However, the cause of this failure was not the complexity of the program, nor the procurement process, nor the testing. The functionality and shortcomings of Healthcare.gov are the result of bad management decisions made by policy officials within the Administration; they did this to themselves. And if they are now surprised, it is because their own policy officials failed to inform them of the decisions they had made and the consequences associated with those decisions.

Policy Decisions Needed

As soon as this legislation was passed, there were policy decisions which needed to be made. These policy decisions would drive the technical design of the Healthcare.gov IT system; they fundamentally determined the work flow and business processes driving how the law would be implemented.

I've been on both sides of policy implementation - as a career civil servant and as a political appointee. The problems with Healthcare.gov are symptomatic of a recurring problem: Passing a law or issuing a policy is not enough. If there is a new law, management reform, or policy initiative you want to accomplish, then you, as the policy official, need to be engaged during the implementation to assure there is an appropriate integrated project team in place to manage the day-to-day operations. All levels of the organization need to be willing to get "in-the-weeds," to understand these intricate aspects of management and implementation, because the devil is in the

details; someone can change a seemingly innocuous requirement in a meeting and cause a huge impact on schedule, cost, or functionality. IT projects are particularly good at highlighting management failings because they require coordination between many different parts of an organization. If the agency CIO is not actively at the management table, participating in those decisions and, more importantly, explaining the ramifications of the policy decisions they are making, then projects get off-track and ultimately fail.

For example, one policy decision that is causing problems with Healthcare.gov was whether the system had to verify the identity of an individual before allowing the user to browse the marketplace. That is a policy decision, not a technical decision. Technology can actually do whatever is required. The policy decision that drove the technical implementation created a bottleneck at the front end. I do not want to speculate on why this identity verification option was selected. But the generally accepted procedure and best practice for decisions on implementation requirements is to list each possible viable option along with the advantages and disadvantages of each.

Another policy decision was the requirement to directly interface with insurance provider systems and with other government systems at IRS and SSA. Again, these were not technology questions; the technology exists. And these were not statutory requirements; the law did not say, "the system shall interface to system X at the IRS." These implementation requirements were driven by policy decisions and arbitrary interpretations of the law. Such questions must be answered by policy officials because they require value judgments and cost-benefit trade-offs. For example, "Does the IRS have to verify the identity of people, or can a private insurance agency do that?" You're seeing this play out now with the issues of determining eligibility for subsidies and concerns about improper payments. Unlike the regulatory process, the functional specifications driven by these policy decisions are not necessarily subject to the public notice and comment rulemaking process. These are huge management and implementation issues that need to be reviewed from both a political and policy perspective.

A former CMS senior executive, when the management failures came to light, said in a recent interview that he did not see the launch of Healthcare.gov as a major part of his job. Rather, he said, "Those were staff level functions,"[1] while he focused on more important policy issues. However, these implementation management questions were driving massive requirements for system implementation, and that was going to impact the timeline of the system launch. For any political appointee, the IT system implementing a major Presidential policy initiative must be highest priority, and this must be communicated to their entire team.

Elevate Policy Questions

The Chief Information Officer (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. When a technical implementation specification hinges on a policy decision, the technical team depends upon the CIO

1 Boston Globe, October 24, 2013

to elevate the question to the appropriate decision maker. Because the CIO can speak to senior executives in terms that are relevant to them, and can state potential consequences in terms of political and policy values (e.g. public opinion, unfavorable news stories), the CIO is in the unique position to ensure that policy officials do not regard these decisions as "staff level functions." And if these potential consequences are significant, then Departmental and White House officials may need to be briefed by their CIOs.

For example, during my tenure as the OMB E-Gov Administrator, the FBI Virtual Case File (now knows as Sentinel) program faltered. In my management oversight role, I began meeting weekly with the Department CIO, the Bureau CIO, the program management staff, and the contractors - all in the same room - so that I could understand the project and raise policy issues to White House senior officials as necessary. This "integrated project team" or "IPT" developed an agreed upon project plan to correct the deficiencies and move forward.

Focus Management Attention

In addition to elevating policy decisions to White House officials, the E-Government Act[2] directs the Administrator to help improve the management of IT in the agencies. During my tenure, I 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 in IT management tools (e.g. earned value management), would readily know the status of projects in their agency, and could call me if they had questions. And I was able to flag suspicious or obviously incorrect data for further investigation of those projects.

Pressure to Succeed

Recent news stories indicate that a CMS official signed the authorization for Healthcare.gov to "go live" without the system having undergone adequate testing. While this may have satisfied the statutory requirements of FISMA[3], it certainly circumvents the intent of the law. Here again, the CIO is in a unique position to ensure that senior executives understand the decisions they're being asked to make, and the implications of each option available to them.

Establish a Go/No-Go Milestone Date

Some have cited the tremendous pressure of public expectations as compelling administration officials into the decision to "go live." But again, this was a situation of their own making. Any high profile project should establish a go/no-go milestone, and stick to it. A go/no-go milestone is simply a date by which the project must have completed a specific, measurable amount of progress in order for the entire project to be completed by the due date. Thus, you know that if you haven't met the milestone by the date, you're not going to make it. In this case, having a go/no-go date for Healthcare.gov, perhaps a year before the go-live date, would have allowed the President and

2 E-Government Act of 2002, PL107-347

3 Federal Information Security Management Act of 2002, Title III of PL107-347

his advisors to manage public expectations, to develop a fallback plan and provide the remediation plan to address the known deficiencies.

For example, when we were initially implementing Homeland Security Presidential Directive-12, (HSPD-12), the President's directive requiring uniform employee identification cards at all agencies, we had publicized the planned completion date. But when we reached our go/no-go date, we had failed to complete the key milestone, so we knew were not going to meet the announced completion date. Because of that, I was able to notify senior policy officials well in advance of the announced completion date. This allowed us to formulate a corrective action plan with each department and agency, and to develop a communications plan to temper the expectations of the public and the press; instead of crashing on the runway, we got on the PA system and told everyone we were going to circle around for another landing attempt.

The Role of the CIO

In the wake of the Healthcare.gov implementation failure, some analysts have asserted that the private sector could have done this better, thereby implying that there is some condition inherent in Federal IT which impedes success and impairs Federal CIOs. It is certainly true that Federal CIOs are burdened by the deliberate restraints placed upon them by the Congress and OMB. But Federal CIOs also enjoy freedom from competition and the whims of the market. Overall, Federal CIOs and Commercial CIOs are more similar than different. And we have the same job description: to be the technology-savvy member of the executive management team, to provide value through innovation, to manage data as a strategic asset, and to lead a large team of technologists and inspire them to achieve greatness. Whether a CIO is at a large organization or small, bureau level or department level, public sector or private; the scale may differ, but the management challenges are the same. Attachment A includes some key questions which every CIO should be asking but more importantly the CIO should be able to answer these questions for their leadership in clear business terms.

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

Attachment A - IT Management Checklists

Vetting potential new investments - Does the project sponsor have a clear vision of what he/she is trying to accomplish and how the IT system will support the new product or service? CIOs should evaluate the sponsor's answers to these questions:

For this program/project:

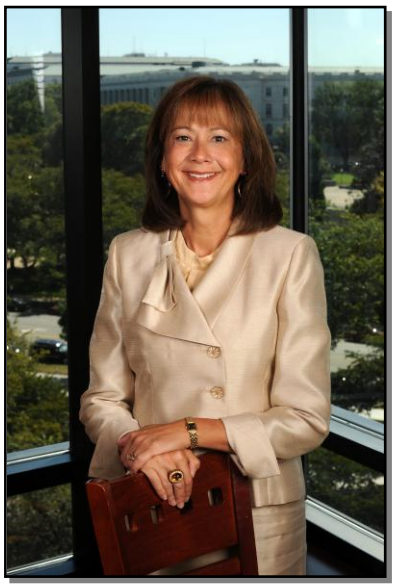
- ✓ What will be different?
- ✓ What problem are you solving?
- ✓ When do you need to be complete?
- ✓ How will you measure success?
- ✓ What does it cost?
- ✓ Are you being realistic?

Six Keys to Success - These six attributes reflect lessons-learned from numerous IT projects in both government and private industry. While these elements do not guarantee success, the absence of any one of them almost certainly will guarantee failure.

- ✓ Strong Executive Leadership;
- ✓ Well-Defined Governance Models;
- ✓ Alignment with budget process;
- ✓ Clearly Defined Outcomes and Performance Measures;
- ✓ Accountability and Transparency; and
- ✓ Stakeholder Outreach.

KAREN S. EVANS

Karen S. Evans is serving as the National Director for the US Cyber Challenge (USCC). The USCC is the nationwide talent search and skills development program focused specifically on the cyber workforce. She serves as a Voice of Authority for Safegov.org, an on-line forum specifically focused on cloud computing policy issues. She is also an independent consultant in the areas of leadership, management and the strategic use of information technology. She retired after nearly 28 years of federal government service with responsibilities ranging from a GS-2 to Presidential Appointee as the Administrator for E-Government and Information Technology at the Office of Management and Budget (OMB) within the Executive Office of the President. She oversaw the federal IT budget of nearly $71 billion which included implementation of IT throughout the federal government. This included advising the Director of OMB on the performance of IT investments, overseeing the development of enterprise architectures within and across the agencies, directing the activities of the Chief Information Officers (CIO) Council, and overseeing the usage of the E-Government Fund to support interagency partnerships and innovation. She also had responsibilities in the areas of capital planning and investment control, information security, privacy and accessibility of IT for persons with disabilities, and access to, dissemination of, and preservation of government information. Included in her accomplishments are making IPv6, HSPD-12, and SmartBUY (which is leveraging the federal government requirements) a reality; elevating the importance of transparency with the publication of the Management Watch List and High Risk List projects; increasing the focus on cybersecurity to include the Federal Desktop Core Configuration for the government; and balancing the expanded use of technology for citizen services with increasing demands for privacy.



Prior to becoming the Administrator, Ms. Evans was the Chief Information Officer for the Department of Energy. There she was responsible for the design, implementation, and continuing successful operation of IT programs and initiatives throughout the Department. During this time, she was the Vice-Chairman of the Federal CIO Council. Elected to the post in December 2002, she coordinated the Council's efforts in developing federal IT programs and improving agency information resources practices.

Before joining Energy, she was Director, Information Resources Management Division, Office of Justice Programs (OJP), U.S. Department of Justice, where she was responsible for the management and successful operation of the IT program. OJP's bureaus and offices provide funding opportunities for initiatives such as Safe Schools, Safe Start Program, Community Prosecution, Native American Tribal Courts and other programs of high local, state and national interest. Key accomplishments included the implementation of an on-line grants management system to process grants from discretionary, formula and large block grants programs, to streamlining capabilities to ensure for the expeditious processing of claims benefits to families of public safety officers after the September 11th attacks.

She currently serves as a Director on the boards of the NIC, Inc; Center for Internet Security; The Department of Veterans Affairs Acquisition Academy and Women in Technology Education Foundation and is advisory board member for several information technology companies. In addition, she chaired the West Virginia University MBA Advisory Board where she recently was inducted to the roll of distinguished alumni.

Recent honors also include election to National Academy of Public Administration and the University of Maryland University College's Cybersecurity Leadership Award.

She holds a Bachelor's degree in Chemistry and a Master of Business Administration degree from West Virginia University. She resides in Martinsburg, WV with husband, Randy and her two children, Jake and Samantha.

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

Name: Karen S. Evans

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.

-Research cooperative agreement competitively awarded by the Air Force Research Lab (AFRL) on behalf of the Department of Homeland Security (DHS) Science and Technology Directorate for competitions as they relate to cyber security workforce issues. The cooperative agreement is for one base year with three options in the amount of $502,861 per year.
-Honorarium from the Office of Personnel Management (OPM) for courses provided at the management development centers. These are competitively awarded and the honorarium fee is $1,000 per course.

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

N/A

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.

I certify that the above information is true and correct

Signature: Karen S. Evans

Date: 11/11/13