

Through the Government Looking Glass *Increasing Transparency Through Industry and Technology*

by Marla Tuchinsky and Christine Robers

Abstract

The American Council on Technology (ACT) and the Industry Advisory Council (IAC) hosted a discussion between more than 100 professionals, who shared ideas and brainstormed about how government and industry can work together. Participants defined the five pillars of transparent government proposed by CTO Aneesh Chopra and CIO Vivek Kundra, described what success would look like in two years, identified barriers and challenges to success, and came up with three to five actions to reach the goal.

This paper summarizes their discussions. Additional commentary highlights common elements across the pillars: cooperation between government agencies, cultural effects, accessibility of government and individual information, and cybersecurity.

Introduction

“What we need is a forum for candid conversation and collaboration.” In Washington DC, a city too often known for political divides and siloed behavior, we heard and experienced a new rallying cry among technology professionals from industry and government who gathered for dinner and discussion. More than 100 professionals shared ideas and brainstormed about how government and industry can work together to solve some of our critical IT needs; how technology can strengthen our government and make it more effective and efficient; how technology can facilitate innovation.

The American Council on Technology (ACT) and the Industry Advisory Council (IAC) hosted the event. To move its 2009 strategic agenda forward and begin to create a shared vision on technology under the Obama administration, ACT-IAC convened in a new format. Microsoft’s Teresa Carlson worked with Martha Dorris, out-going president of ACT, to arrange the dinner, which was facilitated by Kim Taylor-Thompson, CEO of Duke Corporate Education. Over the course of a meal, each table of participants would look at one the five pillars of transparent government proposed by CTO Aneesh Chopra and CIO Vivek Kundra. They were asked to agree on a succinct definition, describe what success would look like in two years, identify barriers and challenges to success, and come up with three to five actions to reach the goal.

This paper represents a summary of the proposed definitions, challenges and action items for each of the following five pillars of transparent government (see appendix for full descriptions):

1. Increase government transparency
2. Increase citizen engagement
3. Lower the cost of government operations
4. Promote and encourage innovation in government
5. Safeguard the computing environment

Further events will develop the thinking that resulted from the collaborative and lively discussion.

continued on next page ►

ACT is a non-profit educational organization established in 1979 to assist government in acquiring and using information technology resources effectively and efficiently. In 1989 ACT established the IAC to bring industry and government executives together to exchange information, support professional development, improve communications, and build partnership and trust, thereby enhancing government's ability to serve the nation. ACT and IAC work together to provide an objective, professional and ethical forum where government and industry leaders can collaborate on addressing common issues towards a shared vision.

*To be truly transparent,
the group felt a
fundamental change
was required...*

Increase government transparency

The discussion centered on transparency as a visible and understandable accounting of the government's use of its resources to achieve goals, with the purpose and benefit being "to promote innovation, improve performance, build trust and increase accountability."

To be truly transparent, the group felt a fundamental change was required — a move from a "need to know" policy and mindset of information sharing to an approach of sharing everything except what must be protected. Government must show citizens how money is spent and how decisions are made, sharing data in a timely and accurate manner.

Clearly, determining what information to share and what information to protect requires careful consideration. Some information must obviously remain secure, including items covered by the Privacy Act, contractually sensitive data and personally identifiable data. Citizens could play a role in defining when transparency can result in better government. Strategic planning and specific performance goals for transparency will also need to be established and monitored.

Transparency and information sharing may force government to more clearly define measures of success. Government transparency includes not just government-to-citizen transparency but also transparency between government agencies. Increased government transparency should result in improved citizen involvement and trust in the government process. In turn, government will be able to work together more seamlessly and deliver better services to citizens.

A clear definition of transparency must be established and accepted. Key challenges include:

- a lack of coordination and agreement in policies and processes among agency CXOs;
- security risks, as disparate data from various sources will need to be pieced together; and
- the potential for industry to become less collaborative and innovative as companies must share their data publicly.

In addition to performance metrics and measures, budget and guidelines for creating infrastructure for successful information sharing must be established.

Any government program under the transparency initiative should identify clearly what value it brings to citizens. To achieve success, communities of interest could be created, bringing federal, state, local, non-profit and industry stakeholders to address comprehensive and coordinated solutions for specific, shared problems. For example, increasing the number of teens graduating from high school requires action from various local, state and federal agencies such as HHS, HUD, ED, etc.

A defined rewards structure with a set of risk/reward metrics and incentives for government professionals will encourage cultural change at the agency level. Emphasis must be placed on inspiring innovation and change among CXOs.

continued on next page ►

Increasing Citizen Engagement

The core of the discussion was around “the government providing information and tools that enable interested parties to engage in the civic business of the country.” The intent is for people to know what’s happening and be able to participate. Although it’s tempting to say, “Let’s just put up some web sites for citizen comments and discussion boards,” most people in the conversation favored broad access and multiple avenues for citizen engagement.

A challenge, though, is balancing one set of citizen rights with another: how do we honor rights to free speech and open discourse and yet preserve the protections of the Privacy Act? How do we ensure equal access to all citizens (regardless of age, expertise or location) yet not have government agencies stall as they first absorb a potential avalanche of opinions?

Some initial areas for action might be those programs that touch more citizens directly, such as health care, housing (e.g., mortgage lending), education or retirement benefits. Find ways to allow people to more easily get information, research legislation in plain language, or offer their ideas on how they’d like to engage with their government. Another avenue is first to simplify the government; address outmoded policies/legislation and enforce measures designed to limit how much information the government collects, processes and stores. Finally, we could benefit from benchmarking: how do other nations engage citizens effectively and efficiently?

Lower the cost of government operations

This discussion was about value and leverage, specifically about how to lower the cost of services to citizens while increasing the value. A critical challenge is the silos in which agencies operate, and the redundant systems for common services. For example, project management, identity management and clearances could fall under a single architecture -- but right now, they don’t.

Participants discussed why operations aren’t as cost-effective as they might be. Part of the problem is how agencies are set up, monitored and budgeted. OMB funding and monitoring happens within agencies, not between. So, two agencies may provide similar services but are budgeted and evaluated separately, and may not even be aware that they could partner on those services. Given the need to project 2-4 years out, some agencies aren’t able to accurately predict costs, so they over-budget to err on the safe side. Yet there may not be demand to revise estimates downward.

A solid first step would be to identify opportunities for collaboration across agencies, around systems or services. OMB examiners might be well-positioned to spend time in the agencies and highlight specific programs for partnerships or services that could move to a shared services agency. What are the core processes for agencies to accomplish their missions and how can they be streamlined and aggregated? Another step might be to aggregate Federal purchasing power for technology buys, such as software licenses. Finally, participants suggested creating a scorecard focused on results instead of level of activity – an ROI for government services in place of a McDonald’s-like “2.25 million served” measure.

Promote and encourage innovation in government

Innovation is applying new practices, processes or tools to produce a valuable outcome. It involves experimenting to find better solutions to complex problems, or getting to a desired outcome in a cheaper, faster or better way.

continued on next page ►

One of the big challenges to being innovative in government is the culture in most agencies. Innovation requires risk and failure, rewarding the attempts instead of punishing the inevitable mistakes along the way. Many agencies have neither an R&D culture nor a willingness to listen to younger, less-experienced staffers. These same young staffers, though, tend to be more tech-savvy than their older colleagues. Gen-Y and Millennials are innovating prolifically, but mostly in private industry.

If a culture does not encourage or embrace innovation, it quickly dies.

If a culture does not encourage or embrace innovation, it quickly dies. Leadership will need to exercise budget and political capital if they wish to transform their agencies into more innovative environments.

Participants believed that there are ways to transform government agencies into innovation incubators. In addition to information sharing and spreading success stories widely, reward and recognitions systems would need to change. Make performance and results the focus for pay policies. There needs to be a celebration of those who develop innovative solutions, and no punishment for those who try in good faith yet fail. The notion that only experienced people are worth hearing also needs to shift. A final suggestion was around portfolio: have one set of innovation activities aimed at maintaining and sustaining operations, and a second set for investment and growth.

Safeguard the computing environment

The discussion on cyber security focused on “secure, resilient, trustworthy information sharing.” In a truly secure internet environment that enables information sharing, the right people are able to access the right level of information, while the government is able to protect data from intrusion by any outside means. IT security experts may follow trends, as done in artificial intelligence, to recognize threats before intruders can gain access to secure information.

In today’s world, functions do not take place in controlled, discreet domains, but are instead interconnected. Hence, cyber security concerns are more and more dominant, and there is a need for clear standards across agencies. When the security standards exist and are well established, people feel comfortable sharing information. There is a generation gap in comfort, though. Gen-Y or Millennials may feel secure in their information-sharing activities while Boomers – who did not grow up with the Internet at their fingertips – can require a different level of security standards. Increasing transparency between agencies and people can become a challenge if people rush to use tools and software without identifying a real need and considering the security implications.

Another key issue is the lack of skilled individuals in the technology field who are needed to create or enforce appropriate security levels; government employees would require training and support. Many agencies find it difficult to recruit young IT professionals to these jobs.

How do we address legacy systems? Would we apply new cyber security standards retroactively? Significant budget will obviously be required to improve all of these systems and processes.

To move forward, some initial actions may be:

- Deliver training awareness program to include national level commitment to cyber education so that people are able to use information-sharing functions.
- Research and Development groups to put budget and incentives into automating security throughout government.

continued on next page ►

- Develop a clear strategy for managing critical vs. non-critical data. This includes defining what information is being protected and creating classification levels for security.
- Hold software and hardware vendors accountable for security standards.
- Complete projects in process.
- Finish Trusted Internet Connection (TIC).
- Smart card deployment.
- Coordinate vulnerabilities at one office to make everyone aware of preventative measures.

Commentary

Across the discussions, several common elements surfaced:

1. Most government agencies work in silos. There is little conversation or cooperation between agencies, which causes a lack of trust and further reduces the desire to share information or systems. This results in duplicate services and systems, instead of streamlined and joint services. There are also opportunities to collaborate with the private sector that some agencies aren't taking.
2. Culture affects who chooses to enter and stay in government agencies, as well as whose voice gets heard. Unfortunately, not enough technology experts, technicians or engineers are currently part of the government workforce. The tech gap in human resources makes it challenging to overcome the tech gap in equipment (and attitude).
3. In an age of information overload, how much is enough but not too much? Transparency and engagement are laudable goals; however, how much information can decision-makers assimilate? How do we ensure accountability and information use in context, when the sheer volume of information is so staggering that it has to be parsed to be understood?

There are additional issues that the participants did not address but that are ripe for consideration. Cyber security is focused on preventing attacks to data systems and unwelcome access to information. It's about balancing who needs to know what and who does not, and gatekeeping effectively. However, the focus seems to be on safeguarding today's data systems and stymieing intrusions. Yet, we also need to focus on what information is being safeguarded for the future, and how it should be archived effectively for reference. Most of us cannot play 8-track tapes or read 5¼ inch floppy disks anymore. We throw out the hundreds of credit card receipts we get, but save the monthly statements. So, critical questions to address are: what information do agencies need to keep, and how do we ensure they can access it later?

Another issue bridges citizen engagement, transparency and security. On the one hand, government operations must be open to citizens. The basis of democracy is participation and representation of citizens' views, needs and mandates. Citizens have a right and an obligation to both be aware of and to help inform their government's actions. Therefore, more access and more information should be better than less. However, what degree of access or engagement should citizens have, and to what end? What media for participation will serve our democracy well, balancing "we the people" with effective government action?

This leads to a corollary set of issues: how much information should be public, how much

information is truly necessary for agencies to collect, and at what point do concerns for privacy (and the Paperwork Reduction Act provisions) compel us to say “don’t collect nor grant access to these kinds of data”? For example, there is discussion now about establishing a medical records database. If government computers house medical records for 300 million people, will they truly be confidential? To start, tens of thousands of health care workers potentially have access. This alone poses a true security challenge. Agencies like the FDA, HHS, and EPA could make a case to “data mine” people’s private records; if so, how private can the records truly be? The answers are only partly based on technology solutions; they also have to mesh with ethical considerations.

Clearly there is need to continue these conversations. The issues are complex, nuanced and evolving, just as our technology is.

APPENDIX: The Five Pillars of Transparent Government

1. Increase government transparency: Provide citizens with information and data about the operations of government to promote citizen engagement, increase accountability across government, and encourage innovation. Potential issue areas include:

External transparency (citizen facing) – Improve the public’s trust in government by enhancing transparency and engagement.

Internal transparency (government-facing) –create a more efficient government by promoting information sharing across government to improve decision-making and reduce waste and inefficiencies. Promote a more integrated government by working across functional and mission silos

American Recovery and Rehabilitation ACT (ARRA) – Use best practices and innovative technologies to provide citizens with accurate, timely and detailed information regarding the investment of economic stimulus funds.

Tie input to outputs - Develop processes and systems that identify the outputs achieved with specific investments, and measure the value of those outputs.

2. Increase citizen engagement: Create a government that is open and encourages greater participation so that decisions may be informed before they are made rather than after.

Access to information – protect and enhance the public’s right to access government information

New technologies – Use cutting-edge technologies to increase citizen inclusion in government while protecting security and privacy and reduce the digital divide.

Policy implications – What are the policy implications on the use of new media to increase citizen engagement? How do we break down the perceived barriers?

Return on investment – How much does it cost to increase citizen engagement?

3. Lower the cost of government operations: Reduce the cost of government while improving its efficiency of operations and delivery of services to the public.

Open source technologies – Reduce the need and cost of building proprietary IT systems for the government through the use of open source and SaaS technologies

Cloud computing – Identify best practices and policies for taking advantage of cloud computing to reduce government expenses.

Improve the procurement process – Identify opportunities to improve the procurement process to increase innovation and reduce the time it takes to procure major systems while enhancing competitive opportunities.

continued on next page ►

Enterprise-wide initiatives – Identify cross-cutting government operations shared by multiple organizations and reduce government expenses through the reduction of duplication.

Electronic health records – Reduce the cost of government and improve national health care through electronic health records.

Green IT – Explore the use of energy efficient technologies to reduce energy costs and promote a cleaner environment.

Renovate an out-of-date government inventory – identify opportunities to reduce costs by replacing obsolete and out-of-date government IT systems.

Improve the budget process - Improve the federal budget process through the application of enterprise architecture principles.

4. Promote and encourage innovation in government: Restore innovation to government IT and improve the delivery of services to the citizen.

Acquisition innovation – Explore acquisition reform and strategies that will promote innovation.

Encourage risk taking within the federal workforce – Identify policies and practices that will encourage risk-taking and greater accountability on the part of the federal workforce

Emerging technologies – Identify emerging technologies with potential application to government activities and recommend ways to permit government agencies to take advantage of those technologies.

Small business – Promote innovation through support for small businesses with leading-edge ideas.

Improve American competitiveness - Manage government IT as a national strategic asset that contributes to America's ability to compete in the global marketplace.

Modernize the financial regulatory system – Develop an up-to-date and integrated IT system to support a financial regulatory system based on complex financial transactions and public transparency.

5. Safeguard the computing environment: Create a safe environment for government IT assets that protects the national interest and privacy while promoting the appropriate exchange of data.

Personally identifiable information (PII) – Developing methodologies for protecting PII is critical in this age of identity theft.

Data and infrastructure protection – Data systems and infrastructure must be secured in order to maintain the day-to-day operations of government.

Identity management – Continue the development of standards of identification to protect electronic and physical assets.

Promote public-private partnerships – Establish a collaborative partnership with the private sector that provides the networks and systems used by government.