MEMOS TO NATIONAL LEADERS

SUBJECT: MR. PRESIDENT/MR. SPEAKER: HERE IS YOUR IT AND TRANSPARENCY AGENDA

FROM: ALAN BALUTIS, GARY D. BASS, DANIEL CHENOK, FRANK REEDER, and ALAN SHARK.

In the aftermath of September 11, 2001, we heard again and again that our government needed to be better managed. "Everything has changed" was the constant refrain—11 years ago. Fortunately, now there is a unique convergence between current challenges, the need for government leaders to act in a fundamentally different way, a generational shift in executive ranks, and powerful new collaborative technologies. Here are some of the changes that await our next commander in chief and the leaders of the incoming Congress:

Human Resources: The Chinese write the word "crisis" with two characters, one of which means "danger" and the other "opportunity." The pending workforce crisis (or as some refer to it, "the retirement tsunami") also can be viewed as a tremendous opportunity to reshape the federal government, flatten hierarchies, remake the way government and citizens interact, and change the culture of the bureaucracy.

Changing Workplace: Consider how the world has changed in the last thirty years. Then people came to work at a central office, the major role of the U.S. General Services Administration (GSA) was to manage or build the multitude of federal buildings and offices to house all those workers, and telework was largely unknown. Contrast that with today and what the Gartner Group terms "Future Worker 2015." Personal computers and cell phones are ubiquitous, telework is routine, and business partners are as likely to be on different continents as in different cities.

Changing Workforce: The Federal Chief Information Officers Council (CIOC) recently completed a study entitled "Net Generation: Preparing for Change in the Federal Technology Workforce." Discussing this new generation of federal employees, the report said:

"As a generation, they are over 80 million strong, larger in fact than the Baby Boomer generation. They cannot be ignored as the major source of talent to recruit, develop and retain over the next decades. Additionally, there is much to admire about this generation. They are ambitious and innovative, enjoy teamwork, and understand technology."

Changing Technology: One can argue that Web 2.0 technologies have ushered in a new era of rapidly expanding content and information sharing capabilities. And, over time, they will dramatically change the way organizations work internally and how they interact with their external citizen and customer base. A number of departments and agencies are increasing their use of Web 2.0 social media technologies for both internal and external applications. Collaborative tools can now be considered mainstream.

The federal government will be undergoing tremendous change on many levels over the next several years. Any one of the changes listed above would be a major driver for government, but their convergence creates a

perfect management storm for our nation today and an opportunity for the next President, partnering with the new Congress, to dramatically reshape the bureaucracy by leveraging IT to forge a 21st century government. To do so, we have made the following recommendations:

- Issue a Statement of Principles and an Action Plan for implementing An Enhanced Digital Government Agenda;
- Foster a Dynamic Citizen Engagement program;
- Reorganize the Office of the Chief Information Officer;
- Improve IT Project Management;
- Rebuild trust in government through greater transparency; and
- Improve information security while ensuring personal privacy.

Memo #1: An Enhanced Digital Government Agenda

The "Great Ideas Hunt," an initiative the General Services Administration launched in May to help develop cost saving ideas, as well as the annual White House call for employee ideas to incorporate in the President' budget submission, characterize innovation as "rounding up the usual suspects"—reviewing and cancelling newspaper and magazine subscriptions, printing on both sides, putting government publications online, getting rid of paper checks, and so on. A plan to go agency by agency, publication by publication, subscription by subscription, across the vast array of government and its more than two million employees will not transform the way the government does business. We need a statement of principles and an action plan for implementing digital government. The following steps are a start (but only a start)for how the government can move beyond the Digital Strategy released earlier this year:

- The primary manner in which client services could be improved is through single points of access to multiple sources of service, a coherent whole-of-enterprise vision of client services, electronic delivery of services and public kiosks, and one-stop shops and agency-to-agency cooperation;
- All services that can be provided digitally should be. However, agencies should prepare a universal service plan to indicate how federal services will remain available to those who cannot communicate digitally. Technology can provide some solutions (wireless devices, cable television, over the phone, and so on);
- The availability of funding—and flexibility in the ability to reprogram funds—is critical if we are to achieve digital government. Increase funding for such initiatives and allow greater reprogramming authority to support new projects;
- Use electronic funds transfer in all monetary transactions;
- Use electronic checks;
- Issue government benefits through electronic benefits transfer;
- Expand federal smart card applications; ensure they are interoperable with private sector applications;
- Focus on intergovernmental (as opposed to federal only) solutions; and
- Support the equal access requirements of Section 508, the Rehabilitation Act Amendments of 1998, which require access to electronic and information technology provided by the federal government.

There is no reason the government cannot operate with as much speed, responsiveness and resiliency as the private sector. In fact, there is no reason government should not be the leader when it comes to technology adoption and service delivery. Of course, a digital strategy and agenda is about more than IT and electronic transactions. It is also a plan to rethink and reform the way the government does business. Once agencies have implemented these recommendations, they should move on to the next step – seriously rethinking and reorganizing their filed office, delivery systems, human resources strategies and plans, budget requirements, and so on. Once information and online transactions become central to government service delivery and business processes, serious reorganization and restructuring must be a mandate.

Memo #2: Citizen Engagement

The President and Congress should continue and build upon previous efforts in creating new and innovative ways to use technology to further citizen engagement efforts. While transparency may be a tool to help citizen engagement, it alone does not create the multi-dimensional communications channel needed for engagement. Similarly e-government – using the Internet to improve management and service delivery – does not amount to citizen engagement. Given the explosive growth of mobile devices as well as Internet penetration, there is enormous potential to transform the relationship of governments to the public.

The following represent just some steps and initiatives to foster a realistic and dynamic citizen engagement program.

1. **Create a new Federal Office for Citizen Engagement.** There needs to be a central coordination body that works to coordinate citizen engagement initiatives among agencies and commissions. The Office would also work with public interest groups to better promote the need for improved citizen involvement.
2. **Continue Presidential Directives on Trusted identities**. For citizen engagement to truly work, government and citizens alike must know that postings are from the people who they say they are. Certifying forms of trusted Identities is critical to citizen engagement initiatives.
3. **Develop Clear Guidelines for Agency Online Participation Activities.** Agencies should be asked to document the number and type of online consultation they already conduct.
4. **Continue Experimenting and Fine Tuning Challenge.Gov** Challenge.com was created to seek comments and ideas from the public on various issues. The results to date appear mixed. The site should be re-vamped and made more user-friendly with interactive issues, and buckets where citizens can weigh in and offer advice.
5. **Utilize GIS Postings.** The use of GIS mapping and sharing would be a positive addition to engage citizens. With over 40% of our citizens using "smart phones and mobile devices" picture posting and information posting is an excellent tool to encourage citizen engagement, as was nicely demonstrated by recovery.gov.
6. **Experiment with Ad-Hoc Communities.** Citizen engagement initiatives should be structured so they can be meaningfully unstructured. In other words the Federal government should establish a "Rapid Ad Hoc Response System" where mechanisms can be created almost instantly in times of crisis and also in times when a certain issue surfaces that could benefit from citizen engagement techniques.
7. **Promote Collective Intelligence.** Similar to Ad-hoc Communities, Collective Intelligence is a concept that identifies experts or opinion leaders in a particular field or area of expertise and can be called upon to help solve specific challenges and problems.
8. **Utilize Wikis.** Wikis can be useful mechanism for building knowledge, sharing ideas, and engaging informed citizens;
9. **Ensure that Agency Staff have Adequate Skills to Support On-line Participation. Promote Crowdsourcing.** Leaders can gain valuable input to the development of policies and priorities by seeking broad input. This can also increase citizen understanding and support for government action.

Memo #3: Reorganizing the Office of the CIO

The issue is not really or solely the role of the CIO, but more the lack of continuous management improvement across government; that management gap generally involves IT because our government is information intensive. There is a constant need to align budgets, technology, people, and acquisitions to achieve program goals, thus a holistic management approach. And continuity in senior management leadership is essential to ensure the agency mission is executed successfully with measurable improvement to both mission and operational performance. That includes introducing new business processes, modern financial and business systems, and other technology enabled advances.

We recommend that this be done by creating a Chief Management Officer (CMO) within all major departments and agencies, to serve a fixed year term akin to that of the Controller-General, the head of the Government Accountability Office. All management and administrative positions should report to the CMO—finance, budget, IT, acquisitions, human resources, information security, the chief performance officer, the assistant secretary for administration, and so on—and all these positions should be filled from career SES ranks. Let's focus here on the role of the Chief Information Officer (CIO). Each CIO will report directly to the CMO and will assume five functions:

1. Strategic use of information and technology, with primary responsibility for identifying leading practices that utilize IT to improve mission performance;
2. Management and maintenance of the IT and information infrastructure;
3. Identification, deployment, management, measurement, and (if applicable) scaling new technologies, applications, and data;
4. Management of the Agency Transformation Fund, a proportion of the agency IT budget which is set aside for new starts; and
5. Information security.

Both the Chief Technology Officer and the Chief Information Security Officer should report to the CIO.

Memo #4: Improving IT Project Management

Major business transformations in the federal government are often treated merely as an IT initiative, as opposed to the complex organizational change management challenge they actually are. But the reality is that large IT projects invariably involve significant changes to business processes but oftentimes lack organizational resolve, dedicated political-level sponsorship, or adequate project oversight. Here are some ideas within governance, planning, and procurement that will integrate the whole organization into each project:

Governance

- The Deputy Secretary's group (hereafter referred to as the PMC or President's Management Council) should determine the government's capacity for large IT-driven business transformations and govern the number and size of concurrent projects both within an agency and across government accordingly.
- The sponsoring organization should commit and hold accountable senior executive leaders for the duration of the project.
- Project leadership should shorten project approval cycle times for incremental and low-risk projects.
- The Office of the Chief Information Officer should continue to strengthen overall project reporting processes to provide the PMC with an effective means to assess the progress, timeframe, and risk profile of ongoing projects quickly.
- The PMC and the CIO should ensure project post-mortems are a regular part of project oversight.
- The PMC should establish an Independent Advisory Committee (IAC) for IT to provide expert and independent advice on the issue of large IT transformations.

Planning

- The PMC should take a Portfolio Management approach to major IT investment and management.
- Project sponsors should invest a greater percentage of the project budget than they now do in up-front planning to ensure more robust business and project plans.
- The PMC and the CIO Council should establish and formalize a gateway review process for project approvals and funding.
- The Gateway Project Review Process is a series of short, focused, independent peer reviews at key stages of a program or project. The reviews are undertaken in partnership with a project team and all stakeholders. They are designed to highlight risks that, if not addressed, would threaten the successful delivery of the project, though the reviews are not audits. Passing through a gateway means that the project is ready to progress to the next stage of development or implementation.

Procurement

- Project sponsors and leads should prepare more thoroughly for procurement and begin projects only when a clear business case has been developed.
- Procurements should incentivize the achievement of strategic goals as the first selection and review criterion, rather than focusing on procedural goals or accomplishments.

Contracts should contain "off-ramps" (that give the government the option of terminating the relationship with an underperforming or unsuitable vendor and replacing the vendor with a new one, or stopping the project).

Memo #5: Transparency

In a period when trust in government is at an all-time low, transparency may be a tool to rebuild that trust. Government transparency may be defined as the public's right to know about actions of its government and power elites as well as access to tools that foster greater participation in democratic actions. Transparency is one element – albeit an essential one – of an open government.

Despite the clear importance of transparency in building a more effective and accountable government, the federal government continues to fall short of the openness we need. While progress has been made, we continue to struggle with the responsibilities of our often longstanding right to know laws, such as the Freedom of Information Act (FOIA). Today's laws and policies on public access are inadequate for today's 24 hour-7 day a week Internet world. Under the Freedom of Information Act, the bedrock law on openness, the burden is on the public to request information (and wait for a response); there are far too many loopholes to allow agencies to withhold information; and the law is designed for the paper world functioning in an electronic era. These policies need radical overhaul.

The President and new Congress can put in place a new open government policy that creates an affirmative obligation for government agencies to proactively disclose information. While some government information must remain secret, the burden to justify withholding information should be a government responsibility, should be set at a high standard, and should be fully disclosed and explained in terms all can understand. Any time the government proceeds to collect information, it should presume that the information will be disclosed in a timely and searchable manner.

To begin this affirmative disclosure model, the next President should immediately issue a new directive to agency heads establishing standards for information that all federal agencies must disclose. This standard would be a floor that agencies would be encouraged to go beyond. At a minimum it should include:

- General information about the agency that helps the public better understand how to contact key agency personnel and types of activities top level employees are engaged in, such as organizational charts, list of employees and how to contact them, logs of visitors meeting with top level officials, and calendars of top level officials;
- Policies guiding agency actions that will help the public better understand how decision-making and operations occur within an agency;
- Unclassified communications and reports prepared by an agency, such as communications to Congress and reports of an agency Inspector General; and
- Other records and data that will help the public hold government agencies accountable, such as logs of requests for records filed under the Freedom of Information Act and information about who is participating in federal advisory committees and what is being done by such committees.

There are other top level policy reforms needed including strengthening disclosure of information about: special interest influences and ethics of those working in government; administrative governance, including rulemakings and paperwork requirements; and federal spending, including tax expenditures. The President also needs to make sure that information withheld from public disclosure warrants secrecy. This includes ensuring the classification process is sharply reduced in scale, duration, and complexity.

Here are four principles that government should follow in using new information technologies to make data available to the public:

- **Make sure the information can be found and is timely and accurate.** If information cannot be found when the public is looking for it, then the agency is not truly being transparent.
- **Data standards are essential.** The development and use of standards for metadata will also be critical to facilitating the retrieval of the right information, especially as release of government data sets increases.
- **Make sure commercial services can be used.** Agencies and government employee should take advantage of the same open, free, commercial services the public uses to communicate and share information, such as Facebook, YouTube, and Twitter.
- **Data must be structured so it can be mashed-up.** With the disclosure of more and more government databases, the demand to link various data increases. Government has responsibility to enable such use of databases by developing a system of common identifiers for companies, locations, industries, activities, etc. to be used across agencies.

At present, disincentives are built into the way government agencies operate. Civil servants need to be given the freedom to disclose information and be rewarded for doing so.

Agency staff, beyond those responsible for implementing FOIA, should also be required to go to periodic trainings on transparency issues so that they are familiar with the public's right to know, as well as the tools they can use to carry out transparency efforts. The mandatory trainings could also result in a certification that signifies a level of understanding in how to disseminate government information.

Memo #6: Privacy and Security

The introduction of information and communications technologies has raised challenges as to how we can protect privacy and security while exploiting the benefits that innovation offers. The Internet has created the global village that was, until recently, merely a figure of speech. But, as recent revelations about misuse of personal data suggest, social networking and other innovative technologies create potential hazards for those who use them. And our growing dependence on these technologies for everything from routine financial transactions to the operation of the power grid potentially makes us more vulnerable to failures in that technology.

While some of the reforms in existing policy may require legislation, much can be done with existing legal authorities to mitigate the risk we assume in using information technology while also reducing the potential unwarranted intrusions upon personal privacy. Some specific, actionable recommendations follow for both security and privacy:

With respect to security:

1. Under the current policy regime, lengthy checklists and outdated guidance cause agencies to waste scarce resources on measures that do little to mitigate risk. There is hard evidence that continuous monitoring, measurement, and mitigation against a defined set of high risks are far more effective in addressing real threats in an environment in which those who seek to do us harm move quickly. Changing Federal Information Security Management Act (FISMA) implementation from a compliance approach that focuses on process rather than outcomes to one of continuous monitoring is the single most important action that leaders can take. We recommend that OMB use the authority provided under the existing statute to encourage this important reform.

   Moreover, the debate on whether and how the government should impose cybersecurity standards on the private sector asks the wrong questions. By modeling best practices, the government can lead by example and develop de facto standards of due diligence that will render these questions moot.

2. The national security and intelligence communities have cybersecurity competencies that are critical to protecting civil systems such as banking and utilities. Those capabilities can and should be used without comprising civil values. We thus recommend revisiting authority structures to reflect the reality of a changing world; namely (1) the critical role in information security for the Department of Homeland Security, which did not exist at the time the underlying statutes and current OMB policies were last revised, and (2) the need to redefine the roles and relationship between national security and non-national security systems, to encourage sharing of cyber information across agencies.

   With respect to information privacy, a "Code of Fair Information Practices" first articulated in 1973[1], underpins most privacy laws, including the Privacy Act of 1974. We need a new set of principles for leaders to follow that govern cases where security and privacy conflict in cyberspace, Such principles

[1] *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health Education and Welfare, July 1973 [available at http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm]

may include:

- Risk analysis that informs the level of protection, detection, and mitigation– high risk/threat gets more oversight
- Notice to individuals if their machines are causing a problem
- Court review for access to electronic records
- Proper review where cyber protection requires individual surveillance consistent with law
- Examine content of messages only in cases of imminent threat
- Privacy-by-design and Privacy-enhancing security technologies should be favored in system development
- Officials with a privacy interest (e.g., agency CPOs) should be in the room during consideration of actions needed for cyber protection, not after the fact
- Correct for false positives – destroy information that should not have been tracked via mitigation
- Audits should be done to ensure accountability.