Interested in learning more about security?

SANS Institute InfoSec Reading Room

Federal Information Technology Management and Security

The Federal Information Technology (IT) budget has grown to nearly $60 billion. The President introduced "Expanding Electronic Government" as part of his management agenda1 to "improve the management and performance of the federal government." 2 The challenge for the President's Office of Management and Budget (OMB) is how to re-engineer Federal electronic business processes while reducing the Federal IT budget. These two objectives appear to be diametrically opposed. However, OMB contends it can: 1) reduce annual IT s...

Federal Information Technology Management…and Security

by John L. Hopkins
July 15, 2003
Version 1.4b (August 2002)
Option 1

TABLE OF CONTENTS

Executive Summary

The Federal Information Technology (IT) budget has grown to nearly $60 billion. The President introduced *"Expanding Electronic Government"* as part of his management agenda[1] to "*improve the management and performance of the federal government."*[2] The challenge for the President's Office of Management and Budget (OMB) is how to re-engineer Federal electronic business processes while reducing the Federal IT budget.

These two objectives appear to be diametrically opposed. However, OMB contends it can: 1) reduce annual IT spending; 2) ensure collaboration in e-Government interoperability; and 3) improve security.

This paper examines the long-standing vision of one senior OMB manager to re-enforce a seven year-old plan he helped draft that uses the Federal IT budget planning process to accomplish these three principal objectives. It also reviews his contention that improving IT Security requires better management, not increased funding.

Reducing Annual IT Spending

Mark A. Forman started public life as a presidential intern after completing a Master's Degree in Macro Economics from the University of Chicago. For the next seven years he specialized in IT issues as a staff member of the Senate Governmental Affairs Committee. The committee drafted the Information Technology Management Reform Act of 1996, which came to be known as the Clinger-Cohen Act. The Clinger-Cohen Act:

- established **Chief Information Officer** (CIO) positions in every department and agency in the federal government;
- established the **CIO Council** of 28 major federal agencies, two small agencies, and OMB;
- defined **Information Technology Architecture** (ITA) as an integrated framework for evolving and acquiring information technology to achieve the agency's strategic goals and information resources management goals, which is now known as **Enterprise Architecture** (EA); and
- implemented formal **Capital Planning Investment Control (CPIC)** (IT budget planning) process requiring cost, schedule, and performance goal reviews of IT projects (Figure 1)[3]. OMB grades projects and funds accordingly, with an "at-risk" category. The risk involved is not receiving funding for the project.

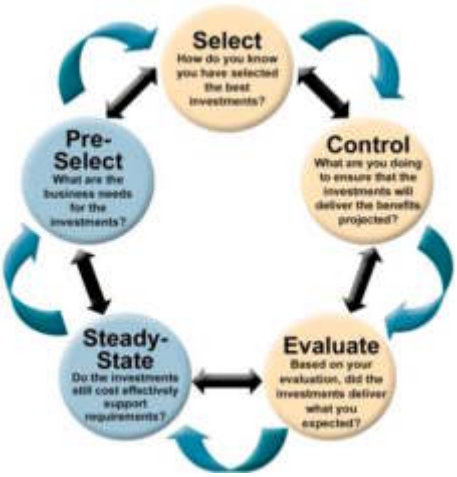


Figure 1

Forman moved to the private sector and worked as vice president of e-Business and federal systems at Unisys Corporation. In June 2001 President Bush appointed him as Associate Director for Federal Information Technology and e-Government at the Office of Management and Budget and Forman immediately moved to improve federal IT efficiency. He formed a Quicksilver Task Force of Federal department and agency IT professionals to identify e-Government Initiatives (Figure 2)[4].

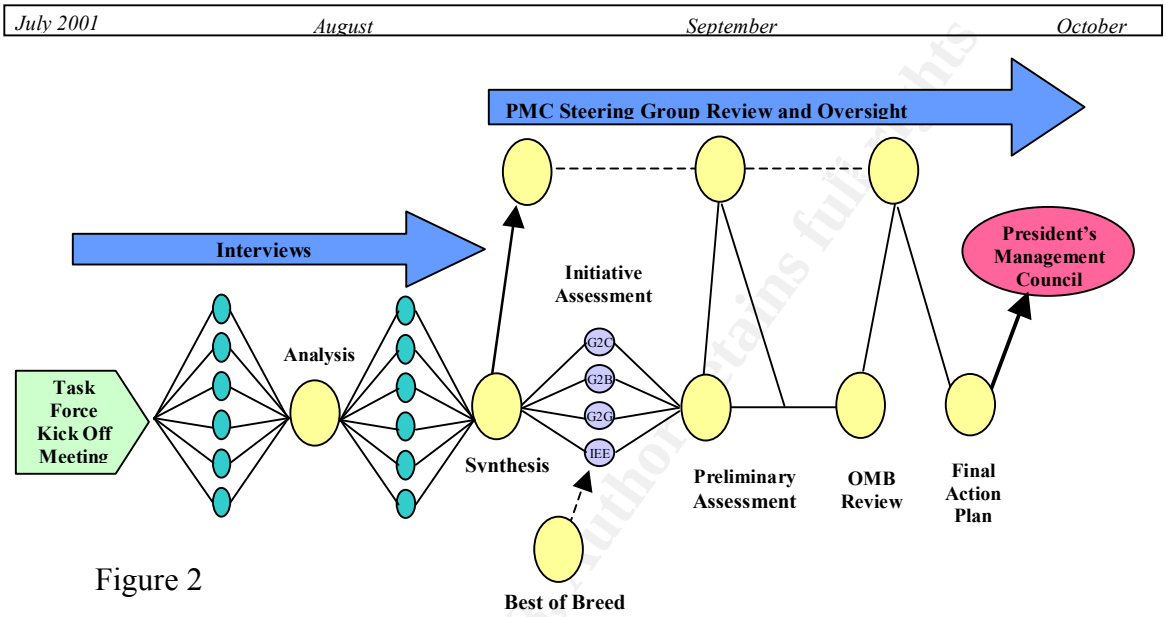


Figure 2

The challenge of finding a common method for the Quicksilver Task Force to unify and simplify the Federal IT landscape was imbedded in legislation Forman helped craft in 1996. Under Clinger-Cohen, every department and agency Chief Information Officer (CIO) was responsible for *"… developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency."*[5]

Fiscal Year 2003 (FY03) IT budget submissions to OMB had to map to the Information Technology Architecture per OMB Memo 97-02, "*Investments in major information systems proposed for funding in the President's budget should be consistent with Federal, agency, and bureau information architectures which integrate* ***agency work processes and information flows*** *with technology to achieve the agency's strategic goals and specify standards that enable information exchange and resource sharing."*[6]

The CIO Council started work on the Federal Enterprise Architecture Framework (FEAF) in April 1998 to promote shared development for common Federal processes, interoperability, and sharing of information among the Agencies of the Federal Government and other Governmental entities.[7] The collection of individual architectures was intended to represent the entire federal architecture…an architecture of architectures.

The flexibility built into the FEAF allowed agencies and departments to identify and create their own work processes or lines of business. Allowing each agency to identify their work processes (lines of business) independently was the failure in the FEAF. The result was a multitude of business lines.

The Quicksilver Task Force met from June to September 2001 to identify redundancies in agency work processes, the day-to-day business operations of the Federal government.[8] They identified 487 business lines operating in agencies, prompting Forman to call it *"…the business architecture that isn't."*[9]

Without a common reference, the resulting list of business lines was so large and diverse that attempting to identify redundancies was difficult. However, even with 487 different lines of business, the task force found some lines of business being done at an average of 19 agencies. During later testimony before the House Subcommittee on Technology and Procurement Policy, Forman said the 24 quicksilver initiatives generated cost savings and improved effectiveness by *"…unifying agency work processes and information flows."*[10]

The Quicksilver Task Force was able to identify 24 Initiatives based on redundancies in the FY03 submissions. These consolidation opportunities equated to budget reductions and laid the groundwork for horizontal integration of systems across the federal enterprise.

Forman decided a Federal Enterprise Architecture was needed to help simplify and unify lines of business. In February 2002, just five months after the task force report, the CIO Council delivered a Business Reference Model (BRM) with 39 lines of business and 153 sub-functions and mapped each agency or bureau to the BRM, telling each what its lines of business were perceived to be. The Federal Enterprise Architecture Program Management Office (FEAPMO) was established to define the federal architecture.

Forman's vision was beginning to result in real change in the federal government. "We're creating new workflows, meaning: How do you manage the flow of information and how do you actually work across agencies or between federal, state, and local (government)?" His answer to the question was structure. "In the past, we've done that on an ad hoc basis. There didn't need to be anything formalized."[11] However, that was about to change.

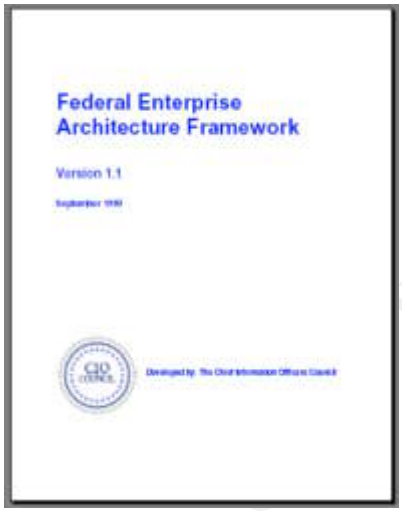
Under Forman's guidance, OMB directed agencies to use the BRM and agency mapping tools from the FEAPMO in their FY04 IT budget submissions, thus creating the needed common reference. They were to identify lines of business associated with IT budget line items.

OMB now reviews all IT budget submissions for business case redundancy. Investment decisions are made based on opportunities to finance a line of business once, not several times. Combining agency efforts unifies and simplifies the architecture and thereby reduces the Federal IT budget.

Collaboration in e-Government Interoperability

The events of 9/11 meant, "…that we have to operate as a team, and that takes some different infrastructure; it takes some process re-engineering and process integration," Forman pointed out in a June 2002 interview with CNETnews.com.[12]

Following the terrorist attacks, Senators, Congressmen, journalists and citizens scrutinized failures by the government to share information and collaborate on solutions. Had they looked at the FEAF that was released in 1999, they might have seen language that pointed to one symptom, under the heading ***Inability to Share Information***, which read, **"**Without standards and guidelines, Federal organizations will continue to experience **difficulties in sharing business information through technology mediums**, such as word processing documents, e-mails, databases, and other applications, which in turn, require redundancy and add costs. The knowledge infrastructure is not in place to allow knowledge management. Public expectations for a simple interface to the Federal Government will be elusive."[13]



While the FEAF had described the preparation of an enterprise architecture (EA) in 1999, GAO reported in February 2002 that 98 of 116 agencies surveyed had the minimum criteria developed by GAO for creating EA awareness or building an EA management foundation.[14] Only five agencies satisfied GAO practices to effectively manage EA activities.

Forman pushed for production of a Federal Enterprise Architecture (FEA) after joining OMB in June 2001. In 1996, Clinger-Cohen required every agency to have an IT architecture. However, the FEAF produced by the CIO council in 1999 did not result in an FEA that provided components or models. It resulted in 487 different lines of business in FY03 IT budget submissions (submitted to OMB in February 2001), making it difficult to identify collaboration opportunities and therefore creating "***difficulties in sharing business information through technology mediums."***

The first component model of the new FEA, the Business Reference Model (BRM), was released in February 2002, the same month the GAO report

on Enterprise Architecture was released. Version 2 of the BRM was released in June 2003.

An OMB press release announced the Federal Enterprise Architecture in July 2002. "The Federal Enterprise Architecture, as the name suggests, provides a foundation for the effective implementation of the President's agenda," said Mark Forman."[15]

The collaboration zones and enterprise connectivity necessary for homeland security are based on a working FEA, thus requiring replacement of the unworkable FEAF that had not produced a Federal structure. "The lines of business and sub-functions that comprise the BRM represent a departure from previous models of the Federal government that use antiquated, stove-piped, agency-oriented frameworks," Forman pointed out in House testimony.[16]

The Federal budget process has historically financed those stove-piped systems. These islands of automation benefit business process owners but offer little to citizens, businesses, and other government entities outside the agency. "Agencies generally buy systems that address internal needs, and rarely are the systems able to interoperate or communicate with those in other agencies. Consequently, agencies cannot easily share information," said Forman.[17]

The key to interoperability is forcing the IT budget process to finance systems that link to the agency EA and contribute to the FEA. OMB guidance in Circular A-130 on the Capital Planning Investment Control (CPIC) process says it must "…build from the agency's current Enterprise Architecture (EA) and its transition from current architecture to target architecture."[18]

Enterprise Architecture

What exactly is Enterprise Architecture? When technologists begin describing Enterprise Architecture (EA) most normal people suffer a serious case of *MEGOS* ("my eyes glaze over" syndrome). Here is a simple way to view it.

The first push for a coast-to-coast highway started in 1800 and resulted in an Act passed by Congress and signed by President Thomas Jefferson in 1806. However, construction did not start until 1815. The first section was built of crushed stone, opened in 1818, and ran from Cumberland to Wheeling, West Virginia. That was the only road that went horizontally across this great country.[19]

Following the end of World War I, General John Pershing returned from Europe with stories of how he could transit an entire country horizontally by road. He directed a young Lieutenant Colonel in 1919 to take 81 vehicles and drive from Washington, D.C. to the Presidio in San Francisco. They averaged 3.5 mph and it took 61 days. The report confirmed Pershing's suspicions of sad conditions.[20]

By 1922, Pershing had developed a plan for an 8,000-mile interstate system. It was not well received at the White House or on the Hill because incumbents said that the railroads were all that was needed. Three more Federal Aid Highway Acts were introduced with little or no success.[21]

Finally, in 1956, Tennessee Senator Al Gore, Sr. submitted a Federal Aid Highway Act that passed Congress[22] and was signed into law by the same Lieutenant Colonel who made the cross country trek back in 1919 - President Dwight D. Eisenhower.

The act provided $25 billion (90% federal) to develop a capability for transiting from one state to another on a common roadway 41,012 miles long with nationwide design standards: 10 foot shoulders; 12 foot lanes; two lanes in each direction; and 50-70 mph capacity.

How does this relate to Enterprise Architecture (EA)? Answer: Its simplicity. EA's are comprised of three parts:

1) As-Is Architecture
2) To-Be Architecture
3) Transition Plan or Modernization Blueprint

Pershing took an inventory of the roadways' conditions and established an "As-Is" roadway architecture. Federal agencies take an inventory of existing or legacy applications or systems, business processes, data elements, and technologies to prepare an "As-Is" EA.

Next, as in Pershing's experiences in Europe, agencies prepare a vision (strategic plan) of what is possible, or a "To-Be" EA. Agencies are required to prepare and submit strategic plans that describe a future vision. The applications or systems, business processes, data elements, and technologies required to carry out that strategic vision represent the "To-Be" EA.

Finally, the Federal Aid Highway Act represented the plan to transition from the old roads to the new vision of a coast-to-coast freeway. The transition plan in an EA is the modernization blueprint for transitioning from "As-Is" to the "To-Be" architecture.

Highway plan specifications ensured that each state built roads the same, or similar enough so there could be interoperability across state lines. In the Enterprise Architecture, models released by the FEAPMO represent specifications that help ensure continuity and interoperability in the Federal IT enterprise. This architecture allows one system to transit the enterprise from border to border across each agency and in some cases across the entire Federal government.

A common highway architecture with standardized specifications, allows an automobile to go seamlessly and efficiently from state to state. With a common Federal IT enterprise architecture, data can be seamlessly and efficiently accessed across agency and department boundaries without having to change systems. This enables horizontal interoperability.

Getting states to support the U.S. Highway system was a problem because they often balked at the construction costs. When the national superhighway system began being viewed as a critical part of national defense, the federal government paid for 90% of the construction costs and states supported the Interstates. Similarly, the events of 9/11 have changed agency views of the importance of an FEA to support information sharing across Federal Agencies.

The Federal Enterprise Architecture will help define the requirements, capabilities, computing and communications platforms, and supporting products and standards necessary to share information across Federal agencies, and with State and local government organizations. Federal IT budget submissions to OMB

- must identify the *line of business* it supports from the BRM. This immediately identifies redundancy in the agency and across the federal enterprise.
- must demonstrate a clear linkage to the enterprise architecture and contribute to the agency modernization blueprint or *transition plan* to the TO-BE architecture.
- will not be considered for funding by OMB if initiatives do not demonstrate linkages with the EA.

Agency CIOs have been looking for methods to force operating units within agencies and departments to make IT investments that are compatible with their organizations. To that end, Forman has introduced new requirements for the FY 06 budget requests. OMB will require a single large business case from each agency justifying investments in networks and computers agency-wide in addition to individual business cases for software investments.

"This move will really empower [chief information officers]," said Forman.[23]

Improving Security

Federal IT security spending continues to rise year after year. IT security spending was $2.7 billion in FY02 and indications are that IT security costs will continue to increase. "Federal spending on IT security products and services will continue to rise annually by 7% through 2008…the federal security spending will increase from $4.2 billion this fiscal year (FY03) to nearly $6 billion within five years."[24]

The Computer Security Act, Public Law 100-235 (H.R. 145), was signed into law on January 8, 1988. However, after 15 years, the security of data on

Federal systems is still being questioned. GAO reviews of computer security (four reviews in two years) indicate continuing risks to federal operations.

- Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. GAO-03-303T November 19, 2002
- Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO-02-231T November 9, 2001
- Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk. GAO-01-600T April 5, 2001
- Computer Security: Critical Federal Operations and Assets Remain at Risk. T-AIMD-00-314 September 11, 2000

GAO reviews are summaries of Government Information Security Reform Act (GISRA) reports submitted annually to OMB. GISRA requires risk assessments of systems to identify weaknesses and Plans of Action and Milestones (POA&M) to remedy them. The prologue in the most recent GAO review summarizes, "Implementation of the Government Information Security Reform provisions ("GISRA") is proving to be a significant step in improving federal agencies' information security programs. It has also prompted the administration to take important actions to address information security, such as integrating security into the President's Management Agenda Scorecard."[25]

A common theme emerges during discussions about IT security. As former OMB Director Mitch Daniels was fond of pointing out, his organization was the Office of *Management* and *Budget*, not just an office of the budget. He wanted *management* on the agenda and that *management* included IT security. Forman was happy to carry that torch and offered "help" to agencies through the IT budget process. "Agencies find themselves faced with the same security weaknesses year after year," he said. "They lack system level security plans and certifications. Through the budget process, OMB will assist agencies in prioritizing and reallocating funds to address these problems."[26]

Management, not Money

Dr. Peter Tippett, Chief Technology Officer at TruSecure, is emphatic about putting risk in perspective before spending. He notes that although the number of viruses that could cause damage has doubled every year for the last seven to eight years, the dollar value of damage from viruses has risen only 30-35 per cent per year. In other words, each attack is getting easier or cheaper to deal with although the frequency of attacks continues to increase. Carnegie Mellon's Computer Emergency Response Team (CERT) data indicates that less than 2 per cent of all cumulative computer-related vulnerabilities discovered between 1995 and last year actually resulted in real attacks.

The trouble with computer security, says Tippett, is the focus on vulnerability instead of *risk*. “We should ask, 'How do people actually die in car accidents?' and not, 'What are all the ways people could possibly die in a car?' I could be hit by a meteor while driving. That's a possibility but not a risk!”[27]

An IT toolbox survey of 430 IT decision-makers around the globe conducted in May 2003 found that security ranked second of 16 budget line items implemented in the previous six months.[28] However, in the June 16th edition of eWeek magazine, Jerry Brady, chief technology officer at Managed Security Services Company Guardent Inc., in Atlanta said, “We’re seeing shifts away from technology people to risk management individuals.

“We’ve seen a renewed focus on regulatory needs or standard ways to address their problems,” said Brady. “Security assessment is looking at what your risks are and then mapping out action plans to bring out better or managed security procedures.”[29]

“Everything in the enterprise is scarce in resources and abundant in demands. The challenge is to achieve balance between sensible investment in security and not lose productive business ground in the process,” says Frank J. Bernhard, technology economist and managing principal with Omni Consulting Group in Davis, California.[30]

Forman and the GAO agreed that the single most important solution to system security was management, not increased funding. “The bottom line is that we spent a lot more money to fix these problems, but money is not the panacea. In fact, we found that the problems or the quality of an agency or department’s security plan was not correlated with the amount of money that they spend. There are many management issues here as well.”[31]

Forman’s testimony on November 9, 2001 before the House Committee on Government Reform forcefully indicated that the focus had to be on management of security by program officials (interpreted to mean program project managers). The 2000 Government Information Security Reform Act (GISRA or Security Act) “…divides security programs into three basic components – management, implementation, and evaluation.”[32] This testimony was less than one month after the 9/11 events. Forman continued to explain,

- **“For management**, it recognizes that while security has a technical component, it is at its core, an essential management function.

- **For implementation**, it recognizes that program officials (not security officers or CIOs) are ultimately responsible for ensuring that security is integrated and funded within their programs and tied to the program goals.

  Thus the Security Act highlights the reality that when security funding and implementation are separated from the operational program,

program officials and users begin to ignore it. Separation sends the incorrect signal that it is not a program responsibility

CIOs have a significant role. They must take an agency-wide strategic view of implementation and ensure that the security of each program is appropriately consistent and integrated into the agency's overall program and enterprise architecture.

- **For evaluation**, the Security Act requires program officials and CIOs to annually look at what they have done and what remains to be done and for Inspector Generals to verify it."

Therefore, better security management and not more money is the answer. GISRA required reports to OMB that measure agencies' progress each year in assigning each major system a level of risk, reviewing and collecting IT system weaknesses, developing a plan of actions to correct those weaknesses, drafting contingency plans for systems that become disabled, and updating IT security plans. GISRA expired in 2002, prompting Congress to pass the 2002 Federal Information Security Management Act (FISMA), which makes GISRA mandates permanent. FISMA has been rolled into the e-Gov Act of 2002.

Robert Dacey, the GAO's Director of Information Security said, "The most prevalent [weakness] relates to security program management… Agencies should have in place programs to manage their information security across the organization."[33]

Forman uses the budget and the PMA scorecard as useful motivators for management of systems security. "To ensure successful remediation of security weaknesses throughout an agency, every agency must maintain a central process through the CIO's office to monitor agency compliance," Forman said. "OMB has and will continue to reinforce this policy through the budget process and the President's Management Agenda Scorecard."[34]

In addition, Forman and OMB continue to make the case that the Enterprise Architectures are critical to security solutions. "Agencies have to make sure [security] is in their enterprise architectures, in their business cases, and in their system administration, operations and support practices."[35]

Emphasis on EA and IT security alignment began with the passage of Clinger-Cohen seven years ago. Forman has remained committed to this theme and has used the budget to coerce cooperation and compliance.

After Clinger-Cohen

Senator Joe Lieberman (D-Con) has watched and reviewed the Clinger-Cohen Act for the past three years. He joined Senator Fred Thompson (R-Ten) to review the act in 2000 as the minority member of the Senate Governmental Affairs Committee.[36] As the act was about to expire in 2002, Lieberman and Thompson asked GAO for a review of Enterprise Architecture development as

required by Clinger-Cohen. Lieberman introduced sweeping follow-on legislation in the E-Government Act of 2002, which became effective April 17, 2003.

The E-Gov Act made the CIO Council a federal body and ultimately made Forman the Federal CIO. He now manages all agency CIOs, positions he created in Clinger-Cohen six years earlier. The E-Gov Act:

- codifies OMB's role with the establishment of the E-Gov Administrator position and the Office of E-Government (Federal CIO)
- codifies the CIO Council
- directs that agencies develop citizen and productivity-related performance measures to support agency objectives, strategic goals, and mandates
- endorses and requires agencies to support cross agency initiatives.

Review of Forman's progress

On September 20, 2002, a year after 9/11, and 15 months into Forman's tenure at OMB, the International Council for Information Technology in Government Administration, (ICA) outlined activities necessary for governments contemplating future shared IT initiatives:[37]

1. **Develop a governance structure for IT investments**, standards and decision-making that would better balance whole -of-government goals and strategic objectives with those of individual agencies;
2. **Provide centralized funding for government-wide initiatives** to provide agencies with a greater incentive for full participation than would be the case if they were individually responsible for the costs;
3. **Focus first on the definition of shared business processes and common data definitions**, and only then on the most effective system solutions for implementing those processes;
4. **Consider a common, government wide infrastructure** for secure reporting, data sharing, workflow and interoperability;
5. **Consider a shared services approach** whereby a professional, fee-for-service agency becomes fully accountable for the delivery of specified services, and thereby assumes responsibility for (and a vested interest in) technology decisions related to how those services may be delivered most efficiently and effectively;
6. **Do a comprehensive business case** which includes total cost of ownership; and
7. **Benchmark existing costs, define appropriate performance measures, and track costs and performance through the full life cycle of any new initiatives** so as to be able to accurately determine whether anticipated benefits are indeed being realized and make any necessary adjustments.

As a Senate Governmental Affairs Staff member, Forman helped write most of these steps into Clinger-Cohen. As OMB's Associate Director for

Information Technology and e-Government, he had the opportunity to implement most of them.

1. **Develop a governance structure for IT investments –** Forman used FY 03 budget passback[38] language to move agencies closer to the Clinger-Cohen Capital Planning Investment Control (CPIC) process. Section 53 of OMB circular A-11 outlines the governance process. "The governance processes required as attendant documents to this section (IRM Plan, documented CPIC process, and the Enterprise Architecture) are used in connection with the business cases (Exhibit 300) and this "Agency IT Investment Portfolio" (Exhibit 53) to demonstrate the agency management of IT investments and how these governance processes are used to make decisions about IT investments within the agency."

2. **Provide centralized funding for government-wide initiatives –** The e-Government Act of 2002 contains provisions for a fund to finance cross-agency initiatives.

3. **Focus first on the definition of shared business processes and common data definitions** – This has always been a Forman mantra… "*Lines of business"* has been the basis for the Quicksilver consolidation efforts and the FEAPMO Business Reference Model and Data Reference Model are key components of the Federal Enterprise Architecture.

4. **Consider a common, government wide infrastructure –** State Department's successful completion of a worldwide infrastructure on time and under-budget has inspired Forman to consider the same concept government wide.[39]

5. **Consider a shared services approach –** with the administrations move to outsource more and OMB's direction to unify and simplify, this is a distinct possibility, although not currently evident.

6. **Do a comprehensive business case -** Forman has introduced new requirements for the FY 06 budget requests. OMB will require one large business case justifying investments in networks and computers agency wide in addition to individual business cases for software investments.

7. **Benchmark existing costs, define appropriate performance measures, and track costs and performance through the full life cycle of any new initiatives –** Major new initiatives have to complete an exhibit 300 submission to OMB which outlines costs, performance measures, and ROI calculations. Because the IT budget is zero based, each years IT submissions must track costs and performance against

previously outlined performance measures. Further, OMB has mandated stronger performance measures, ROI, and Evaluation methodologies be included as part of every agencies President's Management Agenda Scorecard.

Conclusion

There is an old saying in Washington that goes, *"If it is not in the budget, it is not important."* The nearly $60 billion this nations taxpayers spend on Information Technology this year indicate that it is critically important. "What Mark Forman needs to ensure is that agencies are **managing** IT resources more effectively within an agency and across agencies, to achieve economies of scale," according to Representative Tom Davis (R-VA), Chairman of the House Committee on Government Reform.[40]

Mark A. Forman realizes the importance of **managing** Federal Information Technology spending to maximize service to citizens. He helped craft legislation in 1996 that laid out a design to improve the governance, interoperability, and security of the federal IT enterprise.

Clinger-Cohen required agencies to **manage** their IT budgets by adhering to a Capital Planning Investment Control (CPIC) process, developing an Enterprise Architecture (with a security element), and establishing a Chief Information Officer.

GISRA (the Security Act) further required system program managers to **manage** the security elements of their individual programs. It required annual reviews of systems to identify vulnerabilities and risks, and plans to address those risks.

Mark Forman's clear vision of how the federal IT landscape should look has not changed for the past seven years. The e-Gov Act of 2002 renews Clinger-Cohen and the Federal Information Security Management Act (FISMA), which has been called GISRA with teeth, was signed into law and rolled into the e-Gov Act.

OMB's contention that security management at the program level leads to increased security across the entire enterprise is a sound argument. Weaknesses in program security are failures by system managers to

- prepare system level security plans,
- complete Certifications and Accreditations,
- include security in their programs related to the Enterprise Architectures, and
- include security in their programs business cases, system administration, operations, and system support practices.

Mark Forman's and OMB's plan to trim the $60 billion FY 2004 IT budget, as outlined in this paper, include efforts to improve security within the Federal IT budget process while ensuring progress in e-Government interoperability.

Representative Davis concluded, "He [Forman] is heading in the right direction with the kinds of things he is trying to do."[41]

Bibliography

[1] http://www.results.gov/agenda/index.html
[2] Budget of the United States Government, Fiscal Year 2004; The White House Office of Management and Budget; May, 2003; Page 335
[3] U.S. Department of Agriculture; Information Technology Capital Planning and Investment Control Guide; April 2002, Chief Information Officer
[4] David Godesky, Deputy Project Manager for the Consolidated Health Informatics E-Gov Initiative; Powerpoint; October 10, 2002
[5] Op. Cit.
[6] OMB Memorandum 97-02; *Funding Information System Investments; October 25, 1996*
[7] Ibid
[8] OMB Memorandum M-97-16; *Information Technology Architectures*; Director Franklin D. Raines; June 18, 1997.
[9] *A Passion for E-Government;* Mark Forman; Power Point Presentation
[10] Statement of Mark Everson and Mark Forman before the House Subcommittee on Technology and Procurement Policy (S. 803 –Egov Testimony); September 18, 2002
[11] News.Com Vision Series Profile: U.S. Office of Management and Budget's Mark Forman; by Alorie Gilbert; 2001
[12] *Leading the Government's Digital Transformation,* by Alorie Gilbert; CNET News.com; June 11, 2002
[13] Federal Enterprise Architecture Framework (FEAF), Version 1.1; CIO Council, September 1999
[14] *Information Technology: Enterprise Architecture Use Across the Federal Government Can Be Improved*, GAO, Feb 2002
[15] OMB Releases New Business Reference Model to Improve Agency Management**;** Early Application Critical to Citizen Service; OMB Press Release 2002-50; July 24, 2002.
[16] Statement of Mark Everson and Mark Forman Before the House Subcommittee on Technology and Procurement Policy (S. 803 – Egov Testimony); September 18, 2002.
[17] Statement of Mark Forman before the Committee on Government Reform, Subcommittee on Technology and Procurement Policy, U.S. House of Representatives; June 7, 2002
[18] OMB Circular A-130, *Management of Federal Information Resources*
[19] http://www.infoplease.com/ce6/history/A0834968.html
[20] http://rip.physics.unk.edu/kearney/hiway2.html
[21] http://www.factmonster.com/spot/interstate1.html
[22] http://spider.georgetowncollege.edu/htallant/border/bs10/mitchell.htm
[23] *Administration Changes IT Budget Rules,* by Karen Robb; Federal Times.com; June 20, 2003; http://federaltimes.com/index.php?S=1958321
[24] *As threats rise, feds shelter their IT,* by Richard Walker; Government Computer News, 6.16.03

[25] Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. GAO-03-303T November 19, 2002
[26] Mark Forman before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census; Committee on Government Reform; United States House of Representatives; March 4, 2003
[27] *Spending more might not ensure computer* security, by TANG WENG FAI; Biz IT; April 14, 2003
[28] http://security.ittoolbox.com/pub/research/spending_survey.htm
[29] *Managing Risk* by Timothy Dyk; eWeek Magazine; June 16, 2003
[30] The Art of Uncertainty, by Elaine Cummings; CSO Magazine; December 2002
[31] *Leading the Government's Digital Transformation* by Alorie Gilbert; CNET News.com; June 11, 2002
[32] Mark Forman statement before the committee on Government Reform, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations; U.S. House of Representatives; November 9, 2001
[33] Op. Cit.
[34]Statement of Mark Forman, before the Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, U.S. House of Representatives; November 19, 2002.
[35] *As Threats Rise, feds shelter their IT,* by Richard Walker; Government Computer News; 6/16/03
[36] *Investigative Report of Senator Fred Thompson on Federal Agency Compliance with the Clinger-Cohen Act;* October 20, 2000; http://www.senate.gov/~gov_affairs/101900_table.htm
[37] International Council for Information Technology in Government Administration, ICA Study Group on SHARED SYSTEMS, Experience Gained and Lessons Learned; Draft 5 – September 20, 2002; http://www.ica-it.org/
[38] When agencies submit budgets to OMB, they are reviewed and a "*passback*" document discussing issues in the agency budget process is prepared and returned to each agency.
[39] *For State Department Employees, Internet Access is Something New,* by Karen Robb; Federal Times; June 16, 2003
[40] *Interview: Rep. Tom Davis, IT procurement reformer*; Government Computer News; March 4, 2002
[41] Ibid

Last Updated: October 2nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced