

Management of Large Public Information Technology Projects
The United States Federal Government
Presented by Jack Arthur
Chief Information Officer USDA Forest Service
October 25, 2000

General Institutional Framework Country Report

Introduction

A. Policies

- 1. Background**
- 2. Contemporary Policy**
- 3. Consolidated IT Management Direction**

B. Emerging IT Management Issues

- 1. Y2K Problem**
- 2. E-government**
- 3. Cyber Security**

C. IT Funding/Decision/Assessment

- 1. Selecting**
- 2. Controlling**
- 3. Evaluating**

D. IT Project Management Elements

- 1. Investment Management**
- 2. Information Management**
- 3. IT Architecture**
- 4. System Development Environment**
- 5. Management of the Paperless Environment**
- 6. Information Security**

E. Cases and Lessons – Real Life Examples of Good News and Bad News

- 1. Advanced Interactive Weather System**
- 2. National Atlas of the United States**
- 3. Docket Management System**
- 4. Large Scale Federal Land and Minerals Records System**
- 5. Large Agency Modernization**
- 6. “ILOVEYOU” Virus**

F. Websites

Introduction

Despite the best efforts of the federal government, most policy makers are troubled by the high failure rate of large IT projects. It is difficult to understand how many of these projects can go on for years, returning no useful product, finally requiring them to be scrapped. At the same time there are many notable successes, many valuable lessons learned, and much improved policy and direction to help ensure success in new projects. This report summarizes the policy framework for managing IT projects in the U.S.

federal government, as well as experience with specific cases during the last few years. References to lessons learned and several emerging IT management issues, are also discussed.

A. Policies

1. Background

During the last 40 years, the federal government has been working to increase the effectiveness of the management of information and technology to its' business. The first major policy direction was provided by the 1965 Brooks Act, which established central oversight of federal information technology acquisitions by the General Services Administration (GSA)¹. This law was primarily aimed at the effective purchase and use of the large and expensive mainframe computers of the time.

In 1980, the Paperwork Reduction Act (PRA) addressed the management of information, reducing the burden of the collection of information, and emphasizing lifecycle management principles in doing this. It also created senior information resource management officials across government to manage IT activities, focusing management attention on the importance of these efforts in effective operation. Responsibilities were spelled out for planning, budgeting, controlling and reviewing all information management activities including major IT projects. The act also created the Office of Information and Regulatory Affairs in the Office of Management and Budget (OMB)², which oversees Federal regulations and information requirements, and develops policies to improve government statistics and information management. A major responsibility of this office is to direct, manage and review IT policies and activities across the government. The law also includes the following goals for federal agency use of information technology:

- improve service delivery and program management,
- increase productivity,
- improve decision making,

¹ GSA provides policy leadership and managed space, supplies, services, and solutions for the U.S. Government. GSA also provides workspace, security, furniture, equipment, supplies, tools, computers, and telephones, as well as travel and transportation services, and develops, advocates, and evaluates government-wide policy.

² OMB's predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's budget and with Administration policies. In addition, OMB oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies. In each of these areas, OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public.

- reduce waste and fraud, and reduce information processing burden for the federal government and for the publics that provide information to the federal government.

2. Contemporary Policy

In the early 1990's, additional direction was provided for overall organization performance, recognizing the critical role of IT and information management in the delivery of government functions. The Government Performance and Results Act (GPRA)³ of 1993 requires that agencies set strategic goals, measure performance toward the goals, and report on their progress. Effective implementation of GPRA critically relies on agencies' ability to produce the meaningfully integrated information needed to manage performance and measure results.

Further policy and direction was provided with the reauthorization of the PRA⁴ in 1995 which requires that agencies indicate in strategic information resources management plans how they are applying information resources to improve the productivity, efficiency, and effectiveness of government programs, including improvements in the delivery of services to the public. Provisions in this law also require OMB to help agencies acquire and use information technology through the review of agency budget requests, other plans, and analysis that support information technology projects.

3. Consolidated IT Management Direction

In 1996, policies for management of large IT projects were consolidated and reformulated in the Clinger-Cohen Act⁵. This law describes responsibilities and actions for the executive branch of government including:

- The Director of the OMB, and
- Executive Agencies (including Chief Information Officers).

IT policy is provided for:

- capital investment decision processes to ensure good return on investment,
- modular development processes to avoid "large scale failures",
- risk assessment processes to ensure sound security practices and high success probability, and
- post implementation review and evaluation processes to ensure continuing results and course corrections where appropriate.

The Act prescribes specific direction for:

³ Section 5501 of Title 15, Public Law 103-62.

⁴ Public Law 104-13.

⁵ Public Law 104-106, previously known as the Information Technology Management Reform Act (ITMRA).

- creation of Chief Information Officers in each major agency,
- planning and acquiring of IT,
- IT multiple award schedule contracting,
- incremental procurement of IT, and
- maintaining a directory of information resources.

Provisions of this law are described in more detail below, particularly the direction for the capital investment decision process.

B. Emerging IT Management Issues

The above IT management policies were formulated and implemented through the mid-1990's. Since that time, three major issues have evolved that have strongly influenced IT management across the U.S. Government:

- Year 2000 (Y2K) problem,
- transformation of government functions to the electronic medium (E-government), and
- problems with computer or "cyber" security.

1. Y2K Problem

Beginning in earnest in the Spring of 1997, the course of IT in all sectors was altered significantly with the extraordinary effort on the Y2K problem. By 1999, the U.S. federal government had designated "resolving the Y2K problem as our foremost management objective". IT and related general management policies, practices and processes were all refocused during this period until the Y2K problem was successfully solved in January, 2000. The primary success factors that were reinforced and are now being incorporated into policies and practices as a result of this effort are the value of:

- top-level management attention,
- effective risk analysis in guiding direction,
- complete systems inventories,
- independent reviews by independent auditors and contractors,
- comprehensive testing methods and procedures, and
- business continuity and contingency planning.

The IT management institutional framework has been strongly influenced by the successful experience with these factors and by the sheer force of experience in the Y2K effort.

2. E-government

With the phenomenal growth and impact of the Internet and the World Wide Web over the past five years, there has been a strong recognition of the need for the federal government for interaction with the public to be brought fully into this environment.

Guidance for converting federal government activities to electronic commerce and general paperless operation is provided in the Government Paperwork Elimination Act (GPEA)⁶. This Act requires that federal government agencies “must offer the option, when practicable, for the maintenance, submission, or disclosure of information by electronic means by October 2003”. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages federal government use of a range of electronic signature alternatives. The implementation of GPEA is rapidly driving many major IT projects to meet these E-government initiatives in addition to their original objectives. IT policies and guidance are being transformed to accommodate this shift.

3. Cyber Security

Rampant federal government computer break-ins, denials of service, and general disruption of computer services has been causing increasing concern that these services can continue to operate and grow effectively unless further actions are taken to mitigate the risks. In partial answer to public concern about these issues in both the private and public sector, guidance and direction on Computer Security has been provided in the President’s January, 2000 National Plan for Information Systems Protection⁷. Among other general provisions, this plan outlines a number of new, centrally managed entities and projects that have been initiated to assist agencies in strengthening their security programs and improving federal intrusion detection capabilities. In addition, on March 3, 2000, in response to recent Internet disruptions, the President issued a memorandum to the heads of executive departments and agencies urging them to renew their efforts to safeguard their computer systems against denial-of-service attacks from the Internet. These risk considerations cause particular concern on the interdependence of IT systems and inject another element of complexity in the application of the above policies governing a particular IT project.

C. IT Funding/Decision/Assessment

The U.S. Government spends more than \$38 billion each year on IT, and this number will continue to grow as virtually all functions of Government take advantage of efficiencies provided by IT. Well selected, controlled, and managed IT projects provide some of the best opportunities for agencies to fulfill their missions with the lowest cost and greatest benefits. The Budget of the U.S. Government for FY 2001 includes a priority management objective to strengthen government-wide management by using capital planning and investment control to better manage IT. For a summary of these investments, Table 22.1 of the Analytical Perspectives of the FY 2001 Budget⁸ provides both a total of all IT investments for the U.S. Government and a selection of IT investments focusing on program and performance benefits.

⁶ Public Law 105-277.

⁷ Defending America’s Cyberspace: National Plan for Information Systems Protection: An Invitation to a Dialogue, issued by the President on January 7, 2000.

⁸ Budget of the United States Government for FY 2001.

These three central management offices play the major role in the IT investment and decision making process in the federal government:

- Office of Management and Budget,
- General Accounting Office (GAO)⁹, and
- General Services Administration (GSA).

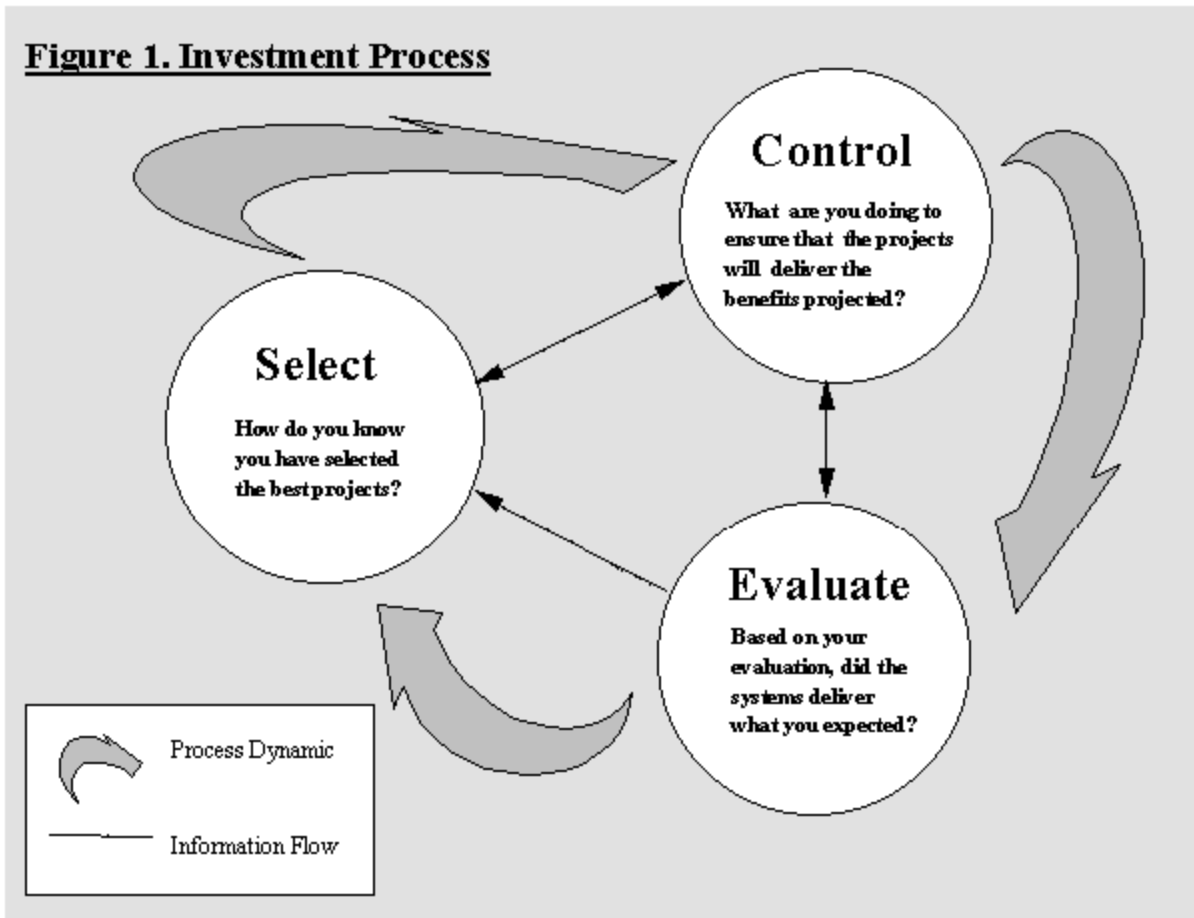
The Office of Management and Budget provides direction on Evaluating Information Technology Investments¹⁰. This direction describes three major phases of the investment and control process for IT projects:

- selecting (screening, evaluating risks and return, and mission mix),
 - controlling (monitoring against costs, schedule and performance), and
 - evaluating (post implementation reviews, adjustments, and lessons).
-

⁹ The General Accounting Office is the investigative arm of Congress. GAO exists to support the Congress in meeting its Constitutional responsibilities and to help improve the performance and accountability of the federal government.

¹⁰ Office of Management and Budget Memorandum M-97-02 and additional guidance.

Figure 1. Investment Process



This IT investment process is followed in each agency as it proposes IT investments in the annual budget process. OMB reviews and decides on all aspects of an IT proposal, including what level of funding will be contained in the President’s Budget when it is submitted to Congress. Final funding decisions are made in the Fiscal Year Appropriations process as the Congress of the United States sends each of the 13 Appropriations Laws to the President for signature. Large IT projects are always multi-year, and at any point in the project lifecycle OMB may conduct a review to determine progress. At least annually, as part of the Budget process major technology projects must be reported on and reviewed¹¹.

Additionally, at any point in the funding and decision process, GAO may be asked to conduct a review of an IT project by any member of the U.S. Congress. These reviews may be at the proposal, funding, implementation, or post-implementation stage. Agencies are generally allowed to comment on, and respond to, the contents of these reviews before they are presented to the requester or made public. There are also occasions where private reports are provided to the requesting member and no public

¹¹ As stipulated in OMB Circular A-11, Preparation and Submission of Budget Estimates.

report is made. GAO has described an IT Investment Framework¹² which describes five maturity stages and the critical processes for each. This framework is used as a standard in reviewing IT investment processes in agencies:

Stage 1 – Creating Investment Awareness

Critical Processes

- IT spending without disciplined investment processes
- IT subordinated in mission expenditures

Stage 2 – Building the investment foundation

Critical Processes

- IT investment board operation
- IT project oversight
- IT asset tracking
- Business needs identification for IT projects
- Proposal selection

Stage 3 – Developing a common investment portfolio

Critical processes

- Authority alignment of IT investment boards
- Portfolio selection criteria definition
- Investment analysis
- Portfolio development
- Portfolio performance oversight

Stage 4 – Improving investment process

Critical processes

- Post-implementation reviews and feedback
- Portfolio performance evaluation and improvement
- Systems and technology succession management

Stage 5 – Leveraging IT for strategic outcomes

Critical processes

- Investment process benchmarking
- IT-driven strategic business change

Agencies expect to be reviewed on these criteria, and have a strong incentive to develop the critical processes described in this framework.

GSA formulates and administers IT investment policy as well, and is the controlling agency for the IT procurement process. This includes the oversight and management process for granting Delegated Procurement Authority (DPA) for large IT projects, and is required to proceed with procurements with the IT industry. GSA also has a division for

¹² Information Technology Assessment Management: An Overview of GAO's Assessment Framework, May 2000

providing specific IT services¹³ to agencies, these services allow agencies to more easily procure specific technical skills and IT management expertise.

D. IT Project Management Elements

For large IT projects, within the policy framework above, major management elements are:

- investment management,
- information management,
- IT architecture,
- system development environment,
- management of the paperless environment, and
- information security.

IT investment management is an integrated view that provides for life-cycle management of the IT project. As described above, there are three phases of the process: selection, control, and evaluation. In the selection phase, the agency or organization determines priorities makes decisions about which projects will be funded based on the technical soundness of the projects, their contribution to mission needs, performance improvement priorities, and overall IT capital funding levels. The costs, benefits, and risks of all IT projects are assessed and the projects are compared against each other and ranked. In the control phase, all projects are compared at similar stages in development. Progress reviews, in which progress is compared against projected cost, schedule, and expected mission benefits, are conducted at key milestones in each project's lifecycle. The evaluation phase compares actual performance against estimates to identify and assess areas in which future decision-making can be improved.¹⁴

Information management is the proper consideration for the collection, use, and dissemination of the information itself, which is contained in a large IT project. Each system must provide for public access to records where required and appropriate. The system must be designed so that it will collect or create only that information necessary for the proper performance of agency functions and which has practical utility. Agencies must ensure that proper records are maintained, and that the public is not unduly burdened by the requirement to provide information mandated by an information system.¹⁵

IT architecture is a blueprint -- consisting of logical and technical components -- to guide the development and evolution of a collection of related systems. The architecture provides a high-level description of an organization's mission, the business functions

¹³ GSA Federal Technology Service delivers a range of telecommunications, information technology systems, hardware and software, consulting services, information security services and products and integrated technology solutions.

¹⁴ More detail can be found in the GAO Guide "Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making", February 1997.

¹⁵ More detail can be found in OMB Circular A-130 "Management of Federal Information Resources".

being performed, and the relationship among the functions, the information needed to perform the functions, and the flow of information among the functions. Technically, the architecture provides the rules and standards needed to ensure that the interrelated IT projects are built to be interoperable and maintainable.

A systems development environment is also defined so that each major IT project can apply the elements of that environment for consistent management and control. Systems development is the most sensitive part of large IT projects, and most failures occur because the development of software never meets expectations, or cannot be made operational. To provide the software needed for a major IT project, the organization can develop software using its own staff, use a contractor to develop software, use commercial off-the-shelf software, or a combination. To effectively manage software development and acquisition processes, however, the organization needs to have well-defined software management processes, including methodologies and standards that will be used. Key processes for software development include requirements management, project planning, project tracking and oversight, quality assurance, and configuration management. For software acquisition, additional management is needed for solicitation, contract tracking and oversight, product evaluation, and transition to implementation and support.

Management of the paperless environment, is the increasingly important consideration of how the business of the agency is conducted in the electronic medium. This involves consideration of how electronic commerce is conducted between agencies, the public, and the commercial sector. Large IT projects must participate in this environment, and special consideration must be given to authenticity, electronic signature, adequate electronic audit trails, and related elements when conducting business. Consideration must also be given to equal access by participants in a system, when electronic access is required to do business. Paper, or other alternatives may need to be maintained, if some participants cannot practically gain electronic access¹⁶.

Information security policies and practices provide the framework to protect an organization's computer-supported resources and assets. This protection ensures the integrity, appropriate confidentiality, and availability of the data and systems of an organization. Integrity ensures that data have not been altered or destroyed in an unauthorized manner. Confidentiality ensures that information is not made available or disclosed to unauthorized individuals or entities. Availability ensures that data will be accessible or usable upon demand by an authorized entity. Key activities for managing information security are risk assessment, awareness, controls, evaluation, and central management. Risk assessments consist of identifying threats and vulnerabilities to information assets and operational capabilities, ranking risk exposures, and identifying cost-effective controls. Awareness involves promoting knowledge of security risks and educating users about security policies, procedures and responsibilities. Evaluation involves monitoring effectiveness of controls and awareness activities through periodic evaluations. Central management involves coordinating security through a centralized group.

¹⁶ This is sometimes known as the "digital divide" issue.

E. Cases and Lessons – Real Life Examples of Good News and Bad News

We often cite notable failures of major IT projects when looking for lessons, but it is also important to recognize when major information systems are working well, making real contributions to the business of government. An example of this type of recognition is the Government Technology Leadership Awards¹⁷ program, whose purpose is to highlight IT program contributions and successes. Three recent winners of this program are summarized¹⁸ here as a reminder of the kind of results being achieved by major IT projects, in spite of the risks and problems that exist.

Case 1 – National Weather Service “Advanced Interactive Weather System”

On May 3, 1999 more than 70 tornadoes ripped through Oklahoma and southern Kansas. The tornadoes left hundreds injured, took almost 50 lives and caused more than \$1 billion in damage. Had the National Weather Service been caught unaware, casualties could have been worse. Thanks to NWS' new \$540 million Advanced Weather Interactive Processing System (AWIPS), forecasters were able to issue warnings with an average lead time of 32 minutes before severe weather hit. The Norman, Okla., office issued 70 tornado warnings and 46 severe thunderstorm warnings over 10 hours on May 3. NWS attributes part of their successful coverage to the use of multiple AWIPS workstations that enabled NWS forecasters to divide their areas of responsibility geographically.

"We've put in place a new line of super computers for atmospheric modeling," says Mary Glackin, AWIPS program manager. "The key element of this is AWIPS. It brings all of these new data sets right to the forecaster on one display and allows for data analysis in a short amount of time." Glackin says speed in forecasting is vital. "Many hazardous weather events happen in a short time frame, like flash flooding or tornadoes," says Glackin. "We can manipulate the data and get a warning out virtually within seconds." "With AWIPS we are able to pick up precursors of significant weather events," adds Glackin. "Even a few minutes improvement makes a lot of difference." Glackin says that AWIPS employs an open systems architecture that allows the NWS to continually modify the system. "Our intent is not to let it get obsolete. Ultimately the goal is to keep pace with the sciences of meteorology and hydrology."

Case 2 – U.S. Geological Survey “National Atlas of the United States”

When the first National Atlas of the United States appeared in 1970, it weighed 12 pounds and was limited to a production run of 15,000 copies. Almost 30 years later, in a meeting between U.S. Geological Survey officials and Sen. Slade Gorton, R-

¹⁷ Sponsored by Government Executive Magazine and a public-private partnership.

¹⁸ Government Executive Magazine, December 1999, Vol. 31, Number 12.

Wash., the senator hefted a copy of the 1970 behemoth and asked, "When are you going to do another one of these?"

In 1997, the USGS received the first \$1 million of \$5 million in congressional funding for its National Atlas project. However, this National Atlas is very different than its predecessor—it's on the World Wide Web. Users can create their own maps on the Web using data from the USGS, Census Bureau, Environmental Protection Agency and other agencies. "This has been a leadership role for the USGS and as much a coordination role as anything else," says Jay Donnelly, the Atlas' managing editor. "With the World Wide Web as the publishing medium we no longer have to restrict content. We can make the digital representations of maps available to the public regardless of theme." This means users can create maps using a standard Web browser. The maps can combine demographic, environmental, geographic, geologic and even biological data. For example, users can create a map that displays the nation's streams and watersheds overlaid with data on toxic releases or Superfund sites.

USGS has produced hard-copy maps for the project, but the days of the 12-pounder are gone. These are separate maps on specific subjects such as the nation's principal aquifers/groundwater resources, watershed boundaries and the distribution of federal and American Indian-owned land. Most recently the USGS released a shaded relief map of North America. It will issue a map on the nation's wetlands next. All printed maps have Web-based counterparts.

Case 3 – U.S. Department of Transportation “Docket Management System”

When the Transportation Department prepares new rules on air bags or hazardous material transport, each new regulation is tracked with a bulging file of petitions, public comments and final decisions called a docket. In 1993, Transportation operated nine docket rooms, each with its own staff. Researching a docket sometimes meant long, hot waits. Then there were the trips between the docket rooms only to find a docket was missing and presumed lost forever. So the agency formed a central docket room in Washington. And then DOT went one step further: It moved the whole process to the Web. No more lawyers gnashing their teeth over a prized docket.

Now, interested public and private sector parties can stay up to date by looking at the Docket Management System (DMS) Web site. All information that is contained in a single paper-based docket--commentary, adjudications, extensions -- are now available to everyone at once. DMS lists the top-requested dockets on the system. Last fall, for example, the leader was a Maritime Administration docket on attempts to re-register eight ships designed to carry liquefied natural gas under a foreign flag. It had chalked up more than 12,000 hits. Interested parties include everyone from the petitioning companies and concerned citizens to the sailors on the ships that would be affected by such re-registration. Commentary and official documents can be submitted on paper or via e-mail. Decisions handed down by DOT officials are listed

as well. DOT is in the process of putting its entire backlog of paper-based docket online.

Of course, many major IT projects do not work well, and are subject to intense scrutiny in the management and oversight process. Several cases are summarized here to highlight problems, characteristics, and help identify lessons that can be learned from these efforts as well.

Case 4 -- A large scale federal land and minerals record system – a failure

In a review of this troubled system in 1999, GAO¹⁹ described the history as follows:

During the energy boom of the early 1980s, the bureau found that it could not handle the case processing workload associated with a growing number of applications for oil and gas leases. The bureau recognized that to keep up with increased demand, it needed to automate its manual records and case processing activities. Therefore, in the mid-1980s, it began planning to acquire an automated land and mineral case processing system. At that time, the bureau estimated that the life-cycle cost of such a system would be about \$240 million.

In 1988 the bureau expanded the scope of the system to include a land information system (LIS). The expanded system was to provide automated information systems and geographic information systems technology capabilities to support other land management functions, such as land use and resource planning. The bureau combined the LIS with a project to modernize the bureau's computer and telecommunications equipment, and estimated the total life-cycle cost of this combined project to be \$880 million. The project was reduced in scope in 1989 to respond to concern about the high cost. The project consisted of three major components—the Initial Operating Capability (IOC), a geographic coordinate database, and the modernization of the bureau's computer and telecommunications infrastructure and re-host of selected management and administrative systems. Estimated life-cycle costs were \$575 million (later reduced to \$403 million), and the bureau planned to complete the entire project by the end of fiscal year 1996.

The IOC was to be the flagship of the modernization, and was to replace various manual and ad hoc automated systems. The bureau designated the IOC a critical system for (1) automating land and mineral records, (2) supporting case processing activities, including leasing oil and gas reserves and recording valid mining claims, and (3) providing information for land and resource management activities, including timber sales and grazing leases. The system was expected to more efficiently record, maintain, and retrieve land description, ownership, and use information to support the bureau, other federal programs, and interested parties. It was to do this by using the new computer and telecommunications equipment that was deployed throughout the

¹⁹ GAO Congressional Testimony GAO/T-AIMD-99-102, March 4, 1999.

bureau, integrating multiple databases into a single geographically referenced database, shortening the time to complete case processing activities, and automating costly manual records.

Despite the promise of IOC to significantly improve business operations, repeated problems with its development have prevented deployment. For example, during a user evaluation test in May 1996, problems were reported involving unacceptably slow system performance. Subsequent testing in 1996 uncovered 204 high-priority software problems, which delayed project completion by about a year. In testing conducted in November 1997, the bureau encountered workstation failures and slowdowns caused by insufficient workstation memory and by problems discovered in two bureau-developed software applications. Some of these problems had been identified in earlier tests but had not been corrected. Additional testing uncovered software errors that resulted in missing, incorrect, and incomplete data, and error files that contained accurate data. As a result of these problems, the bureau postponed the Operational Assessment Test and Evaluation (OAT&E) that had been scheduled for December 1997. The OAT&E was to determine whether the IOC was ready to be deployed to the first state office.

In October 1998, the OAT&E was conducted and showed that the IOC was not ready to be deployed because it did not meet requirements. During the test, users reported several problems, including that the IOC (1) did not support the bureau's business activities, (2) was too complex, and (3) significantly impeded worker productivity. For example, one tester reported that entering data for a \$10 sale of a commodity, such as gravel, required an hour of data entry using the IOC, whereas with the existing system, the same transaction would have taken about 10 minutes. Users also reported that system response time problems were severe or catastrophic at all test sites. One user said "It is ridiculous to spend 2 or 3 hours to enter information in this system, when it takes 30 minutes to an hour to process the information into the legacy system." Finally, users reported data converted from legacy databases were not accurate, and that validation of the converted legacy data required inordinate effort and time.

Because these problems are significant, senior bureau officials have decided that the IOC is not currently deployable. According to the bureau, it obligated about \$411 million on the project between fiscal years 1983 and 1998, of which more than \$67 million was spent to develop the IOC software. The \$67 million does not include the IOC costs that are part of other cost categories, such as costs for work performed from fiscal years 1983 through 1988, project management, computer and telecommunications hardware and software, data management, and systems operation and maintenance.

This is not an isolated incident, but it is hard to understand how so many years and so much energy could be expended on a project before deciding to stop development and terminate the project. In looking for shortcomings leading up to the cancellation of this project, it was concluded that the bureau:

- did not develop a system architecture or formulate a concept of operations before designing and developing the project,
- never had a credible project schedule, reliable milestones, or a critical path to manage the development and deployment of the project,
- faced serious risks because it had not established a robust configuration management program for the project,
- incurred serious risks because it had not established a security plan or security architecture for the project,
- invited serious risks because it had not established transition plans to guide the incorporation of IOC into its daily operations,
- faced serious risks because it had not established operations and maintenance plans, and
- invited serious risks because it planned to stress test only the IOC component—and not the entire system workload including email, office systems and other production applications.

All of these items are covered in policies and direction above, but were not made a critical part of the project management process. A major lesson here is the value of independent project review and evaluation, objectively identifying risks and problems in the direction of the project. In this project, there were reviews and warnings along the way (in the “monitoring and controlling phase”), but were apparently never taken seriously enough by bureau management. An additional lesson is the danger created by the momentum of a project that is too ambitious in scope, and takes on a life of its’ own. This can have the effect of threatening the reputation of the organization to the point that “it cannot fail”, causing a defensiveness and lack of objectivity on the part of organization management. A more modular project formulation (instead of the “grand design”²⁰ approach) with more opportunities to adjust to changes in circumstance, technology, and requirements could have avoided the “all or nothing” nature of the cancellation.

Case 5 – A large agency modernization – getting coherence in major systems.

In a review in May 2000 GAO²¹ described this system as follows:

Over a decade ago, the Service began its systems modernization program, then called Tax Systems Modernization (TSM), to establish a virtually paper-free tax processing environment where taxpayer information would be readily available to service employees for updating taxpayer accounts and responding to taxpayer inquiries. In 1995, we identified serious management and technical weaknesses with TSM that jeopardized its successful completion. Accordingly, we made over a dozen

²⁰The “grand design” approach involves investing in a large, long-term, expensive project based on cost and benefit estimates prepared at the outset and attempting to deliver the entire project years later as a single increment.

²¹ GAO Report GAO/AIMD-00-175, May 2000.

recommendations to fix the problems, such as formulating a comprehensive business strategy, establishing information technology (IT) investment management processes, and completing and enforcing an integrated enterprise architecture. In addition, because of the seriousness of the weaknesses, we designated TSM as a high-risk IT initiative, placed the modernization on our list of high-risk federal programs, and have continued to monitor this program.

In 1998, the Congress established an Information Technology Investment Account (ITIA) and limited the Service's obligation of ITIA funds until the Service submits to the Congress for approval an expenditure plan that meets certain conditions. The conditions are that the plan should (1) implement the modernization blueprint, (2) meet OMB's IT investment guidelines, (3) be reviewed and approved by the Service's Investment Review Board, OMB, and the overseeing agency Management Board and be reviewed by GAO, (4) meet the requirements of the Service's life cycle program, and (5) comply with acquisition rules, requirements, guidelines, and systems acquisitions management practices of the federal government. To date, the Congress has appropriated \$506 million for the account via the Service's fiscal year 1998 and 1999 appropriations acts.

In May 1999, the Service submitted its first or "initial" expenditure plan, requesting about \$35 million for modernization initiatives and commitments to be delivered by October 31, 1999. As part of this plan, the Service also stated its intention to modernize its systems incrementally and submit incremental expenditure plans for release of ITIA funds. We reviewed the plan and reported in June 1999 that this incremental approach was an industry best practice, and if properly implemented, the plan was an appropriate first step. However, to measure the Service's modernization performance and accountability on this and future expenditure plans, we recommended that each plan fully disclose the Service's progress against incremental goals, deliverables, and benefits set forth in earlier plans. Based on our report, the House and Senate Appropriations Subcommittees approved the Service's \$35 million expenditure plan in June 1999.

At that time, the Service planned to submit a second expenditure plan in October 1999. However, it was unable to do so on time, and in early December 1999, submitted to the House and Senate appropriations subcommittees a "stopgap" funding measure to obligate about \$33 million from ITIA until the next plan was submitted. We reviewed the "stopgap" funding measure and raised concerns about projects that were scheduled to begin detailed design and software development before, among other things, the enterprise architecture and the Enterprise Life Cycle (ELC) was defined and implemented. Later that December, the appropriations subcommittees approved the Service's \$33 million "stopgap" funding measure but in discussions and correspondence, directed IRS to (1) expedite completion of the architecture and implementation of the ELC and (2) explain in future expenditure plans how it plans to manage the risk of performing detailed design or development work if the architecture is not completed or the ELC is not implemented.

This is a case where concerns with the coordination and control of the “modernization” of the tax systems were so pervasive, that special funding controls were put in place to help manage the projects. Concerns centered on the need for a coherent enterprise lifecycle and enterprise architecture before detailed systems design and implementation were begun. These concerns were heightened by past problems in delivering IT projects in the Service – there have been many previous cases with lack of performance. One of the lessons learned from this case, is that the basic policies for management and control of a very large environment are not very different in concept from projects of a far more moderate size. The need for life cycle funding and management, the need for a coherent enterprise architecture, the need for incremental goals, the need for tracking deliverables, and the need to accurately measure benefits are all directly applicable for the largest of projects.

Case 6 – “ILOVEYOU” virus -- system security in an interconnected world.

In Congressional Testimony on May 10, 2000, GAO²² testified on this system as follows:

ILOVEYOU is both a “virus” and “worm.” Worms propagate themselves through networks; viruses destroy files and replicate themselves by manipulating files. The damage resulting from this particular hybrid— which includes overwhelmed e-mail systems and lost files—is limited to users of the Microsoft Windows operating system.

ILOVEYOU typically comes in the form of an e-mail message from someone the recipient knows with an attachment called LOVE-LETTER-FOR-YOU.TXT.VBS. The attachment is a Visual Basic Script (VBS) file. As long as recipients do not run the attached file, their systems will not be affected and they need only to delete the e-mail and its attachment. When opened and allowed to run, however, ILOVEYOU attempts to:

- send copies of itself using Microsoft Outlook (an electronic mail software program) to all entries in all of the recipient’s address books,
- infect the Internet Relay Chat (IRC) program so that the next time a user starts “chatting” on the Internet, the worm can spread to everyone who connects to the chat server,
- search for picture, video, and music files and overwrite or replace them with a copy of itself, and
- install a password-stealing program that will become active when the recipient opens Internet Explorer and reboots the computer.

In short, ILOVEYOU looks a lot like Melissa in operation: it comes via e-mail; it attacks Microsoft’s Outlook; it’s a hybrid between a worm and a virus; and it does some damage—but it mostly excels at using the infected system to e-mail copies of itself to others. The one main difference is that it proliferated much faster than Melissa because it came during the work week, not the weekend. Moreover,

²² GAO Congressional Testimony GAO/T-AIMD-00-171, May 10, 2000.

ILOVEYOU sent itself to everyone on the recipient's e-mail lists, rather than just the first 50 addressees as Melissa did.

In fact, soon after initial reports of the worm/virus surfaced in Asia on May 4, ILOVEYOU spread rapidly throughout the rest of the world. By 6 pm the same day, Carnegie Mellon's CERT Coordination Center had received over 400 direct reports involving more than 420,000 Internet hosts. And by the next day, ILOVEYOU appeared in new guises, labeled as "Mother's Day," "Joke," "Very Funny," among others. At least 14 different variants of the virus had been identified by the weekend, according to DOD's Joint Task Force-Computer Network Defense. These variations re-triggered disruptions because they allowed the worm/virus to bypass filters set up earlier to block ILOVEYOU. At least one variant—with the subject header "VIRUS ALERT!!!"—was reportedly even more dangerous than the original because it was also able to overwrite system files critical to computing functions.

Reports from various media, government agencies, and computer security experts indicate that the impact of ILOVEYOU was extensive. The virus reportedly hit large corporations such as AT&T, TWA, and Ford Motor Company; media outlets such as the Washington Post and ABC news; international organizations such as the International Monetary Fund, the British Parliament, and Belgium's banking system; state governments; school systems; and credit unions, among many others, forcing them to take their networks off-line for hours.

The virus/worm also reportedly penetrated at least 14 federal agencies—including the Department of Defense (DOD), the Social Security Administration, the Central Intelligence Agency, the Immigration and Naturalization Service, the Department of Energy, the Department of Agriculture, the Department of Education, the National Aeronautics and Space Administration (NASA), along with the House and Senate. We still do not know the full effect of this virus on the agencies that were penetrated. While many were forced to shut down their e-mail networks for some time, many also reported that mission-critical systems and operations were not affected. Of course, if an agency's business depends on e-mail for decision-making and service delivery, then the virus/worm probably had a significant impact on day-to-day operations in terms of lost productivity.

After this incident, GAO highlighted six areas of management and general control problems in computer security:

- Poor security planning and management is the rule rather than the exception. Most agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of controls they rely on. These are fundamental activities that allow an organization to manage its information security risks cost-effectively rather than by reacting to individual problems ad hoc.

- Agencies often lack effective access controls to their computer resources (data, equipment, and facilities) and, as a result, are unable to protect these assets against unauthorized modification, loss, and disclosure. These controls would normally include physical protections such as gates and guards and logical controls, which are controls built into software that (1) require users to authenticate themselves through passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can take.
- Application software development and change controls are weak. For example, testing procedures are undisciplined and do not ensure that implemented software operates as intended, and access to software program libraries is inadequately controlled.
- Agencies lack effective policies and procedures governing the segregation of duties. It is commonly found that computer programmers and operators are authorized to perform a wide variety of duties, such as independently writing, testing, and approving program changes. This, in turn, provides them with the ability to independently modify, circumvent, and disable system security features.
- Reviews frequently identify systems with insufficiently restricted access to the powerful programs and sensitive files associated with the computer system's operation, e.g., operating systems, system utilities, security software, and database management system. Such free access makes it possible for knowledgeable individuals to disable or circumvent controls.
- Service continuity controls are incomplete and often not fully tested for ensuring that critical operations can continue when unexpected events (such as a temporary power failure, accidental loss of files, major disaster such as a fire, or malicious disruptions) occur.

This incident is a typical example of the emerging cross cutting issue of international cyber security. It is not related directly to the formulation, development, and management of a single IT project, but requires the focus of IT management at all levels to address the potential vulnerabilities across the entire world-wide electronic infrastructure. In that sense, it is very similar to the Y2K issue, and will have a large impact on the formulation and management of large IT projects during the next several years, as well as the retrofitting of the existing IT infrastructure. The lesson here is that we now must provide more focus on cyber security risk, vulnerabilities, and architecture in the design of IT projects. If we don't change, we can predict more spectacular failures due to these vulnerabilities in the future. Old IT project designs have new flaws.

F. Websites

Websites containing IT project management direction, policy and related documents:

Office of Management and Budget – www.whitehouse.gov/OMB/index.html

General Accounting Office – www.gao.gov

General Services Administration – www.gsa.gov

Chief Information Officers Council home page – www.cio.gov

General Services Administration listing of IT policy document – www.policyworks.gov/policydocs/policy_list.htm