



---

**\*The GSA IT Newsletter**

---

**U.S. GENERAL SERVICES ADMINISTRATION****INFORMATION TECHNOLOGY NEWSLETTER**

This newsletter is being provided as a service from the **GSA Office of Information Technology (MK)** of the **Office of Policy, Planning and Evaluation (M)**

**March 1996**

---

**Keys to Success for IT Pilot Projects Illustrated**

A new GSA publication, *Information Technology Pilot Projects: Keys to Success*, addresses the key factors that lead to the success of major information technology (IT) pilot projects. Pilot projects provide an effective method for ensuring the success of large and complex systems. The Federal government has the most complex computer systems in the world. Federal agencies spend billions of dollars each year to develop, implement, and maintain these systems. Proper up-front planning for these large and complex systems is often a key to their success. One of the best ways to support this planning and reduce risk is to develop a pilot project to test the proposed system on a smaller scale before major implementation begins.

Nine key principles are described that aid in determining if a pilot project will be successful: (1) heavy user involvement; (2) early identification of training issues; (3) adhering to the schedule; (4) anticipating time required for uncontrollable problems; (5) developing appropriate evaluation criteria; (6) thoroughly testing the system; (7) starting small and building on successes; (8) choosing the correct contract vehicle; and, (9) managing end-user expectations. The publication also provides in-depth coverage of pilot systems at the FBI, DOD, and IRS by way of case studies.

This publication is available in electronic form via the FedWorld bulletin board system in the "GSA, Information Technology Service, Library of Files" section. Login to FedWorld (703-321-3339) and at the main menu type F. (Note: Press the "enter" key after each letter selected.) At the next two successive menus type B and F respectively. Choose F at the next menu selection and then select F once again to see a listing of file names available for downloading. Scroll to the PILOTRPT file name and press "enter" over the version that best fits your application format (i.e., doc, wp, or txt). Follow the on-screen

instructions to download the selected file. The FedWorld Help Desk can be reached at 703-487-4608 if you need assistance. We are also planning to add this document to our Internet home page in the near future (<http://www.itpolicy.gsa.gov>).

To improve the chances of success, agencies should keep the key principles discussed in this document in mind during the planning and implementation of a pilot project, and adopt them where appropriate. If you have any questions on this subject, please contact Robert Karr in the Strategic IT Analysis Division at 202-219-6630 or via Internet: [robert.karr@gsa.gov](mailto:robert.karr@gsa.gov).

## **DOS IRM Initiatives Save \$\$**

Who said the Government isn't as efficient as private industry? Two years ago, the Department of State's (DOS) Office of Information Management initiated a domestic pilot program to perform its own maintenance of automated data processing equipment. Two goals were established, to provide quality service at less cost and to reduce the Department's dependency on a single service provider.

Within the first month, the word had spread: "Quality service at half the cost!" Soon, 10 bureaus wanted to join the program. Those bureaus saved over \$1.5 million the first year. The program has since expanded to cover 19 bureaus, with a projected saving of \$3.2 million in this fiscal year. The program provides services to approximately 75% of the Department's office automation/automated data processing equipment.

How has this been accomplished? Using Government personnel to supervise and oversee, and a small amount of money for infrastructure, a service unit was established to compete with private industry. An inventory of spare parts allows the unit technicians quick access to replacements. Much of this inventory was obtained through an excessing operation. Two technicians routinely solicit excess equipment. This equipment is tested and either placed in the inventory as a whole unit or broken down into parts. Almost \$2 million worth of spare parts and inventory have been accumulated. In addition, partnerships were established with local suppliers; parts are therefore only a telephone call and carrier ride away.

As equipment fails, system managers call or fax the Call Management Center. Their service requests are quickly entered into an automated call-tracking system, and a technician is notified. Currently there are 11 technicians on contract from various companies. While all service requests are important, "system down" calls receive the highest priority. Once notified, a technician contacts the system manager to determine the nature of the problem, and to provide telephone assistance and/or an expected arrival time. Once on site, the technician diagnoses the problem and repairs the failed device. Customers are billed to recover the cost of labor and parts. Customers under this maintenance program receive a level of service equal to or higher than what they had received under vendors' premium on-call maintenance contracts. Customers generally save over 50% under the program. Bureaus that pro-actively diagnose and resolve some problems on their own have saved as much as 70%.

The repair unit is not allowed to make any money, nor is it allowed to lose any money. The only

stipulation is that customers of the unit must use their savings to migrate to newer open-systems technologies.

For those customers who want to save even more money, DOS has established a walk-in exchange center. Customers can call ahead to arrange for exchange of customer-replaceable items. Customers exchange their failed keyboards, monitors, removable disk drives and other repairable items themselves. As budget dollars become fewer and more personal computers are installed, many users are becoming increasingly interested in performing their own repairs and upgrades. DOS has purchased video training tapes which teach customers how to repair and upgrade their own computers.

The program is changing the way DOS does business. The biggest challenge has been overcoming resistance to change. A bureau may join the program simply by calling the Management Center and requesting a briefing. Someone from the Center will review the bureau's current maintenance expenditures, providing a briefing, prepare a memorandum of understanding and estimate the cost of maintenance under the program.

As to expanding the program to serve overseas posts, DOS intends to provide telephone support and a mail-in exchange service for desk-top products, i.e., workstations, personal computers and desk-top printers. The Department does not have plans at present to provide software support, but it would consider this if enough customers request it.

In these times of shrinking budgets why hasn't the Department mandated that everyone come under this program? That has never been an objective. Frankly, competition is invited. The program provides quality service at an affordable cost. If another organization can come in and provide the same or better quality of service for less, then so be it!

A second IRM initiative involves software--anti-virus software specifically. DOS has negotiated a two-year contract for a worldwide site license for Norton Anti-Virus (NAV) software; effective September 30, 1995. The contract permits the NAV software and associated documentation to be reproduced and installed on all DOS computer resources (standalone, LAN's and networks) worldwide. In addition, the contract authorizes NAV software to be used by all DOS employees and all other government agencies and contractors engaged in the performance of work for the DOS or utilizing its systems at domestic and overseas locations.

From a management perspective, this contract provides the Department with an excellent opportunity to eliminate the duplication of anti-virus software products, standardize the type of anti-virus software that will be supported by the Department worldwide, eliminates tracking of multiple site license agreements and protects the user community from possible copyright infringements, and provides the cost free anti-virus software definition file updates from the Symantic Bulletin Board System (BBS) to all domestic and overseas users on a quarterly basis.

The Department expects to install the Norton Anti-Virus (NAV) software products on approximately

31,000 computer systems State-wide.

## **SSA Tackles Year 2000**

In only a few short years, we will reach the year 2000. This seemingly innocuous turn of events has great ramifications for computer systems worldwide. The Social Security Administration (SSA), which has hundreds of applications using thousands of dates, is on the cutting edge in tackling the problem.

Generally, applications use two digits to represent a year in a date field. SSA has approximately 25 million lines of code in production, with 25 million more in development. A programmer must look at every line and decide whether it must be changed for the Year 2000. No automated way exists to do this. Since naming standards don't exist for date fields, they can be called anything.

SSA began addressing the problem years ago. Masterfile and database date representation were addressed first. SSA decided to use relative dates to represent these dates. This effort, which lasted 4 years, concluded in 1995.

The next step was to search the marketplace, looking for an automated way to make the source code changes. Year 2000 tools fall into two categories, the first of which changes the system date for a particular program, which shows how that program will react when confronted with a date after 12/31/99. The second category contains products that identify date fields in code, tracing the flow of dates through a system as they move from field to field. SSA began a procurement for a tool from the second category in August, 1994, with an award in July, 1995.

The source code management package, ENDEVOR (Environment for Development and Operations, is the sole repository of SSA's source code. The new tool and the scan capabilities of ENDEVOR, allow the agency to focus on those areas in the code that are most likely to contain date fields. None of these tools do away with the necessity of examining every line of code, but they make that process quicker and easier.

The Year 2000 project team conducted meetings throughout the systems organization to raise the awareness level. Two representative systems were selected as pilots, with all time used to modify them for date changes logged. By extrapolating these results, the team determined that several hundred work years would be needed to make, validate and implement the coding changes. An overall schedule is under development.

All DP installations face the issue of missing source code. Those load modules that have no corresponding source code must be "disassembled" and examined to see if they contain code which operates on dates. The first step is to identify programs with missing source code. Even this effort is painstaking and time consuming. If any are found, the next step is to recreate these programs to determine if any changes are needed to handle century processing.

SSA's on-line systems contain two digit screen dates. To increase the representation to four digit dates would involve overflowing to a second screen and changing all the path logic. Consequently, SSA decided to continue showing two digit years on screens except for dates, such as date of birth, where a century could not be determined through the application of an algorithm.

The passing of data from one program to another, one system to another, and from one agency to another is one of the factors which gives the Year 2000 such complexity. Timing considerations become important because the sender or receiver must convert files from one format to another unless both are ready to make Year 2000 changes simultaneously. SSA is contacting all agencies with whom it exchanges data to begin planning these changes.

Forms were also addressed. Most current forms have a 19\_\_ representation of date fields. These must be changed to handle Year 2000 dates.

All vendors who provide SSA with software, whether in the LAN or mainframe arena, will be contacted to determine which release of their software will handle the Year 2000 correctly.

For more information on SSA's Year 2000 effort, contact Judith Draper at 410-965-5314.

## **OIS Offers Technology Training Courses**

GSA's Office of Information Security (OIS) Center for Security and Technology Training is partnering with commercial organizations to present courses on new and emerging information technologies. The courses are targeted to the needs of the government audience, with a substantial tuition reduction for government or government contractor personnel. The classes represent a quick but intensive look at the latest in information technology and include hands-on and lecture type presentations. Scheduled course locations include Washington, DC, San Francisco, CA., and Kansas City, MO., with the option for presentation at any customer location.

The Phase One training classes will be presented by Telecommunications Research Associates (TRA), which has extensive experience in presenting an emerging technology curriculum. Classes will be held at the GSA Regional Office Building, 7th and D Streets, SW, Washington, DC, conveniently located on the L'Enfant Plaza Metro Line. Tuition for each of these 2 day courses is \$660.00.

March 28-29 Understanding Emerging Technology

April 2-3 Understanding ATM

April 9-10 Understanding Local Area Network Implementation

April 30-May 1 Understanding SONET and Other Broadband Technologies

## May 14-15 Understanding ATM Applications and Implementations

For more information or for enrollment call the CSTT at 816-926-6921 or E-mail [ois.registrar@gsa.gov](mailto:ois.registrar@gsa.gov). For general information on the Office of Information Security or the training center you may also visit the GSA Web site at <http://www.gsa.gov> and access "Security" or "Training".

Technology training is just one in a long list of available OIS services. These worldwide information security services supporting classified and sensitive applications include:

ISSO/NSO - Information System/Network Security Officers

Security and Accreditation Plans - Risk Analysis

Network Management - System Administration

Project Management - System Engineering

Procurements supported by existing IDIQ contracts

Restoration/Installation/Cabling/COMSEC support

Depot Services/Integration & Fielding support

For additional information on OIS services in addition to training, please contact: 202-708-5060 or DSN 325-2658 or E-mail [infosec.service@gsa.gov](mailto:infosec.service@gsa.gov).

## **GSA Publishes Large Distributed Systems Guide**

GSA has issued its thirteenth publication in the Acquisition Guide Series, A Guide for Acquiring and Managing Large Distributed Systems. This Guide provides government program, information resources management, and contracting officials with an introduction to the issues involved when they acquire, implement, and operate a large distributed system. It addresses systems that use distributed processing, data, logical subsystems, organizational control, or acquisition vehicles.

Although large distributed systems use many of the same information technology resources as other systems, their size, scope, and distributed nature present special challenges. This guide addresses these challenges and provides information, advice, and techniques to help agencies realize the full benefits of such systems. Topics include: organizational issues; capacity planning and management; performance and capability validation; and operation, network management, and user support.

Interested readers can obtain copies of the guide from the National Technical Information Service (NTIS) at 703-487-4099. Use code 420 for the information technology list. Use code 354 to receive a price code conversion table and order form. An electronic copy of A Guide for Acquiring and Managing Large Distributed Systems can be downloaded from the GSA-ITS Library of Files at FEDWORLD.

## **GSA Develops BPR Tool**

GSA's Information Technology Management Division has developed a Business Process Reengineering (BPR) tool to help agencies evaluate their readiness to undertake BPR projects. Experts from government and the private sector will validate the tool over the next two months.

As a part of the validation process, the tool was presented to a group of 200 IT industry executives at a recent briefing. The executives supported the assertions on which the tool is based.

Agencies are under tremendous pressure to improve their business processes in response to laws such as the Government Performance Results Act of 1993, and initiatives such as the Contract with America. Consequently, they rush into reengineering without adequate preparation, resulting in far smaller returns on investment than anticipated, as well as outright failures. Providing BPR guidance at the earliest possible stage will allow agencies to focus on the priority issues that need to be addressed before investing in reengineering. This will increase the agencies' chances of successfully implementing BPR.

As a service to the Federal community, GSA plans to provide assistance to agencies conducting pilots using the BPR assessment tool. This will help organizations determine whether the conditions necessary to succeed at reengineering are in place. For more information contact Jim Sheeran at 202-501-4230, or via E-Mail at [jim.sheeran@gsa.gov](mailto:jim.sheeran@gsa.gov).

---

**Posted 3/21/96**