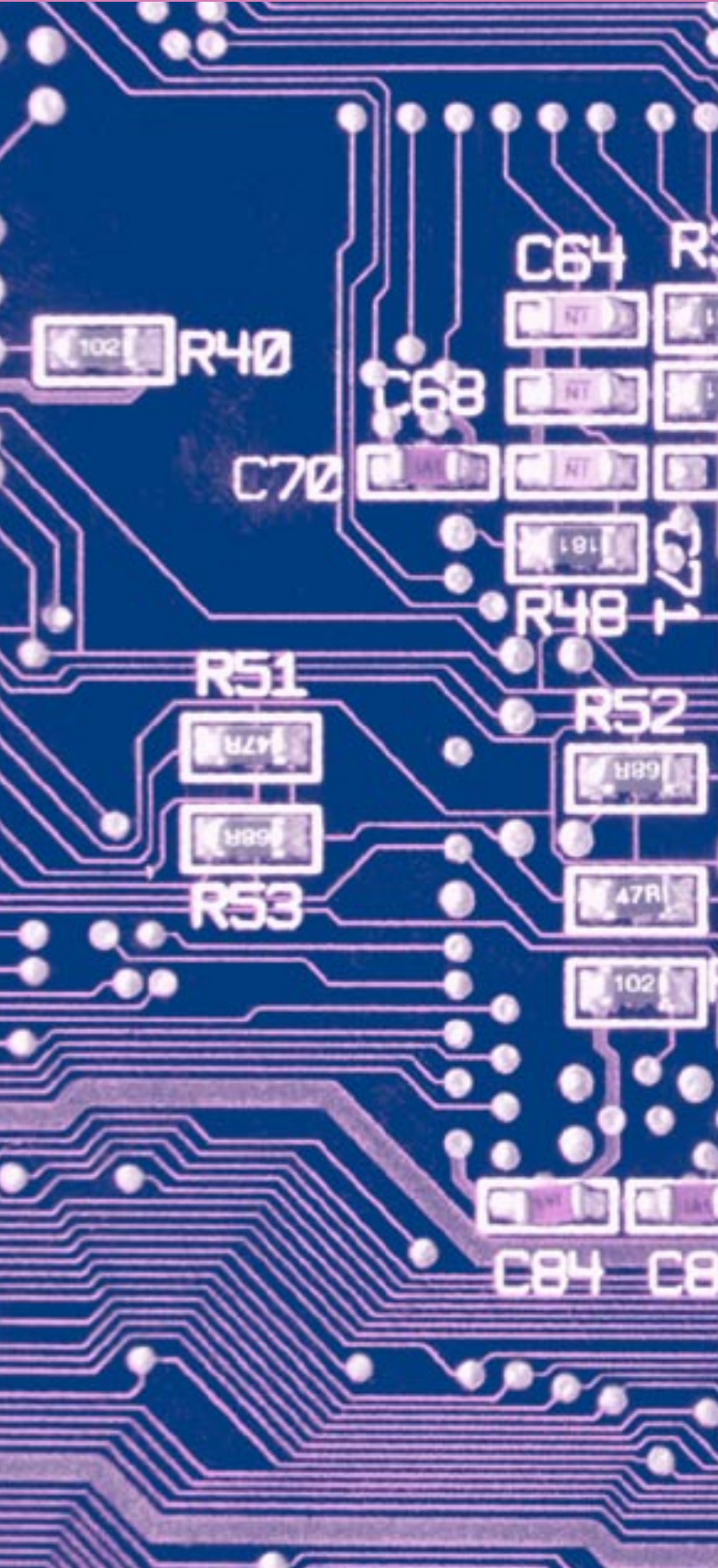


The Journal of

# Public Inquiry

A Publication of the Inspectors General of the United States

Spring/Summer 1999



## EDITORIAL BOARD

**Aletha L. Brown**, Equal Employment Opportunity Commission, Office of the Inspector General (OIG)

**Raymond J. DeCarli**, Department of Transportation OIG

**Stuart C. Gilman**, Office of Government Ethics

**Maryann Grodin**, Nuclear Regulatory Commission OIG

**Donald Mancuso**, Department of Defense OIG

**Thomas D. Roslewicz**, Department of Health and Human Services OIG

**Kelly A. Sisario**, National Archives and Records Administration OIG

**Robert S. Terjesen**, Department of State OIG

**David C. Williams**, Department of Treasury OIG

**Sue Murrin**, Office of Management and Budget

## STAFF

### *Editor*

**David C. Williams**, Department of Treasury OIG

### *Editorial Services*

**Agapi Doulaveris**, Department of Treasury OIG

### *Printing*

**Department of Defense OIG**

**Department of Treasury OIG**

### *Public Affairs*

**Robert S. Terjesen**, Department of State OIG

### *Design & Layout*

**Gaston L. Gianni, Jr. & Sharon C. Tushin**, Federal Deposit Insurance Corporation OIG

## INVITATION TO CONTRIBUTE ARTICLES

*The Journal of Public Inquiry* is a publication of the Inspectors General of the United States. We are soliciting articles from participating professionals and scholars on topics important to the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. Articles should be approximately 3–5 pages, single-spaced, and should be submitted to Agapi Doulaveris, Office of the Inspector General, Department of Treasury, 740 15th Street N.W., Suite 510, Washington, D.C., 20220.

Please note that the journal reserves the right to edit submissions. The journal is a publication of the United States Government. As such, *The Journal of Public Inquiry* is not copyrighted and may be reprinted without permission.

## NOTICE

The opinions expressed in *The Journal of Public Inquiry* are the author's alone. They do not represent the opinions or policies of the United States or any Department or Agency of the United States Government.

The Journal of

# Public Inquiry

A Publication of the Inspectors General of the United States

Spring/Summer 1999

## TABLE OF CONTENTS

### What CIOs Do 1

*Don't Start the Information Revolution Without Me*  
**Kathryn Truex**

### Friendly Fire 5

*Systems Penetration Auditing*  
**Paul Connelly**

### Curb Your Y2K 9

*Cleaning Up after 1/1/2000*  
**Robert Lieberman**

### SCERS for Curs 13

*The Seized Computer Evidence Recovery Specialist Training Program*  
**Carlton Fitzpatrick and Lisa Schaffer**

### The Empire Strikes Back! 17

*Building a New Partnership Across the Federal Government:  
The National Infrastructure Protection Center*  
**Michael Vatis**

### Be Kind to Your Webfooted Friends 21

*E-FOIA Law Increases Access for the Public and  
Brings Changes to Agencies*  
**Joaquin Ferrao**

### Bright IDs 25

*Assurance Services in Electronic Commerce*  
**Jay Ahuja**

### Arresting Ideas 29

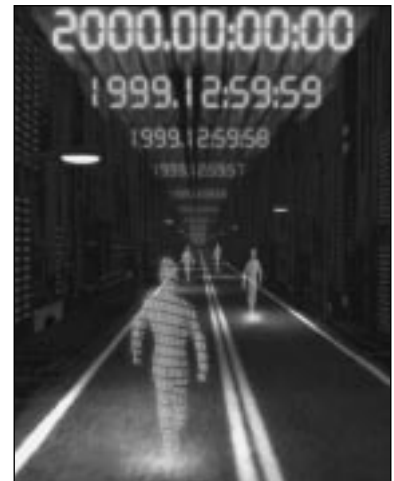
*Securing Computers*  
**Andrew Fried**

### Building the Soul of a New Machine 35

*Auditing Software Development*  
**John W. Lainhart, IV**



pg. 5



pg. 9



pg. 49



pg. 49

**The New de-Tech-tives 39**

*The Social Security Administration Office of the Inspector General's Experience*

**Jack Lewis**

**Moving into the Next Millennium 43**

*System Auditing Capability Development for Internal Auditing*

**Gary R. Austin**

**Message Message 49**

*Ensuring Your Semiannual Message Doesn't Fall on Deaf Ears*

**Brian A. Dettelbach**

**Got Any Change? 53**

*Change is Difficult for Everyone. Here are Four Good Ways that the State Department's Office of Inspector General was Able to Accomplish it*

**James K. Blubaugh**

**Rethinking Leadership 57**

**Warren Bennis** (*Reprinted with Permission*)

**Who Reads the Journal of Public Inquiry?? 61**

*Lots of People!!*

**Kelly A. Sisario**



pg. 56

# What CIOs Do

## *Don't Start the Information Revolution Without Me*

**O**n October 12, 1994, then Senator William S. Cohen of Maine issued an investigative report entitled “Computer Chaos: Billions Wasted Buying Federal Computer Systems”. That report has led to a period of dramatic change in how the federal government acquires and utilizes information technology (IT). Guiding that change has been the Chief Information Officers (CIO) Council.

The Paperwork Reduction Act (PRA) of 1995 and the Information Technology Management Reform Act (ITMRA) of 1996 provided the legislative framework for restructuring the federal approach. ITMRA—officially renamed the Clinger-Cohen Act in honor of its sponsors took effect in August 1996 and quickly changed the perception of federal information technology. It was no longer viewed as just a technical issue, but a major management issue. The Act mandated that agencies replace information resource managers with chief information officers. These individuals would be highly experienced professionals who possess a combination of technical, financial, communication, and managerial skills. Executive Order 13011, Federal Information Technology, established the CIO Council as a government-wide body that addresses critical cross-cutting IT issues. The Council is comprised of the CIOs and Deputy CIOs of the 28 largest Federal agencies as well as senior officials from OMB and the National Archives and Records Administration. The Vice Chair of the PCIE serves as an ex officio member of the Council.

The Council moved quickly to organize its work. Under the leadership of the Deputy Director of the Office of Management and Budget, who serves as the CIO Council Chair, the first Strategic Planning Retreat was held in October 1996. Working Groups were established and an aggressive plan of action adopted. By February 1997, a six month progress report had been published and a CIO Council Charter approved. The Charter established the Purpose of the Council to:

- Develop recommendations for overall federal information technology management policy, procedures, and standards.
- Share experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources.
- Identify opportunities, make recommendations for, and sponsor cooperation in using information resources.

- Assess and address the hiring, training, classification, and professional development needs of the Federal Government with respect to information resources management.
- Make recommendations and provide advice to appropriate executive agencies and organizations, including advice to OMB on the government-wide strategic plan required by the Paperwork Reduction Act; and seek the views of the Chief Financial Officers Council, the Government Information Technology Services Board, the Information Technology Resources Board, Federal Procurement Council, industry, academia, and Federal, Tribal, and State and local governments on matters of concern to the Council as appropriate.

The CIO Council vision is to be a resource which will help the Government work better and cost less by promoting the efficient and effective use of agency information resources. The CIO Council supports business process reengineering, continuous process improvement, and measurable increases in employee productivity in the performance of work related to the achievement of agency objectives.

To quickly disseminate information regarding its activities, the Council established a presence on the internet at <http://www.cio.gov>. Supported by staff of the General Services Administration (GSA), this web site provides a means for rapid communication amongst members of the Council, as well as a forum to make information readily available government-wide and to the public at large. Major policy documents pertinent to or sponsored by the Council are posted on the site in their entirety, as are publications of interest to the government managerial and IT communities. The site is updated regularly, and features links to other government and IT industry sites of interest.

One issue identified at the October 1996 planning retreat as a key impediment to the work of the Council was the widespread impression of “a federal landscape littered with the remains of failed IT initiatives”. As stated in the preface to the publication, “Best IT Practices in the Federal Government”, the accretion of obituaries of “runaway systems” contributes to an impression that:

- (a) The American public and the Congress get little in return for the billions of dollars invested each year in IT in the Federal Government.
- (b) Most Federal systems projects are at risk and examples of fraud, abuse, waste and mismanagement.
- (c) Most Federal IT managers couldn’t run a roadside watermelon stand if you spotted them the watermelons and had the highway patrol flag down the cars.
- (d) All of the above.

Regrettably, the Federal Government does not have a sterling record in delivering quality IT solutions within acceptable cost and schedule. Going forward, however, suc-

cesses as well as failures must be examined if a climate of optimism and progress is to be fostered. The CIO Council utilized one of its partnerships with non-governmental entities for this purpose.

The Industry Advisory Council (IAC) is a nonprofit industry association of IT companies that has regularly assisted the Council since its earliest days. In December 1996, IAC created a Task Force made up of 39 volunteer IT professionals drawn from 26 member companies. The Task Force, working under the guidance of the CIO Council Outreach Committee, compiled and documented representative case studies that demonstrated the successful application of IT in Federal departments and agencies. The results were published in the October 1997 document, “Best

IT Practices in the Federal Government”, which is available for downloading from the CIO Council web site.

The Council published its first Strategic Plan in January 1998. The priorities forming the foundation for this plan were:

- define an interoperable Federal information architecture;
- ensure security practices that protect government services;
- lead the Federal Year 2000 conversion effort;
- establish sound capital planning and investment practices;
- improve the IT skills of the Federal workforce; and



- build relationships through outreach programs with Federal organizations, industry, Congress, and the public.

The Council's goal through these priorities is to support, in partnership with State and local governments, industry, and academia, a Government that utilizes IT in an increasingly responsive manner to the needs of its managers and customers. Six committees have been established to further these goals and each has been able to report significant accomplishments of its own in the brief time of its existence. The second Strategic Plan, prepared jointly by the CIO Council and OMB, was submitted to Congress in response to the requirement of the Paperwork Reduction Act that the Director of OMB annually submit a government-wide strategic plan for information resources management. That plan details the numerous achievements of the CIO Council and its committees, as well as its goals for the next five years. It is clear that Federal IT management has

changed dramatically, and that this change is just the beginning of the revolution.

Over the long term, the success of the CIO community is most likely to be judged by its success in improving the previously lamentable record concerning Federal IT system projects, as well as achieving government-wide increases in efficiency through common system architecture, interoperability and standardization. In the shorter term, it has been confronted in its formative years with two huge challenges: the Millenium Bug and the vulnerability of Federal IT systems to hackers, cyberfraud, and information warfare. This may prove to be as tough as playing the last Super Bowl champion and the runner-up in the first two games of a football season. Regardless of how well those challenges are handled, the combination of strong statutory underpinning and the ever increasing reliance of all government agencies on IT have permanently moved every CIO out of the computer room and into the board room. 🏢





---

PAUL CONNELLY

*PricewaterhouseCoopers*

# Friendly Fire

## *Systems Penetration Auditing*

Recent surveys indicate that most businesses and government organizations are experiencing an increasing number of computer security incidents. More than 37 percent of the 1600 Security and IT professionals surveyed in the 1998 “Information Week”/PricewaterhouseCoopers Global Information Security Survey said their organizations lost more than \$10,000 in such breaches, and more than 16 percent had lost more than \$100,000. The sources of the security breaches? Authorized users, outside hackers, former employees, contract workers, suppliers, and competitors.

The task of protecting the information assets of any organization is vast and complex. The threats come from insiders and outsiders, and vulnerabilities can be found in dial-in lines, Internet links, applications, operating systems—virtually anywhere on the network. Unauthorized outsider and insider access to an organization’s networks and systems can result in theft, modification, and destruction of data; denial of service; fraud; disclosure of sensitive data; misuse of resources; and legal liability stemming from use of organizational resources as a launching point for attacks against outside systems. System down time and re-creation, as well as embarrassment and loss of credibility and confidence can have severe impacts as well. Clearly, the threat is real and the damage can be severe.

Adding to the severity of the issues is the trend toward greater sharing of information via the Internet, virtual private networks, extranets, intranets, and e-commerce. This push is increasing and diversifying the number of system users who are given insider access, as well as the range of potential technical vulnerabilities. Security solutions such as firewalls, network scanners, and intrusion detection systems are equally diverse. How can an organization assess whether its IT security countermeasures are effective in preventing compromises? One answer is penetration testing.

Sometimes referred to as “ethical” or “white-hat” hacking, penetration testing is the use of hacker tools and techniques and other security testing tools within a methodical framework to provide a “real-life” test of systems for vulnerabilities. It is “good guy” testing for security holes before the “bad guys” find them, using many of the same tools and techniques.

Penetration testing can counter threats by identifying technical vulnerabilities in networks and specific systems as well as weaknesses in security policies, standards, and procedures. When properly scoped and executed, penetration testing can also be used to assess user security awareness and compliance with security policies and guidelines; and evaluate the effectiveness of monitoring, intrusion detection, and incident response procedures.

## Why conduct penetration testing?

There are five key benefits to be gained:

1. Penetration testing offers a real-life assessment of vulnerabilities. Vulnerabilities lose the “potential” label when the testing can actually exploits them. The testing finds vulnerabilities, demonstrates how they are exploited, and illustrates the results.
2. Penetration testing ties directly to the threats. A well-designed test by a competent penetration team will encompass many of the same techniques and tools hackers use, in a more methodical and comprehensive manner. One message implicit in the results is—if the penetration team was able to break in, so can unauthorized and potentially malicious outsiders and insiders.
3. Penetration testing can provide an independent verification and validation of security countermeasures. Is the Internet firewall working properly? Are the organization’s intrusion detection and incident response procedures effective? Are users following organizational policies? A well-conceived and executed penetration test will find these answers.
4. Penetration testing can be used to help champion security in the organization. A security review or audit of a remote access system may point out significant vulnerabilities, but not receive priority attention. A penetration test that actually exploits those vulnerabilities, and gains Administrator access rights to company financial systems, production systems, e-mail, Human Resources records, or other sensitive systems is going to make users and management sit up and take notice. Penetration test results help win greater management emphasis and resources for security programs.



5. Penetration testing is recognized as a valuable component of IT auditing. The Federal Information Systems Controls Audit Manual (FISCAM) published by the US General Accounting Office prescribes outsider and insider penetration testing as mandatory components of financial audits. Price-waterhouseCoopers has been employing penetration testing as an audit technique since before the start of the decade, and most of the other Big Five and many other public accounting firms offer the service as well. The use of hacker tools and penetration

techniques within the framework of IT auditing creates a hybrid methodology that utilizes the often highly creative Hacker techniques for testing, but in a detailed and methodical manner.

### Hacking 101

The vulnerabilities exploited by Hackers which are found again and again by our teams include lack of appropriate security technology, failure to delete default accounts, lack of control over remote access points, poor passwords, outdated software versions, unnecessary services, unlimited login failures, excessive trust relationships, lack of security awareness among employees, lack of security policy and guidelines, and poor or non-existent detection and response. These vulnerabilities are preyed upon by Hackers, but are detected and highlighted through penetration testing.

A comprehensive penetration testing plan will have several components—out-

sider testing via the Internet, outsider testing via dial-in lines, insider testing at various levels, physical walk-arounds, and social engineering.

Outsider testing via the Internet consists of performing a comprehensive footprint analysis identifying the organization’s Internet connectivity and topology, conducting an exhaustive search for vulnerabilities on devices identified in the footprint, and attempting to exploit vulnerabilities to gain unauthorized access to internal network systems, firewall systems, and Internet servers. Firewalls, Web servers,

mail servers, and other key targets are focal points of the testing.

Outsider testing via dial-in involves the use of Hacker war-dialing software to dial telephone extensions at the target facility to identify modems. Each modem identified is then attacked, trying different communications software and parameters to find the right match to enable a connection. If a connection is made, and no password is required for access, the system is ready for further penetration. If a password is required, common defaults are attempted, and password guessing scripts which attempt every word in the dictionary and as well as various word combinations can be run. Other techniques can be used to bypass login controls or download data from the terminal that may assist in gaining internal network access.

Insider penetration testing looks at security controls internal to the network or system. Insider testing starts with physical access to a network port. By simply plugging into the network, without an account, can an individual obtain network access? Can a “sniffer” record other users’ IDs and passwords? How far can the access lead? The next step is to start with a low-level user account, and see how far the access can be extended. In many tests, a third level of testing is also included—logging on as a systems administrator or programmer, to see how far those high-level rights can be extended. Insider testing is often left out of penetration projects because organizations feel they can trust their employees, and want to reduce the cost of the testing. This is a mistake. The fact is a majority of computer security breaches come from inside the organization, and insiders can do much more damage because they know the system and key data better than outsiders do. Strong internal network security controls also add additional layers to defenses against exploitation by outsiders. Insider testing makes business sense and is a key part of a comprehensive security audit.

Physical walk-throughs and social engineering can be included in penetration testing to round out the vulnerability picture. Physical walk-throughs typically involve after-hours checks of work areas to see if active terminal sessions are left on, passwords are written down in terminal areas, or other sensitive information is available to anyone with physical access to the area. “Social Engineering” is the term given to the use of social skills to “charm” individuals into giving out passwords or other key data that can be used to gain system access. The results of these tests reflect user awareness of threats and compliance with policies regarding protection of passwords. To conduct Social Engineering, a sample of users, systems administrators, and help desk personnel is selected, and each person is contacted using a rehearsed story (e.g., “I lost my password”) to see if account information can be obtained. These steps are typically segregated from the technical testing to ensure technical vulnerabilities are fully tested without information gained by non-technical means.

Notwithstanding the benefits it offers, penetration testing can adversely impact the organization being tested if not carried out in a controlled manner. Ground rules should be set in advance to cover key issues. My firm typically seeks to work together with a “trusted agent” or small oversight committee from the organization to be tested, to ensure there are no negative impacts on normal business processes. Some of the ground rules we normally set include:

- Advance knowledge of the testing will be limited to a few key individuals to enhance the realism of the test and the ability to observe normal monitoring and response.
- If a critical vulnerability is found, the proper people will be notified immediately to take corrective action.
- No data will be modified or deleted.
- Individuals within the organization who are selected for Social Engineering testing are protected against retribution.
- No denial of service attacks will be employed. Vulnerabilities to denial of service will be identified without exploitation.

When considering penetration testing for your organization, a number of Do’s and Don’ts should be kept in mind:

- DO establish ground rules, specific objectives, and appropriate oversight for your testing to ensure proper controls and results.
- DO utilize outside expertise when needed to augment your skills. Penetration testing is not for novices. It can be damaging when improperly executed.
- DO demand broad and detailed technical expertise from any outside consulting outfit brought in to do your testing. The testers should not just be able to identify vulnerabilities, but also identify appropriate corrective actions and have the technical knowledge to implement any action they recommend.
- DO look for sharing of expertise if you utilize outside consultants. Include a member of your organization on the consultant’s team, to gain first-hand knowledge of how the vulnerabilities are found and exploited. The knowledge gained will prove very useful in implementing corrective actions, and develops in-house skills.
- DON’T use penetration testing techniques and hacker tools unless you fully understand their impacts. They can destroy data, shut down systems, and cause significant damage if not used properly by technically competent individuals.
- DON’T stop short of a comprehensive test. Failure to test from both insider and outsider perspectives,

or use of automated tools only, addresses only part of the vulnerability and threat equation, and can give a false sense of security. Get the whole picture.

- DON'T contract with former Hackers to conduct your testing. Some firms, even other "Big Five" accounting firms, tout the fact that famous ex-Hackers work on their teams. The sensitivity of penetration testing mandates complete trustworthiness as

well as technical competence. Do you want to trust someone who was once part of the black hats' team?

When properly planned and executed, penetration testing is a valuable and effective tool for auditing IT controls and identifying vulnerabilities. It ties directly to threats and commands attention of management and users alike. Put "good guys" to work testing your organization's network before the "bad guys" ride into town. 🚒

---

ROBERT LIEBERMAN

*Office of Inspector General, Department of Defense*

# Curb Your Y2K

## *Cleaning Up After 1/1/2000*



Robert Lieberman

A funny thing happened on the way to the 21<sup>st</sup> century. As governments, businesses and individuals throughout the world opted into the information age and electronic processing became a virtually indispensable aspect of modern life, a very simple habit of programmers was systematically building a fatal flaw into many million lines of code.

Starting in the earliest days of computing, when storage capacity was rudimentary by today's standards, programmers saved space by using two digits to represent years. It was widely recognized among the technicians that the year 2000 (Y2K) would be indistinguishable from 1900 and, as a result, systems and devices using dates to calculate, compare or sort information could eventually fail. In fact, problems in processing post-1999 dates began appearing in applications like demographic forecasting and other long term analyses as early as the 1980's.

A limited number of organizations, the Social Security Administration among them, reacted to the warning signs and began remedial action before the crisis was immanent. In general, however, both users and producers greeted the problem with what can best be termed relentless apathy. Conventional wisdom held that the combination of replacing most older systems and developing cheap, simple technical tools to fix the problem with a few patches on the remaining legacy systems would take care of it. As late as mid-1998, there were numerous reports that up to 70 percent of governments and businesses in the world either had not heard the increasingly explicit warnings ("Iceberg dead ahead!") or ignored them ("It'll melt."). Even those governments who became most engaged with the problem—probably the United Kingdom, Canada and the United States, in that order—conceded they were at least a couple years late in devoting their full attention to it.

The U.S. Federal Government's Y2K awareness developed slowly during 1995-96, as the Office of Management and Budget (OMB), General Accounting Office (GAO), and newly appointed chief information officers struggled to push the problem to center stage and convince managers that it is a potential show stopper for an enormously wide range of programs and services. Not only does continuity of government operations and services have to be maintained, but public confidence in banks, utilities, stock markets, emergency services, pharmacies, and even the suppliers and retailers of food must be ensured. In all but the most underdeveloped countries where reliance on information technology is minimal, if institutions or the public overreact and behavior such as hoarding supplies or converting investments into cash become commonplace, business failures, economic dislocation and perhaps even civil disturbances are not out of the question.

In May 1997, OMB imposed a quarterly reporting requirement to track the progress of over 7,000 mission-critical Federal systems through a series of prescribed conversion

phases. The Treasury-Postal Appropriation Act for FY 1998 mandated that OMB share those reports with the Congress. Increasingly telling Congressional criticism of the limited progress portrayed quarterly, plus growing media coverage, created pressure to accelerate Y2K remediation. The Federal Aviation Administration took the most public hits, although the Government as a whole earned an "F" on the widely publicized report cards issued by Chairman Stephen Horn's House Subcommittee on Government Management, Information Technology. In February 1998, Executive Order 13073 created the President's Council on Year 2000 Conversion, chaired by John Koskinen, former OMB Deputy Director for Management. The Executive Order directed agency heads to:

1. Assure that no critical Federal program experiences disruption because of the Y2K problem.
2. Assist and cooperate with State, local, and tribal governments to address the Y2K problem where those governments depend on Federal information or information technology or the Federal Government is dependent on those governments to perform critical missions.
3. Cooperate with the private sector operators of critical national and local systems, including the banking and financial system, the telecommunications systems, the public health system, the transportation system, and the electric power generation system, in addressing the Y2K problem.
4. Communicate with their foreign counterparts to raise awareness and generate cooperative international agreements to address the Y2K problem.

The Department of Defense offers an interesting case study of the challenges inherent in the Executive Order's formidable taskings. In January 2000, the Department needs to make 9 million active payroll and retiree payments; pay 2 million commercial vouchers; treat thousands of patients in military hospitals; continue operating in dangerous areas like the Iraqi no-fly zone, Bosnia and the Korean DMZ; maintain full control over the strategic nuclear forces; and be prepared to react immediately to terrorism or other contingencies. The threat of hostile attacks on US or allied country assets and citizens may be

especially acute at the turn of the century. Terrorism is often timed to coincide with significant dates. In this instance, this momentous calendar date may well coincide with a variety of disruptions that could magnify the impact of terrorist action and make it harder to deter or respond to it.

Defense has been in the forefront of world computer science and technology since the 1940's. Military interest drove advances in web technology, microelectronics and advanced simulation. Unfortunately, the keen interest in applying computers to Defense functions was not accompanied by equal determination to require standardized data elements, common or at least inter-operable systems, well

documented software and accurately mapped system interfaces. As a result, Defense has to deal with Y2K risk in an incredible array of systems—roughly 3,000 mission critical and 27,000 other systems—and untold numbers of devices containing processors of some type. External data exchange partners include foreign military forces, other Federal agencies, states, banks and tens of thousands of contractors. Ownership of systems and control over related funding are dispersed among hundreds of organizations. Decades of decentralized management have atrophied the Department's ability to collect current, accurate data on all of its systems and their interfaces. Until spring 1998, there was virtually no acknowledgment by the Joint Chiefs of Staff and war fighting commands that Y2K constituted a serious threat to military mission capability.

Finally, as late as early August 1998, the Department was still attempting to manage its overall Y2K effort with minimal staff.

Enter a perhaps unexpected source of help—auditors. The Air Force was probably the first Defense element to recognize the need for audit support on Y2K and the Air Force Audit Agency responded by identifying 5,000 systems missed in the initial inventory for assessment. This was a harbinger of things to come. After the Department's management plan was put into place in April 1997, a series of audits were conducted as an informal partnership between the Chief Information Officer and the Office of Inspector General. At management's request, the initial audits focused on what the unified commands—the war fighters—were doing to avoid losing mission capability. In addition, we began systematic validation of system status



reports, reviewed compliance with new regulations intended to stop the purchase of processors or software with Y2K computing limitations, and identified gaps and ambiguities in the management plan.

The results of the procurement review were alarming; 20 of 35 active major contracts for commercial off-the-shelf information technology products had no Y2K compliance clauses. When this finding was briefed in October 1997 to senior managers, the Department ordered immediate corrective actions. By the time the audit report was formally issued, no further recommendations were necessary. This pattern—expedited auditing, easy access to senior managers, and immediate corrective action—became the template for the several dozen audits that followed. That the pattern was more than a short lived phase was demonstrated again in August 1998, when IG findings on a blind spot in the remediation program—testing executive operating software for mainframe computer domains in Defense “mega-centers”—were briefed to senior officials including Deputy Secretary John Hamre and Mr. Koskinen. A few days later, Secretary of Defense William Cohen issued strongly worded guidance that entailed cutting off funding for any megacenter users unable to develop satisfactory testing agreements for such software by October 1998.

Confronted with a deluge of bad news, as our reports were provided to Congress, OMB and the public, managers found that being able to take credit for helping to focus intensive audit attention on questionable progress reports or particularly hard compliance challenges was far preferable to simply playing defense in reaction to criticism. Throughout late 1997 and 1998, senior Defense officials frequently referred in speeches, congressional testimony, reports and even media briefings to IG “validation” activities as a crucial oversight tool.

In addition to the accelerated pace of the Y2K audits and seemingly limitless management interest in auditor feedback, two other characteristics have been notable in our Y2K projects. First, the fact that the primary challenges in Y2K conversion are managerial, not technical, has meant that large numbers of generalist auditors could augment our limited automated system specialists to do the work. From the audit standpoint, we view Y2K remediation and testing as somewhat analogous to weapon system development, production and testing. Auditors generally do not test welds and I hope none of them insist on taking a turn piloting test aircraft. On the other hand, auditors are astute judges of processes, e.g., the adequacy of production quality controls or testing procedures for weapon systems. Therefore we consciously avoided being drawn into verification of coding changes and concentrated instead on management processes and the reliability of performance information. Had we not done so, we would have been unable to carry

out the especially broad IG audit effort on Y2K (42 projects in FY 1998).

Second, the number of offices involved and the pace of events in the Y2K conversion effort combine to confront every audit team with a constant barrage of information. Extraordinary effort is required to coordinate activity among a panoply of organizations, keep the audit programs as flexible as possible, respond to new ideas and requirements, and share results quickly and efficiently. We established a joint Y2K audit planning group with the other Defense audit agencies and emphasized coordination with GAO. We worked particularly hard to identify Y2K information sources and cultivated close working relations with key Y2K managers, with whom e-mail enabled easy and constant communication. We developed Y2K web sites for both the overall Federal audit community and our own internal use, and benchmarked our efforts with those of auditors in several foreign defense ministries.

Monday morning quarterbacking on the Y2K problem at this point serves only limited purposes. The emphasis must be on removing impediments to making up lost ground and serious contingency planning. Relentless apathy must be replaced by relentless testing. We intend to continue a maximum audit effort on Y2K, probably with another 40 or more projects, until the crisis is past. Given the ongoing downsizing of our non-financial audit program by nearly 50 percent, this is a painful, but necessary, commitment.

What about lessons learned? For Defense, the difficulty of Y2K conversion graphically underscores the folly of fragmented information technology management and past inattention to mundane basics like system documentation. The Chief Information Officer needs more direct control over budgets and far better visibility over the gigantic defense information technology portfolio. Although partially eclipsed by the Y2K crisis, the serious computer network security problem faced by Defense (an estimated 250,000 hacker attempts annually) bears startling resemblance to Y2K conversion in terms of its ubiquity, potential impact on mission capability, and lack of metrics with which to assess risk and progress. Fortunately, the Y2K contingency plans will serve the Department in good stead as contingency plans for information warfare, sabotage and natural disaster.

In the year 2000, as we clean up Y2K loose ends (let's not predict mountains of rubble) we may well find auditors mobilizing for a similarly large scale effort on information assurance. Regardless of what areas are being emphasized, however, the new and especially cooperative working relationships developed during the Y2K conversion serve as a model well worth emulating. As one audit manager exclaimed to me one day, “How can we ever go back, (to old ways) after this?” 🏠





---

CARLTON FITZPATRICK

*Assistant Chief, Financial Fraud Institute*

LISA SCHAFFER

*Senior Instructor, Financial Fraud Institute*

# SCERS for Curs

## *The Seized Computer Evidence Recovery Specialist*

**T**he seizure of computers in a criminal investigation, and the subsequent analysis of disk content, is becoming an almost routine occurrence in law enforcement. Although the seizure of computers is nothing new—it has been a part of criminal investigations for 20 years—there has never been a time when such an action has been more commonplace, nor as potentially ripe for serious procedural errors, than today.

Neither a proficiency in computer usage nor a mastery of particular desktop applications qualifies the investigator to effectively seize computer evidence. Indeed, experience has shown over the years that “a little knowledge is a dangerous thing.” Without an understanding of the internal workings of a computer, especially when it is first turned on, serious evidentiary damage can be done by the unqualified investigator who attempts to analyze the contents of a seized computer.

The question arises: How do investigators learn the processes involved in safely and effectively executing a search warrant at a computer site, seizing computer evidence, and properly determining the contents of the storage media? There are several training opportunities available for the concerned investigator. This article discusses training available from the Financial Fraud Institute (FFI) of the Federal Law Enforcement Training Center (FLETC).

### **FFI’s Approach to High Tech Investigations Training**

FFI, realizing that a two- or three-week training program is inadequate to provide all the skills necessary for a computer investigator, uses a hierarchical approach to training. For those journey-level investigators who are just beginning to unravel the mysteries of modern technology, FFI offers the Microcomputers for Investigators Training Program (MITP). The graduate of this two-week endeavor leaves with functional skills on using the computer as an investigative tool.

For those investigators with substantial proficiency and experience in computer usage, but who need to know how to work computer related investigations, FFI offers the Criminal Investigations in an Automated Environment Training Program (CIAETP). In this two-week program the participant is exposed to a variety of critical legal and privacy

issues, computer investigative techniques, principals of computer search and seizure, and the fundamentals of computer evidence analysis. The climax of the program is a practical exercise involving the actual seizure of a computer system and the analysis of the contents of the seized media.

There are certain investigators who will represent their agency (or, for larger organizations, their region or district) as the resident computer investigations specialist. Such an individual frequently offers technical advise to other agents in the field, serves as the focal point for all major technology-related investigations, and is typically involved in developing agency procedures and guidelines for high-tech investigations. To meet the needs of these individuals, FFI offers the Seized Computer Evidence Recovery Specialist (SCERS) Training Program.

### FFI's SCERS Training Program

SCERS had its genesis in the mid 1980's when the Internal Revenue Service Criminal Investigations Division (IRS-CID) began a major initiative to place highly trained technical investigators in each of its regions. The program was so successful that IRS began receiving (and granting) requests from other agencies to participate in the training program. So extensive were these requests that in 1994, FFI, working with the staff of the IRS National Academy, assumed responsibility for providing SCERS training to non-IRS personnel. The only appreciable difference between the two programs was that FFI, as a multi-agency training facilitator, did not (and does not) present agency policy or procedure. Instead, alternative viable approaches to situations—frequently with recommendations—were presented in class. This philosophy continues to be emphasized in SCERS training.

Until recently, FFI's SCERS has been an intense three-week training program. Recently, because of the proliferation of network (LAN) related investigations, FFI has removed LAN-related issues from SCERS and now offers a

separate two-week program Computer Network Investigations (CNITP). The successful completion of SCERS is considered a prerequisite for registration in CNITP.

With the segregation of LAN issues, SCERS is now a two-week program. It still maintains an almost frenetic intensity and is considered by most attendees to be the most challenging and the most rewarding professional training of their careers.

The purpose of SCERS is to provide criminal investigators (or those that routinely serve as part of the investigative team) the ability to search, seize, and analyze magnetic media originating from a variety of operating systems pursuant to the execution of a search warrant.

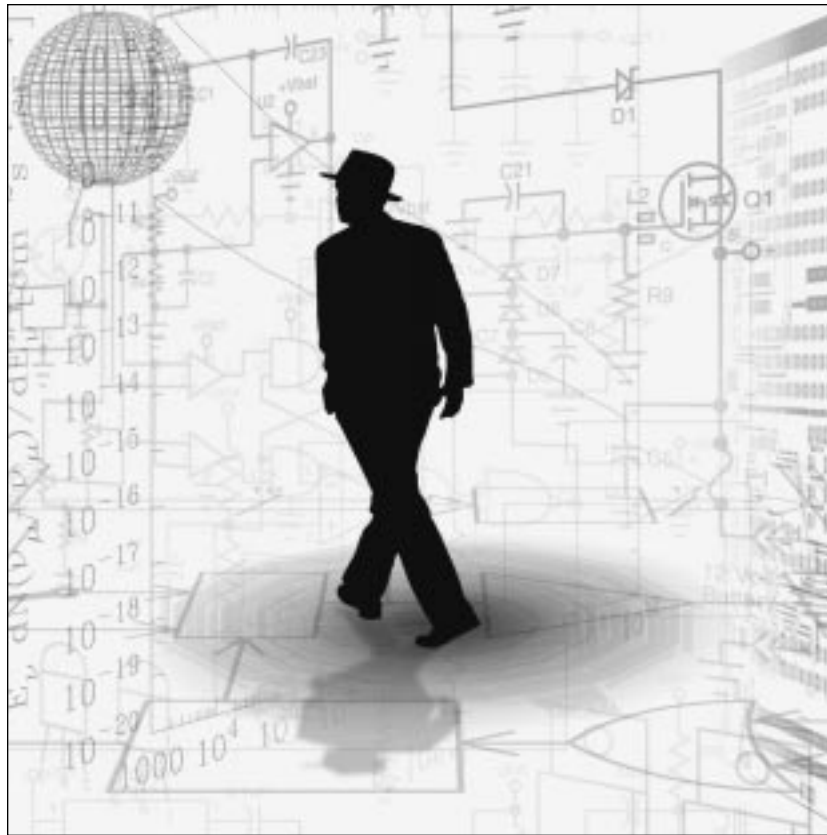
The program is sequential in presentation. That is, the information obtained in a particular course or practical

exercise serves as a foundation for subsequent classes and exercises. Technical, legal and investigative subjects are interspersed more or less equally throughout SCERS.

The training participants (maximum of 24 per class) use modern personal computers (currently Dell Pentium II's) and Hewlett-Packard Laser printers. Microcomputer software stored on student computer systems includes Windows 95/98, Quickview file viewer, Microsoft Office Professional (both versions 95 and 97, including

Word, Excel, Access and Powerpoint), WordPerfect for Windows, Norton Utilities, and several other commercial, non-commercial and proprietary packages. Students also use external Iomega Jaz drives during practical exercises.

Students are encouraged to bring laptop computers with them with appropriate software. A telephone line is provided for students to use their laptops to access a local number to their Internet Service Provider after hours. For those who do not bring their own personal computers, they are allowed to check out laptop/notebook computers for use after hours to complete homework and class assignments.



Course instruction is primarily the responsibility of the Financial Fraud Institute. Guest lecturers from several Federal, state and local agencies are used to supplement FLETC instruction. Participants have responded favorably to instructors who routinely search, seize and analyze computer systems in the field, and typically enjoy learning from their achievements as well as their mistakes.

The training program includes a series of several practical exercises used for evaluation purposes. A series of final practical exercises are constructed around an investigative scenario, which has been designed to provide as much realism as possible in a training environment. All situations contained in the exercises are gleaned from actual investigations, although contexts and names have been altered for training purposes.

Three methods of presentation are used in SCERS (as in all FFI programs). These are:

1. **Lecture/Classroom.** A training situation in which instructional material is being presented by an instructor.
2. **Laboratory.** A training situation in which students are practicing skills under the guidance of an instructor(s).
3. **Practical Exercises.** A training situation in which students, under the supervision or evaluation of an instructor(s), are participating in a law enforcement related activity which will be graded.

### Program OBJECTIVES:

At the conclusion of SCERS, the training participant will have demonstrated, through the successful completion of several practical exercises, a continuing-thread case study, and a written, comprehensive examination, that they have a functional knowledge of:

- Procedures used when searching, seizing and analyzing data from a computer system running DOS/Windows 3.1 and Windows 95/98, while maintaining the integrity and authenticity of the evidence.
- Procedures used to image/analyze data from a personal computer system with a unique configuration or running other operating systems such as Windows NT or Unix.
- Techniques for presentation of a computer related investigation to a U.S. Attorney or other prosecutor, and how to effectively testify about procedures used during imaging/analysis of computer data.
- Methods used to locate encrypted data and determine how (if possible) to break that encryption through the use of software and/or hardware tools.

These objectives are addressed through lectures, discussions, various types of practical exercises involving investigative scenarios, and demonstrations of relevant techniques.

### Other FFI High-Tech Training Opportunities

The seizure and analysis of computer evidence is only a small part of the investigative responsibilities of today's high-tech investigator. To meet the needs of agents in other technical arenas FFI offers several other programs.

**The Telecommunications Fraud Training Program (TCFTP).** This program addresses the complex issues involved in any case relating to investigations in the telecommunications industry. Such issues as wire fraud, call-sell operations, cellular phone fraud, use of dial-number recorders (DNR's), telephone traps and traces, and related subjects are presented. FFI receives substantial instructional assistance in TCFTP from the Communications Fraud Control Association (CFCA).

**Internet Investigations Training Program (IITP).** The unprecedented growth of the Internet and its evolving impact on society has created unique and exploitable criminal opportunities. FFI presents IITP in an effort to broaden the criminal investigator's skills in working such criminal cases. The program is still in the developmental stages and will be initially offered in March 1999.

**Computer Network Investigations Training Program (CNITP).** This program, already discussed, supplements the material presented in SCERS by offering training in the search, seizure, and evidentiary analysis of local area networks (LAN's), with an emphasis on Novell Netware and Windows NT.

**Electronic Sources of Information Training Program (ESOITP).** A staggering amount of information and investigative leads are electronically available to investigators who know where to look. ESOITP opens the door to the technically savvy investigator by presenting a relatively new tool: on-line networks. Commercial information providers, publicly available record providers, and the Internet are all presented as legitimate and invaluable investigative tools.

**Computer Crime Training for Prosecutors (CCTP).** This program was designed by and for prosecutors with an emphasis on non-Federal case investigations and prosecutions. The program is offered in association with a co-sponsoring State Attorney or District Attorney Office and specifically addresses the laws, procedures and Rules of Evidence of the hosting venue.

### Dedicated Departmental Training

An interesting and promising evolution in high-tech investigations training has been adopted by two Departments heavily involved in technical crime investigations: the Department of the Treasury and the Department of Defense. Both organizations have determined that the training needs for high-tech crime investigators are so critical, and consistency in training so vital, that priority initiatives have been approved to assure that investigators from each respective

department are taught the same policies, procedures, and investigative techniques, and provided with common investigative tools. While both projects are now fully operational there is strong indication that the end result will be a growing inter-departmental relationship between all high-tech crime investigators with greatly enhanced sharing of communications and resources.

Agents within Defense or Treasury who wish to pursue high-tech investigations training should first contact their departmental representative instead of a seeking the services of a multi-agency training provider such as FFI.

### Other Training Providers

Although FFI offers a compelling variety of training opportunities, it is not the only provider of excellent training in the field of technical crime investigations. Several other experienced and respected providers are mentioned with Internet addresses included for more information.

The SEARCH Group, Sacramento, California:  
([www.search.org](http://www.search.org))

International Association of Computer Investigative Specialists (IACIS): ([www.iacis.com](http://www.iacis.com))

National White Collar Crime Center (NWCCC):  
([www.irr.com/nwccc](http://www.irr.com/nwccc))

Houston Area Technical Support (HATS):  
([www.ghgcorp.com/cybercop](http://www.ghgcorp.com/cybercop))

Federal Computer Investigations Committee (FCIC):  
([www.fcic-usa.org](http://www.fcic-usa.org))

High Tech Crime Investigations Association (HTCIA):  
(<http://htcia.org>)

Other Contacts of Interest: (<http://cdp.com/TRAIN.HTM>)

### Conclusion

Law enforcement's need for trained and skilled high tech crime investigators will continue unabated. As indicated in this article, there are a variety of agency approaches and training opportunities that address this growing need. Since requisite skills are not addressed in law enforcement basic academies, it is incumbent upon the interested individuals and their agency to fulfill this requirement with committed resources, an interest in personal and professional growth, and a keen eye on the future of criminal activity and law enforcement's response. 🏠

---

MICHAEL VATIS

Chief, National Infrastructure Protection Center, Department of Justice

# The Empire Strikes Back!

## ***Building a New Partnership Across the Federal Government: The National Infrastructure Protection Center***



Michael Vatis

*“[T]he nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation’s security, economic health, and social well being. In short, they are the lifelines on which we as a nation depend.”*

*“The federal government must lead the way into the Information Age by example, tightening measures to protect the infrastructures it operates against physical and cyber attack.”*

Final Report of the President’s  
Commission on Critical  
Infrastructure Protection

As our society continues to rush into the Information Age, we will increasingly rely on electronic networks. As private citizens, we already depend on computers, the Internet, and other information technologies to manage our bank accounts, make credit card purchases, and engage in personal communications. As employees of the Federal Government, we depend on those same tools and technologies to manage our personnel records, store and communicate important and often sensitive information between offices around the country, and help manage the flow of military equipment and personnel to facilities around the world.

Information technologies are now a backbone for the critical infrastructures upon which our industrialized society and national security is based, and this reliance will continue to grow exponentially in the years ahead. These infrastructures—telecommunications, energy, banking and finance, transportation, and government operations to name a few—are highly automated and capable, yet at the same time much more dependent on each other than in the past. For example, the banking system depends on the availability and reliability of the telecommunications system and the Internet, which in turn rely on the generation and distribution of electrical power throughout the country.

While technological advances have resulted in greater efficiency and improved service in all of these infrastructures, they have also introduced new vulnerabilities and have given more people the tools to exploit them. The open and accessible nature of the Internet and modern telecommunications systems allows anyone with a moderate amount of technical skill and the right tools to penetrate the information and control systems of a government agency or company in order to gather data or inflict damage. Those who might conduct such activities include the disgruntled insider seeking revenge on an employer; a recreational hacker testing his or her skills; organized criminal groups seeking financial gain; foreign intelligence services seeking sensitive information; terrorist groups seeking to advance their political objectives; and hostile nations conducting “Information Warfare” attacks against the United States.

### **The National Infrastructure Protection Center (NIPC)**

The NIPC was established in February 1998 to address the growing problem of infrastructure vulnerabilities and threats. Our mission is to detect, deter, assess, warn of,

respond to, and investigate unlawful computer intrusions and other acts—both physical and “cyber”—that threaten our critical infrastructures. It is an interagency Center located at the FBI. It brings together investigators, analysts, computer scientists, other experts from many agencies, and the private sector.

The NIPC traces its roots to a number of Executive branch documents, including the 1995 Presidential Decision Directive (PDD) 39 on counterterrorism issued in the wake of the Oklahoma City bombing and the work of the President’s Commission on Critical Infrastructure Protection, which issued its final report in October 1997. The NIPC’s mission was recognized as a critical part of the Administration’s overall infrastructure protection strategy when President Clinton signed PDD-63 on May 22, 1998. In that Directive, the President directed the NIPC to serve as the nation’s focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. The NIPC is concerned not just with investigating and responding to attacks after they occur. A major focus is the prevention of attacks—learning about them beforehand and taking action to prevent them. This effort requires collecting and analyzing information from all available sources (including law enforcement, intelligence collection, open sources, and private industry), disseminating analyses, and warning of possible attacks to relevant government agencies and other potential victims.

### Success Through Partnership

The NIPC is built on the foundation of partnership—partnership among government agencies at the Federal level, partnership between the Federal government and State and local officials, and partnership between the government and private industry. We are constructing this partnership through *inclusive representation*. When fully staffed, the Center will have representatives from the FBI, the Department of Defense, the intelligence community, U.S. Secret Service, the Department of Energy, and other Federal departments and agencies that have roles to play in infrastructure protection. In addition, it will include representatives from the private sector owners and operators of the critical infrastructures to facilitate sharing of information and expertise on a daily basis and to improve coordination among all the actors in the event of a crisis. Moreover, it will include representatives from State and local law enforcement to help build effective liaison relationships with the people who are often the first responders in a crisis. Finally, the Center will augment the physical presence of these representatives by establishing electronic connectivity to the many different entities in government and industry that might have, or need, information about threats to our infrastructures.

Sharing data on threats, vulnerabilities, and incidents is crucial to the NIPC’s success. We intend to develop a two-

way street for the flow of threat and vulnerability information and incident data between the government and the private sector. The government, with access to national intelligence and law enforcement information, can develop a threat picture that no one company or group of companies in the private sector can develop on their own. At the same time, we would like to learn from industry about intrusions and vulnerabilities they are experiencing. This sharing of information will help paint the threat and vulnerability picture more completely, and will give us a head start on preventing or disabling a nascent attack.

The NIPC is not the nation’s super-systems administrator, responsible for securing everyone’s systems against intruders or advising on the latest security software or patches to fix vulnerabilities. That role clearly must be filled by Chief Information Officers in government agencies, systems administrators in individual companies, and by industry groups and other entities with expertise in reducing vulnerabilities and restoring service. Rather, the

**The NIPC is concerned not just with investigating and responding to attacks after they occur.**

**A major focus is the prevention of attacks—learning about them beforehand and taking action to prevent them.**

role of the Center is to help prevent intrusions and attacks. This mission will be accomplished by gathering and fusing information about threats from sources that are uniquely available to the government (such as from law enforcement and the Intelligence Community), combining it with information voluntarily provided by the

private sector or obtained from open sources, conducting analysis, and disseminating our analyses and warnings to all relevant consumers. If an attack does occur, the NIPC’s role is to serve as the Federal Government’s focal point for crisis response and investigation.

As a new organization attempting to address a relatively new problem, the NIPC has much work to do in building the foundation for its information sharing, analysis, and operational capabilities in partnership with other agencies. In the meantime, NIPC will use and build upon capabilities that exist in and around the government—both at the Federal as well and the State and local levels. We are taking advantage of existing FBI programs for information sharing, such as the Law Enforcement On-Line (LEO) and the Awareness of National Security Issues and Response (ANSIR) systems. We are working closely with all 56 of the FBI’s Field Offices. Each of them now has a Critical Infrastructure Threat Assessment (CITA) team and many offices have regional computer crime squads to investigate significant cyber incidents. We are in the final phases of

evaluating a pilot project developed by the FBI's Cleveland Field Office called InfraGard. This secure, Internet-based system will serve as a vehicle for sharing information among private companies and between the private sector and government agencies. InfraGard looks promising and we intend to expand it into a nationwide program in Fiscal Year 1999.

We also plan on working cooperatively with the Offices of the Inspectors General (OIG) throughout the Government. One example of such cooperation in the computer intrusion arena occurred earlier this year. Many of you are no doubt aware of the well-publicized computer intrusions into a large number of Defense Department, university, and commercial information networks that occurred between January and March 1998. These intrusions took place during a period of heightened tensions in the Persian Gulf and during deployment of US military assets overseas. Many senior decision-makers in the White House, the Pentagon, and elsewhere were concerned that these intrusions may have been part of a concerted effort to impede our ability to move troops and materiel to the region. An investigation, code-named Solar Sunrise<sup>1</sup>, was conducted by a joint task force led by the NIPC (and its predecessor organization, the Computer Investigations and Infrastructure Threat Assessment Center). It involved a number of Federal agencies, including NASA's OIG. In fact, intrusion data

---

<sup>1</sup>The name "Solar Sunrise" was derived from the operating system targeted by the attackers—Sun Solaris version 2.4.

gathered by NASA OIG investigators at California's Jet Propulsion Laboratory and other NASA facilities, and subsequently provided to task force members, proved crucial to identifying an Israeli citizen who went by the name "Analyzer" as one of the principal perpetrators of the intrusions.

The Solar Sunrise case pointed out that timely coordination and information sharing with law enforcement and investigative elements throughout the nation are critical for combating the cyber threat in the Information Age. Indeed, the cross-jurisdictional nature of many cyber crimes—in which attacks or intrusions originate outside state or even national borders and affect multiple targets throughout the U.S. or the world—means that many investigations must be coordinated among Federal, local, and state agencies. Sometimes they must also involve foreign law enforcement partners, as well. Unless such investigations are coordinated, as they were in Solar Sunrise, one investigating agency may not know that the crime it is investigating is related to other crimes occurring across the country. Only by working together can we stay on top of this emerging crime area and potential national security threat.

The NIPC is still in the early stages of development. However, the President and senior policymakers in many agencies have taken important steps in establishing the Center, in defining a national policy on critical infrastructure protection, and in recognizing the need for an inter-agency and public-private partnership. The challenges of the Information Age require creative solutions and new ways of thinking. We look forward to your participation and assistance as we move ahead. 🏠





# Be Kind to Your Webfooted Friends

## *E-FOIA Law Increases Access for the Public and Brings Changes to Agencies*

For over three decades federal agencies, including Inspector General Offices (“IG”), have been required to comply with the Freedom of Information Act (“FOIA”) and the Privacy Act. Since its existence, FOIA has led to the disclosure of waste, fraud, abuse, and wrongdoing in the federal government.<sup>1</sup> For example FOIA has resulted in the identification of unsafe consumer goods, harmful drugs, and serious health hazards.<sup>2</sup> These are precisely the types of activities that Congress intended that IGs would expose when they enacted the Inspector General Act (“IG Act”). Although the FOIA and the new Electronic FOIA were enacted to increase accountability in government, for the most part, neither IGs nor agencies have made FOIA implementation a priority.<sup>3</sup>

The FOIA and Privacy Act govern access to the millions of records and bytes of information that the government generates. A quick glance of the FOIA and the Privacy Act might leave some with the impression that the acts conflict. After all, the FOIA was enacted to facilitate and expand the public’s access to government records. In contrast, the Privacy Act was enacted to restrict access by third parties to personal information that the government collects on individuals. Frequently, however, when a member of the public makes a request pursuant to FOIA, Privacy Act considerations come into play. Regardless of how agencies determine whether a government record can be released, one thing is for certain, the format of records has changed dramatically in the last fifteen years.

### **Need for Access Grows**

Until recently, most of the records that the government collected and released were in paper form. When computers invaded government offices many records began to appear electronically. This new development threatened to unravel the goals of FOIA. Several

---

<sup>1</sup>Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104-231, §2(a)(3)-(4), 110 Stat. 3048 (1996).

<sup>2</sup>*Id.*

<sup>3</sup>See, OIP FOIA Update, Summer 1997. This update provides examples of agencies that have substantially complied with the requirements of the Electronic FOIA.

cases were litigated, and as a result, various courts ruled that certain electronic records were subject to the FOIA. However, the patchwork of cases created uncertainty and a lack of uniformity in the law. Moreover, there was no affirmative obligation to disclose certain information electronically to the public. Although the internet was becoming a common and inexpensive source for extracting information, the public, with some exceptions, did not have electronic access to government records.

At the same time the volume of electronic records generated by the government grew so fast that by the mid 1980's most records were electronic, yet electronic access lagged. After years of wrangling, Congress and the Executive decided to take action. On October 2, 1996 President Clinton signed into law the Electronic Freedom of Information Act ("E-FOIA")<sup>4</sup>. The E-FOIA was passed on a bipartisan basis and marked the first time that Congress addressed electronic access to records. The law also modified some of the requirements under the original FOIA. For example under the E-FOIA:

- Electronic records were explicitly made subject to the FOIA.
- The deadline for responding to FOIA requests was expanded from ten days to twenty days.
- Agencies were required to provide FOIA reports to Congress.
- Agencies were directed to establish a multi-tracking system for processing requests.
- Expedited Processing was made available for certain requesters.<sup>5</sup>

## Law Mandates Electronic Reading Rooms and Agency FOIA Guides

Nonetheless, one of most revolutionary provisions of the E-FOIA requires agencies to make electronically available by November 1, 1997 any reading room record created after November 1, 1996. Although the statute did not specify how the records should be made available, Congress clearly envisioned that departments establish web sites where the public could gain access to information through FOIA electronic reading rooms.<sup>6</sup>

Just what are reading room records? These are records that must be automatically disclosed by agencies independent of any request made by a member of the public. They include a range of public information like agency organizations and functions, rules of procedure, substantive rules and statements of general policy.<sup>7</sup> They also include docu-

ments, which the agency considers authoritative indications of its positions on legal or policy questions.<sup>8</sup> Nonetheless, if any of these records are exempt under FOIA, they can still be withheld and are not subject to reading room treatment.

Equally important, the E-FOIA requires that agencies make the following types of reading room records available electronically:

- Final opinions ... as well as orders rendered in the adjudication of administrative cases.
- Specific agency policy statements and interpretations.
- Administrative staff manuals that affect the public.
- Any records processed and disclosed that the agency determines have or are likely to become the subject of subsequent requests for substantially the same records.<sup>9</sup>

Some of these are not new requirements. FOIA has always required agencies to maintain public reading rooms where the public could inspect and copy certain information; including final opinions, certain administrative staff manuals, and specific agency policies.<sup>10</sup>

However, for the first time, agencies must anticipate if they are likely to or have received multiple requests for a document. Additionally, unofficial Department of Justice ("DOJ") guidance suggest that if agencies receive two requests for documents that are releasable and expect to receive a third, then the agency should place the document, or redacted documents, in its electronic reading room.<sup>11</sup> For redacted documents released under the FOIA, the amount of deleted information must be indicated at the place where the record was redacted. The E-FOIA extends that requirement to electronic records if technically feasible.<sup>12</sup> Thus, agencies will need to be cognizant of these requirements when purchasing new technology.

Assuming that there are still some individuals who are internet-challenged, for these requestors, agencies must honor their request to provide a hard copy. In fact, the agency must honor a requestor's choice among existing formats of a record; assuming there is no exceptional difficulty in providing the record in that format. Furthermore, if a requestor asks for a record in a different form or format, and the record is readily reproducible in that new form or format, the agency must comply with the request. Besides requested documents, records found in the electronic reading room must still be made available in a public reading room. However, agencies may fulfill that requirement by providing a computer and a printer with access to the elec-

<sup>4</sup>Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104-231, §1-12, 110 Stat. 3048 (codified as amended in 5 U.S.C. §552) (1996).

<sup>5</sup>*Id.*

<sup>6</sup>See, OIP FOIA Update, Fall 1996

<sup>7</sup>See, 5 U.S.C. A. sec. 552 (a)(1)(A)-(E) (West Supp. 1997).

<sup>8</sup>See, OIP FOIA Update Summer 1992; *Bristol Myer Co. v. FTC*, 598 F.2d 18, 25-26 (D.C. Cir. 1978); *Attorney Generals Memorandum the 1974 Amendments to the FOIA* 19 (Feb. 1975).

<sup>9</sup>5 U.S.C.A. § 552(a)(2) including (a)(2)(D)-(E)

<sup>10</sup>See, 5 U.S.C.A. § 552(a).

<sup>11</sup>FOIA & Privacy Act Seminar, July 1998.

<sup>12</sup>OIP FOIA Update, Winter 1998

tronic reading room assuming all their public reading room records are in electronic form.<sup>13</sup>

Another important requirement of E-FOIA is that agencies maintain a reference material or guide for requesting records or information. This document must be made available in the electronic reading room and must include:

- an index of all major information systems of the agency;
- a description of the agency's major information and record locator systems; and
- a handbook for obtaining various types and categories of public information from the agency.<sup>14</sup>

Moreover, by December 31, 1999, agencies will be required to maintain an index of all FOIA processed records and provide the index online.<sup>15</sup>

These E-FOIA requirements will have the effect of making records more accessible to the general public. With increased access, there will be more scrutiny and accountability regarding what records the agencies create, collect, store, and release. In addition, federal employees should expect that reading room documents created by them would potentially receive mass electronic distribution. Thus, the E-FOIA may have a deterrent effect on inadequate performers. Indeed, in enacting the E-FOIA, Congress acknowledged that FOIA revelations may have a certain degree of preemptive effect, prompting a higher degree of probity and conscientiousness in the performance of government operations.<sup>16</sup> Clearly, Congress views the E-FOIA as a

mechanism to increase performance. Thus, IG offices should consider making internal E-FOIA implementation, as well as compliance within their respective agencies, more of a priority.

## Interactions with Other Regulations

With the passage of the E-FOIA, agencies will be required to comply with other regulations such as OMB Circular A-130 ("A-130"). A-130 requires that agencies determine what records or information products are appropriate for an affirmative agency disclosure.<sup>17</sup> This provision will force

agencies to deal with complex issues. Under the 1996 directive, agencies were supposed to determine if documents (for example: audit reports or redacted investigation reports) would be available for copying or inspections. Since A-130 did not use mandatory language, many agencies put off the hard decisions. However, with the passage of E-FOIA, it is a mandatory requirement that frequently requested releasable records and reading room material be available electronically. Some agencies are now rushing to comply with the law. Therefore, many agencies are reevaluating the types of documents that should go on their webs as part of their affirmative disclosure requirements.

Another law, the Paperwork Reduction Act ("PRA") of 1995,

provides an administrative framework for agencies to affirmatively disclose information to the public through on-line methods, including the internet.<sup>18</sup> More affirmative disclosures, pursuant to the PRA and A-130, should, in the long term, reduce the burden on agencies to respond to regular



<sup>13</sup>See, OIP FOIA Update, Winter 1997

<sup>14</sup>See, OIP FOIA Update, Fall 1996

<sup>15</sup>*Id.*

<sup>16</sup>H.R. Rep. No. 795, 104<sup>th</sup> Cong., 2d Sess., pt. 1 at 6-7.

<sup>17</sup>See, 59 Fed. Reg. At 37920; OIP FOIA Update, Winter 1995.

<sup>18</sup>H.R. Rep. No. 795, 104<sup>th</sup> Cong., 2d Sess., pt. 1.

FOIA requests. Moreover, with the advent of the “paperless office” the trend of releasing more documents into cyberspace will continue.

### Agencies Struggle to Comply with the E-FOIA

Even though the deadlines to comply with many of the E-FOIA provisions have long passed, agencies continue to struggle in implementing E-FOIA. Specifically, the requirement that agencies set up electronic reading rooms and create agency FOIA guidance materials has not fully been met. Public interest groups, such as *OMB Watch*, have called the E-FOIA compliance by agencies “overwhelmingly inadequate.”<sup>19</sup> According to an OMB Watch Report, as of January of 1998, no agency had fulfilled all of the requirements, 44 fulfilled some, and 13 had no electronic presence.<sup>20</sup> Other groups, such as *Public Citizen* have filed lawsuits against seven agencies in federal district court for not complying with the E-FOIA requirements that mandate that agencies make available guides and indices that assist the public in obtaining agency records.<sup>21</sup> However, groups like *Public Citizen* reserve their harshest criticism for OMB, which they say has not provided the leadership necessary to fully implement the E-FOIA. Some agencies counter that they are hampered by a lack of resources and technology to fully implement E-FOIA. Others have kept costs low while substantially complying with most of the E-FOIA requirements.<sup>22</sup> Congress enacted the E-FOIA without allocating any additional resources. Nonetheless, the view from Congress is that the reading room requirement should actually free up resources to deal with other FOIA requests.

### Challenges Ahead

The E-FOIA has generated a series of challenges for agencies wishing to comply with the letter and the spirit of the law. There are unresolved issues that were not directly addressed by Congress when the statute was enacted. These

decisions are left up to individual agencies but often the lack of guidance causes delay in implementation of the E-FOIA. The following represents issues which agencies and IGs should consider.

Who should oversee the compliance? How should compliance be coordinated? While FOIA officers are well versed in the FOIA they are not necessarily familiar with developing customer friendly internet sites. There are also issues where legal counsel will have to review and determine what records the agency has to affirmatively disclose. Another issue may arise as to who will actually scan records into the electronic reading room.

E-FOIA implementation may raise record management issues. For example, when should reading room records be taken off the net? Currently Justice Department guidelines state that agencies should use their own “best judgement.”<sup>23</sup> How will the FOIA process interface with the electronic management systems under development in various agencies?

How should agencies deal with requirements to make affirmative discretionary releases of information even if they are not technically required to do so under FOIA? What criteria should be used when attempting to release a document into cyberspace? An issue can arise if an agency makes discretionary disclosures of information that may be favorable for the agency. It would seem then that the agency may have an ethical obligation to make affirmative disclosures contained in the same type of documents that may be embarrassing or unfavorable.

If E-FOIA requires redacted documents be put into the electronic reading room, what technology can be used so that third persons cannot hack into the redacted parts? Should the resources to purchase this material come from the FOIA office or should the cost be spread throughout the agency. Specifically, IGs should consider whether audit reports are appropriate for affirmative disclosure. IGs should also be aware that even investigations and inspections are subject to the requirement that frequently requested records be made available in the electronic reading room. On the other hand, E-FOIA does not change Privacy Act restrictions or FOIA exemptions regarding the release of certain records. Coordination between legal counsel, auditors, investigators, FOIA officers, webmasters, and management is crucial to insure compliance with the E-FOIA requirements. 📧

<sup>19</sup>Federal Agencies Hit Over Information Disclosure Law, Congressional Daily/ A.M., June 10, 1998.

<sup>20</sup>Jennifer J. Henderson & Patrice McDermott, *Arming the People with the Power of Knowledge*, OMB Watch Report, April 1998.

<sup>21</sup>Federal Agencies Violating the Freedom of Information Act, *Lawsuit Alleges*. Press Release, Public Citizen, Dec. 4, 1997.

<sup>22</sup>See, Nancy Ferris, *Virtual Records*, Government Executive, August 1997. Some agencies have substantially complied with the E-FOIA while at the same time have not incurred significant extra cost.

<sup>23</sup>OIP FOIA Update, Winter 1998

---

JAY AHUJA

*PricewaterhouseCoopers*

# Bright IDs

## *Assurance Services in Electronic Commerce*

**C**onducting Business in the Internet Age. The Internet provides an exciting new marketing and distribution medium for businesses and other organizations of all sizes. As an inexpensive and ubiquitous platform for conducting commerce, it enables both business-to-business and business-to-consumer exchange of goods, services, and information. Increasingly, organizations are turning to the Internet as a way to reduce costs, extend their market reach, and develop a competitive edge. Forrester Research, Inc., a market research company specializing in information technology and electronic commerce, estimates that buyers and sellers are expected to exchange well over \$10 billion annually by the year 2000.

This article examines the concerns related to electronic commerce transactions and how various Web based assurance services can be used to conduct trusted electronic commerce transactions between trading partners. Particular emphasis is placed on a new Web based assurance service developed by the American Institute of Certified Public Accountants (AICPA) called the WebTrust.

### **Electronic Commerce Concerns**

Conducting business on the Internet poses some new challenges, particularly in establishing trustworthiness and protecting the information exchanged by a business and its customers. Although electronic commerce (e-commerce) is exploding, both buyers and sellers voice concerns about conducting business on the Internet. The basis of this distrust can be illustrated by comparing two alternatives for conducting business.

In the first scenario, a customer uses traditional methods to conduct business with a physical entity such as a retail store. The store's customer can look for physical cues to convince them that they are dealing with a reputable, trustworthy business. For example, customers might note the uniforms and name tags worn by employees, official notices such as business licenses, plaques indicating membership in the Better Business Bureau or local Chamber of Commerce, and whether or not the establishment is clean and well-lit. They can also evaluate the merchandise first-hand, trying it on or trying it out before making a decision to buy. If they decide to purchase an item, they take it to a clearly marked register and observe the store employee place their money in the register or process their credit card. When the transaction is complete, they leave with their merchandise and receipt in hand.

The second scenario involves conducting business in the virtual world of the Internet. In this situation, the customer can be exposed to the risk of mistaking the Web-site of an

unscrupulous con-artist for that of a legitimate business particularly if both sites look equally professional. The absence of physical cues described in the first scenario, low barriers to entry and the ease with which graphics and text can be copied make it possible for almost anyone to create Web sites that appear to represent established businesses or organizations. As a result, organizations need to protect themselves and their customers from such impostors by establishing the authenticity of the Web site.

According to research conducted by the AICPA, would-be electronic customers are very concerned about the privacy and security of information they provide during Web-based transactions. These concerns arise because many questions remain unanswered about online stores. Among those questions are:

- Is this a real company?
- Is this a trustworthy company?
- How safe is the credit card or bank information transmitted to the vendor's Web-site?
- Where will the information provided to a company's Web site end up?
- How can one ensure that they receive exactly what they ordered?
- Will the delivery be as promised?
- Is the money-back guarantee honored?
- How soon will credit be granted for returned items?
- How quickly will the company perform service on warranty items?
- Will the company be able to send necessary replacement parts quickly?

Because concern over security remains the primary inhibitor to electronic commerce on the Internet, the ability to send and receive secure data has become a fundamental requirement. A mechanism is therefore needed to prevent unauthorized access to the information exchanged between businesses and their customers, such as credit card and account information. Furthermore, in this "faceless" environment, a business or organization needs a way to establish its identity and credibility in order to protect itself and its customers from impostors. Site visitors need assurance that the personal information they submit in an online registration form or the credit information they provide when making purchases cannot be read by anyone but the intended recipient site. Accordingly, consumers are increasingly demanding secure session technology for sending and receiving private information and conducting electronic commerce transactions over the Internet.

### **World Wide Web (WWW) based logo services**

In the past few years, Web based logo services or logo programs have been used to build trust between e-commerce

trading partners. Essentially, if a seller fulfills a set of criteria specified by an assurance provider, it can place the provider's logo on its Web site. The logo offers reassurance to concerned buyers that the seller meets the standards established by a trusted third party. Typically, the logo itself is tamper resistant and is linked to the assurance provider's site, which the user can visit to find out more detailed information about the meaning and scope of the logo service.

Even though retail e-commerce receives the most coverage in the press, the dollar value of business-to-business e-commerce transactions (encompassing manufacturing, wholesale trade and services) is significantly larger. According to Forrester Research estimates, the business-to-business market will grow to be eight times larger than that of retail e-commerce by the year 2000. Assurance logos provide an efficient and cost-effective way to screen potential sellers. Using this technique, business buyers can make calls for bids on the Web from a wider universe of suppliers rather than resorting to the business-as-usual scenario of seeking bids from a small number of established suppliers.

### **A Sampling of Logo Services**

There are a number of Web-based logo services that electronic customers have access to. While some logo service providers offer a wide range of services, others address fairly narrow issues. For example, in response to widespread public concern about the security of credit card information on the Internet, Mastercard and Visa collaborated on a joint venture called Secure Electronic Transactions (SET). Electronic vendors that meet SET standards for sending credit card information over the Internet can display the logo.

Another Web based logo service is the Better Business Bureau's (BBB) Online program, which grants a logo to a seller that has satisfied certain criteria or standards. BBB Online addresses the authentication problem by requiring buyers to click on the BBB Online logo residing on the organization's Web site to go to the BBB OnLine Web site, which verifies that the company's site is legitimately displaying the logo.

TRUSTe is a logo assurance service that primarily addresses Internet privacy issues. The TRUSTe logo essentially indicates that the seller has stated how the buyer's information will be used (for example, it will be used only for internal activities or it will be sold to third parties or some variation between the two policies) and the seller will abide by the stated policy. Knowing this policy is important to buyers because sellers can potentially extract information from buyers without their knowledge or permission and sell it to other companies. For example, a travel site may collect information from so-called "cookie files" on a traveler's computer and use it to build a profile for the traveler. Each

time the user visits the travel site, more information is added to the profile. Alternatively, businesses often share information extracted from forms that buyers complete online. To subsequently test a seller's adherence to its pledge, the TRUSTe organization enters a transaction in the seller's database with a phony user name. If that name later appears in another seller's database, TRUSTe knows the first seller has violated its pledge. The first seller could then lose its right to display the logo. Participating sellers also agree to a possible surprise audit by selected CPA firms.

The International Computer Security Association (ICSA), an independent organization that primarily concentrates on security issues, is another Web based logo service that offers Web Certifications Programs. However, ICSA, unlike BBB Online and TRUSTe, focuses on the technology side of e-commerce. The certification process includes a combination of self-reporting, on-site evaluation, remote and spot-checking. Organizations meeting the ICSA criteria can display the logo on their Web sites.

## WebTrust

AICPA's WebTrust is another one of several logo services. The Certified Public Accountants' (CPA) WebTrust criteria incorporates three broad principles:

- **Business Practices Disclosures.** The Web site operator discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.
- **Transaction Integrity.** The Web site operator maintains effective controls to ensure that customers' orders placed using electronic commerce are completed and billed as agreed.
- **Information Protection.** The Web site operator maintains effective controls to ensure that private customer information is protected from uses not related to its business.

Through a rigorous process, specially trained CPAs examine a company's Web site to evaluate whether it meets the logo service's prescribed business practices and control criteria. When successfully completed, a report indicating the site's compliance is issued and the site is granted the CPA WebTrust seal. Consumers can click on the seal to access the report, as well as the CPA WebTrust Principles and Criteria. The site must be revisited by the CPA and the seal must be refreshed at least every quarter. For more dynamic Web sites, this frequency may be increased. Each CPA WebTrust site is linked to a directory of all sites bearing the seal. Just as some companies and government agencies now require their suppliers to be ISO 9000 compliant, they may also in the near future require all suppliers to

display the WebTrust logo for electronic commerce transactions.

## WebTrust vs. Other Logo Services

WebTrust differs from other logo services in at least three important ways:

- The WebTrust criteria includes a broad variety of e-commerce criteria, well beyond that addressed by BBB Online or TRUSTe. WebTrust addresses business practices and internal control criteria. For example, WebTrust requires numerous performance disclosures on the Web site such as delivery times, how returns are handled and a phone number for customer service. The WebTrust criteria include specific technology and internal control disclosures relating to processing orders and protecting customer information.
- WebTrust authorized CPAs fully pre-test, under well-established attestation standards, all the seller's representations regarding the WebTrust criteria before issuing the logo while BBB Online and TRUSTe primarily rely on self-reporting and some after-the-fact testing.
- WebTrust requires that sellers be recertified at least every 90 days.

## Potential Pitfalls for WebTrust

The assurance arena, however, is not without risks. Retail consumers, unfamiliar with a CPA's attestation services, may not understand the limitations of WebTrust. For example, a consumer may believe a CPA firm, by performing a WebTrust engagement, is endorsing the seller's products. This could create the potential for a disappointed customer to bring legal action against the CPA firm. Business buyers generally have a better understanding of attestation engagements, but litigation risks also exist with these organizations. As a result, CPA firms will need to screen their prospective clients, particularly those in the retail e-commerce marketplace.

## Opportunities for Internal Audit and CPA firms


WebTrust attestation is not the only e-commerce service or assurance service that CPA firms could provide. Research conducted to date indicates that most clients of the CPA firms are not ready for their first WebTrust examinations. For example, appropriate internal controls may not be in place at these organizations. Thus, CPAs, in coordination with the Internal Audit department, may have significant opportunities to help clients prepare for WebTrust examina-

tions. Also, companies are justifiably concerned about the new and modified internal controls needed to support e-commerce. For example, the fact that outsiders will now have access to their online systems is understandably a matter of considerable concern. Supplying more in-depth internal control assurance services could provide many new opportunities for CPAs.

### **Role of Information Systems Auditors**

Information systems (IS) auditors, too, can become valuable players in the assurance services area. First, CPA firms are likely to solicit the guidance of Certified Information System Auditors (CISAs) to perform evaluations and test of controls over a company's computer and information systems. All Web servers, regardless of their physical location,

must be subjected to internal controls evaluations and testing, and the knowledge and experience of professional CISAs will be invaluable in this process.

Another potential area of involvement by IS auditors will be the evaluation of Web servers at an Internet Service Provider (ISP) via a SAS 70 engagement. SAS 70 reports are designed to be used by a number of "user auditors" for the customers (users) of the service organization. The SAS 70 report by the service organization's auditor evaluates the design of the policies and procedures in operation at the service organization (the ISP) and typically includes an evaluation of their operating effectiveness. The user auditor is then required to determine whether the internal controls within the user organization operate in conjunction with the reported internal controls at the service organization in such a manner as to provide reasonable assurance of transaction reliability and information protection. 



# Arresting Ideas

## *Securing Computers*

I can recall picking up my first copy of Byte Magazine in 1981. At that time, Byte was the premier computing magazine in the world. What I remember most is paging through all the article titles and looking at all the ads and realizing that I had absolutely no idea what any of them were talking about!

Seventeen years have passed since then. Not only is Byte is out of business but virtually all of the companies that had advertised in the magazine in the 80's are out of business as well. The computer field had progressed from the CP/M based S-100 systems through the Osbornes and Kaypros to over eight generations of Intel based PC's running DOS, Windows, Windows 95, Windows NT, Windows 98 and Linux. The desktop workstations of today have more computing power and connectivity than the largest mini-computers did when I picked up that first issue of Byte.

Today's computer growth industry is tied to networking. Whether your system is connected to a local area network (LAN), wide area network (WAN) or the really big network (the Internet) the computers of today can talk to each other easier and faster than ever before. Unfortunately, controlling who is able to talk to your systems has become a big problem.

Securing your network and systems connected to it has become big business. New magazines are appearing every day dedicated to the subject with articles and advertisements just as incomprehensible to lay persons as those appearing in Byte seventeen years ago. What I hope to accomplish in this article is to present a non-technical, brief overview of computer security as it relates to a networked system.

### **What is Computer Security**

The first concept that must be understood is that computer security is not a science, it is the art of balancing the need for access against the rational need for protection. It is generally the contents of the system and/or the level of connectivity of the system that dictates the level of protection needed.

For example, a computer containing non-classified word processing documents requires far less protection than does a workstation containing names and addresses of undercover operatives. Another analogy would be to examine the filing systems we currently use for paper documents—standard reports are kept in filing cabinets while sensitive or classified materials are kept in safes. Computers that are connected to the Internet or to large wide area networks (WANS) generally require a more comprehensive security policy than do systems part of a local area network.

There is an interesting phenomenon that occurs when users of the systems perceive the security policies are unjustifiably overly restrictive—security is actually lessened. If

users find security is interfering with their ability to do their jobs they'll almost certainly begin finding ways to circumvent it. A good example occurs in the government workplace when users bypass their LAN's firewall to access the Internet by installing unauthorized modems on their computers then dialing directly into the Internet with no protections whatsoever.

This leads to the second important concept of computer security—the users desire for user friendliness and ease of use are often diametrically opposed to stringent security policies. It's important to realize that security policies involving computers are often viewed by the user community as obstacles. From the users perspective a system or network should be easy to use and user friendly. Such systems, however, tend to be inherently insecure, hence the art of balancing the opposing interests.

The traditional approach to network security is to determine the highest level of security needed then enforce that policy across the board. A better approach, however, would be to segregate the high risk systems from the general network and apply heightened security policies to that subnet while leaving the general network easier to use and less costly to secure.

A good computer security program will not only provide each user with a written copy of their security program but will explain why such policies are important in terms they can understand. Once employees understand the rationale for the policies they're more likely "buy into the program."

The third rule of computer security is that 90% of an average security policy addresses 10% of the risks. Traditional computer security deals almost exclusively with keeping the "outsiders" outside, the so-called untrusted, out of the trusted. Unfortunately, past experience has shown that "outsiders" represent only 10% of the overall security incidents while 90% of the security incidents occur from within the organization itself. In essence, the vast majority of your security funding and endeavors go towards protecting your systems against a small portion of the threat.

It makes sense if you stop and think about it. Who is more knowledgeable and has more opportunity to attack a network than an insider? What makes matters worse is that security incidents often involve the ones entrusted to protect the system—the system administrators themselves. Since system administrators have unlimited access to the systems, including auditing functions, it is very difficult to investigate such cases as the evidence is routinely destroyed.

The fourth rule of computer security is what I refer to as the "Ostrich Syndrome". In simple terms, the Ostrich Syndrome is the false belief that those posing a threat to your system have the same technical level of expertise as you do. I can't count the number of times I've heard the comment, "It appears to be really secure—I tried to get in and couldn't." There are some pretty intelligent, ingenious hackers out there who have honed their skills by spending

thousands of hours learning every detail of your operating system and hardware's BIOS. If your systems contain sensitive information, you should gear your security towards that type of threat level rather than that of the average user.

My fifth rule of computer security is more of a prophecy than a rule. Simply put, if a good hacker ever gets into your system you'll never know it. The true hacker elite have an amazing repertoire of tools at their disposal to not only gain entry into a system but to hide their presence once they get in. If you believe some of the hackers accounts, fewer than one in ten "rooted" systems are ever discovered by the system administrator.

### **Hackers—the Threat ...**

Before talking about what we need to do to protect our systems it might be a good idea to know who and what we need to protect them against. This topic could easily fill a book in and of itself but we'll focus on the general population of today's hackers.

The average hacker is a white male, age 16 thru 27. They tend to have above average intelligence and tend to socialize within their own ranks. They have a worldwide network of friends with similar interests and communicate with one another via email and Internet Relay Chat (IRC). They tend to have large egos and seek out the approval, admiration and respect of their associates by boasting about their successful exploits. Interestingly enough, their communications network is second to none—news of exploits are often disseminated worldwide within minutes. They even hold international hacker conventions in Las Vegas!

The hacker population is stratified into two levels - the elite and the "bottom feeders". The elite probably represent less than 1% of the population. They are the ones that discover the various vulnerabilities and write the software programs used to exploit them. The bottom feeders, representing 99% of the hacker community, simply obtain the programs written by the elite and run them. Unfortunately, those well written programs often exploit very obscure operating system vulnerabilities difficult to detect. Once exploited, your system can be modified to such an extent that the only recovery is to totally reformat the hard drives and reload the operating system from scratch.

What's their motivation? The primary goal of most hackers is to "root" a system then use it as a stepping stone towards other systems within the network. Rooting a system refers to the successful penetration of a system and obtaining root or administrator privileges.

How do the hackers attack a system? Step one involves identifying all of the systems in your domain. For that information they generally go to your domain name servers (DNS) and list all of your systems along with their addresses.

The next step involves profiling one or more of your systems. One tool used for this is called a port scanner. A

port scanner goes out to each port on the system and tries to determine which ones are active. Once active ports are identified they are examined more closely in order to determine the exact program running on that port. For instance, the port scanner might indicate that port 25, the SMTP mail port, is active. The hacker simply connects to that port and discovers that the process is the sendmail daemon, version 8.9.1.

Once they have identified your system and the services it is running they research all known vulnerabilities with each of the programs you're running then exploit the identified vulnerabilities.

Why do so many government systems get hacked? The two most prominent reasons are inadequate technical skills on the part of the system administrators and the failure to maintain current software released on the system. By running older versions of operating systems with known, published vulnerabilities, breaking into the systems becomes child's play.

Continuing with the intrusion, the hacker now has obtained access to the system using either a known vulnerability, dictionary attack (discussed later in this article), socially engineering or other means. The next step is to upload a collection of tools often referred to as the "root kit." These tools enable the hacker to obtain root privilege, install additional backdoors into the system, install sniffers and remove all evidence of the intrusion and continued operation of the sniffers.

The hacker has now set up shop on your network using your computer as a tool against you. The sniffer quickly identifies additional user ID/password combinations and the hacker expands his kingdom by rooting additional systems.

To reiterate what I said above, if the hacker is good, you'll never know you've been hacked. This means that you can be running a totally compromised system for years and never know that everything going across the system is being monitored.

One simple defense against sniffers is to use ethernet switches as opposed to standard hubs. A rooted system with sniffers running on it cannot monitor other servers on the subnet if connected via a switch.

Generally, the only time a hacker would maliciously destroy a site is if he or she believed they were being watched by law enforcement and that information contained on the system could be used against them.

Now that we've covered a little about who poses the threat to our systems it's time to talk about simple, common sense tips to secure your systems.

## The Warning Banner

The first requirement for securing your systems is to make sure it displays a warning banner when someone attempts to log in. If someone hacks into your system and the U.S. Attorney's Office discovers there was no banner they will almost certainly decline prosecution.

The banner should contain the following verbiage: "This computer is owned and operated by the government of the United States of America. Use of this system is restricted to OFFICIAL USE ONLY and all activity is subject to monitoring. Continued use of this system constitutes consent to such monitoring. Unauthorized access of this system or exceeding authorized permissions is a violation of federal statutes. If you have reached this system in error, disconnect now."

## System Administration

The single most important factor that determines overall security of your systems and networks is the level of competence of your system administrator. If you hire a person to maintain your system and they are technically incompetent your network will always be at risk—period.

The system administrator should have an extensive background in computer science and possess a demonstrated knowledge and expertise of the computer hardware, software and operating system. That doesn't mean they necessarily require a degree from a University but it also doesn't mean that just because they are an expert with Lotus 1-2-3 or Word Perfect they're qualified to maintain your mission critical system.

Aside from performing day to day maintenance of the systems, administrators should routinely perform five additional functions:

1. Maintaining accurate user accounts
2. Creating frequent backups of the systems
3. Installing and maintaining software updates
4. Installing and maintaining operating systems updates and patches
5. Providing constant vigilance over the systems audit logs looking for anomalies that could indicate a security violation

I'll bet that if you were to examine any system that has been in operation for over three years you'll find "active" users on that system that have quit, died, been fired or retired. It's a good idea to have your personnel office send notification of separated employees to your system administrators on a regular basis to insure that those accounts are deactivated immediately.

Periodically you should have an outside person sit down with the system administrator and make sure all accounts on the system are bona fide. It's not uncommon for system administrators to add fictitious users to the system with root privileges. That way, if they are kicked off the system for whatever reason they have an alternate way back in. Remember, most of your threat originates from within. Without a doubt, your system administrator is in the best position to hurt you the most.

Different systems require different backup schedules. As a general rule, if the system collects information or has

databases that are updated frequently they should be backed up at least once daily. Systems used for special applications like gateways or terminal servers require less frequent backups, possibly monthly.

You should always keep a set of recent backups off-site in the event of a major disaster such as a fire or break in at the facility itself.

It is also important to retain sets of full backups over a long period of time. For instance, you should make a full backup set monthly that are retained for a two year period. Should your system become corrupted, you may find that some files had been corrupted long before your last full set of backups. Also, should you discover that your system had been compromised, reviewing former backups may provide leads on how long your system was insecure and help you to assess the damage.

Updating software has taken on a new meaning with the upcoming year 2000 concerns (Y2K). All software companies offer patches and fixes for commercially sold software. In fact, even public domain freeware and shareware software is routinely updated. System administrators should routinely verify that their systems are running the latest release of the program and that any security patches are applied immediately (within hours of release).

Let's discuss audit trails and system updates separately.

## **System Audit Trails**

From a computer security standpoint, audit trails provide three forms of information. First, they show the health of your system. Secondly, it details who does what on the system and thirdly, it constitutes the primary evidence needed to prosecute those that attack your system.

It's common practice to turn auditing off on systems because of the overhead it imposes and the huge amounts of disk space it consumes. If those become issues, you should get bigger and faster systems and/or larger hard drives. Auditing should be mandatory.

The audit trails are of little use if they aren't examined on a daily basis. Few, if any, administrators examine the logs unless they are debugging a specific problem. Administrators must be told that a critical element of their job is the review and analysis of those audit trails.

In my laboratory we have automated scripts that constantly monitor certain situations and perform real time auditing. Should certain situations occur, such as a port scan, the system automatically sends email to a number of accounts and pages me on my alpha-numeric pager with a brief synopsis of the problem. Real time auditing like this should be implemented on all systems and firewalls connected directly to the Internet.

## **Maintaining the Operating System**

When the hacker community discovers a vulnerability in an operating system they immediately publish the information

across their vast network. Within a day or so the company or group responsible for the operating system will acknowledge the problem, publish a patch then attempt to notify all users of that system to apply that patch.

Several months ago a BIND (domain name server) vulnerability was discovered. BIND is not part of an operating system but is generally bundled with one. Anyway, within four days a patch was developed, tested and released. During that four day period, however, over 100,000 machines were allegedly attacked and compromised. Maintaining current, up to date operating systems is absolutely necessary. If your system is running a process or program that creates a vulnerability and you fail to fix it you will be hacked—guaranteed. The U.S. Government, both military and civilian, is notorious for not properly maintaining their systems. This is why so many hackers attack government systems—they use them as a training ground.

It has been my experience that the vast majority of government owned computers are delivered from the manufacturers with default configurations that are never changed or updated by the system administrators. In most cases the reason is simple—the administrators lack the knowledge of how to update the systems configuration or recompile the operating system kernels.

File servers and multi-user operating systems often run "processes" that are unnecessary. A process is simply a program that is invoked for a specific purpose. Most Unix boxes are delivered with over a dozen such processes running; some of those processes can be exploited remotely by hackers to obtain information on your system that can subsequently be used to attack it. One such "process" found on Unix boxes is "finger", a program that enables others to remotely determine who is logged into your system. Hackers can use "finger" to obtain names of active accounts.

The very first thing that should be done with a new system is to disable all services that are not needed. On Unix boxes, those services include echo, discard, daytime, chargen, time, nntp, comsat, shell, login, talk, imap, uucp, tftp, bootps, finger, systat, netstat, rstatd and NFS.

Most systems come configured with a number of default accounts, all of which should be disabled. Those accounts are often named bin, daemon, admin, lp, sync, shutdown, halt, mail, operator, games and man.

Major operating system components like the mail program (sendmail) and domain name server (BIND) should be kept at the most recent release. If you are running file servers or multi-user operating systems rest assured that security advisories are constantly being published which notify the computer community of vulnerabilities that have been discovered and patches that are available to fix those vulnerabilities.

I can't stress this enough—if your system is connected to the Internet and your administrators are not constantly updating the operating system, streamlining processes and

applying security patches you'll become a prime target, actually, an easy prime target.

## User Authentication

The most basic and rudimentary form of security involves the use of user ID's and passwords for authentication. The user ID identifies the user, the password insures that the user is who they say they are.

Most systems store the user information in a system file along with the password in an encrypted state. On some systems, users actually have access to the file that contains the encrypted passwords (older versions of Unix) while more modern operating systems store the passwords in a special protected system file which prevents users from accessing it (i.e the shadow file on newer Unix systems).

The password functions much the same as a combination of numbers does on a combination lock. The strength of the password is determined by it's length and uniqueness. On a combination lock, each of the numbers can range from 1 to 100. If the combination consisted of only one number, you would have 100 passwords possible. If the combination contained two numbers, you would have 100 to the second power of combinations, or 100 times 100 which equals 10,000 possible unique combinations. With three numbers there would be one million discrete combinations available.

Since passwords are limited to printable characters, you generally have approximately 120 characters at your disposal for each and every character contained in the password. With a password of only four characters you would have 207,360,000 (120 to the fourth power) discrete passwords while with eight characters you would have 120 to the eight power of combinations or 42,998,169,600,000,000 (120 to the eighth discrete passwords available).

On the surface, text based passwords appear secure as the number of possible permutations is far too great to conduct a brute force attack on (trying each and every possible combination). In reality, however, passwords are often easy to bypass due to user laziness. User supplied passwords can often be guessed (social engineered) or cracked using a dictionary password cracker.

A dictionary password cracker is a program that takes a list of common passwords, encrypts them then compares them to the encrypted entry found on the host system. I obtained a program called Cracker Jack which came with a password dictionary of only 2500 passwords. When I ran it

against one of our mission critical systems it was able to identify over 30% of the passwords. Common passwords found—"Thursday", "qwerty", "secret", and "password."

There are two ways to increase security over passwords. One way is to install a program that prohibits users from entering simple passwords containing names or single words. The second method is to replace simple passwords with a token based authentication system. In my lab we utilize SecurID which is a token based authentication system. Users carry a small credit card that produces a six digit number every 60 seconds. When the user logs into the system they enter the token based number plus a personal identification number. It's a little pricey but extremely secure.

## Conclusion

Make sure your systems display a warning banner that advises the user that they've connected to a government computer system, that all activity is subject to monitoring and continued use of the system constitutes implied consent to be monitored.

The security of your network is directly related to the expertise and dedication of your system administrator. If you are using a modern operating system and your systems are properly configured, extraneous services are minimized and patches are applied in a timely manner and your system should be adequately protected. Systems requiring more stringent security policies should employ some form of token based authentication and sit behind firewalls.

There are a number of automated tools available that can be used to test your system against literally hundreds of known vulnerabilities. These tools are updated on a regular basis and offer extensive reporting; one such tool is called Ballista. A good security program should include periodic testing of your network using such tools.

If you believe your network has been compromised immediately contact your agencies computer support staff and have them work with your criminal investigators who will hopefully aggressively investigate and prosecute those responsible.

The Internal Revenue Service's Internal Security conducts training classes for criminal investigators actively involved in working computer crime cases. If your agency is interested in participating in future training programs please feel free to contact me for further information. I can be reached by phone at (202) 622-3535 or via email at [afried@cis.fed.gov](mailto:afried@cis.fed.gov). 📧



---

JOHN W. LAINHART, IV

*CISA, Inspector General, House of Representatives*

# Building the Soul of a New Machine

## *Auditing Software Development*



John W. Lainhart, IV

With the ever increasing dependence of our organizations on the effective and efficient use of information technology and the mission critical information produced by this technology, the Inspector General community must place increased emphasis on audit and control of this mission critical information and the technology that produced it. Since the mid-1970's, the General Accounting Office has required auditors, in its *Government Auditing Standards* ("Yellow Book") to "obtain sufficient, competent, and relevant evidence that computer-processed data are valid and reliable when those data are significant to the auditor's finding."<sup>1</sup> Furthermore, the "Yellow Book" goes on to state that "when the reliability of a computer-based system is the primary objective of the audit, the auditors should conduct a review of the systems' general and application controls."

In addition to these long-standing "Yellow Book" computer-based system auditing requirements, recent events have led to the development of additional requirements for all Federal departments and agencies related to control and audit of "cyber-based systems." These new requirements are a result of Presidential Decision Directive 63 which directs every department and agency of the Federal government to develop a plan to protect its own critical infrastructure, including, but not limited to its cyber-based systems. This plan should consider the organization's identified critical infrastructures and their vulnerabilities.

To assist organizations in fulfilling these critical infrastructure protection responsibilities related to cyber-based systems, the Critical Infrastructure Assurance Office, contracted with KPMG Peat Marwick LLP to develop Vulnerability Assessment guidance.<sup>2</sup> Through a three-step process, the Vulnerability Assessment Framework (VAF) is designed to assist organizations to define their Minimum Essential Infrastructure, identify and locate interdependencies and vulnerabilities, and provide the basis for developing needed remediation plans. The VAF was designed with inherent scalability so that is applicable to all levels of government and the private sector, as well as broad sectors of the National Infrastructure. It is based on existing security requirements and standards from both the Federal government and private industry. As indicated in the VAF, one such primary

*A Methodology for Managing  
and Controlling Information and  
Information Technology Risks  
and Vulnerabilities*

CobiT™

---

<sup>1</sup> *Government Auditing Standards, 1994 Revision*. U.S. General Accounting Office, June 1994, page 86.

<sup>2</sup> *Vulnerability Assessment Framework 1.1*. Critical Infrastructure Assurance Office, October 1998.

source that was used “heavily” in developing the VAF methodology, was COBIT<sup>TM3</sup>, or Control Objectives for Information and related Technology.

### CobIT Overview

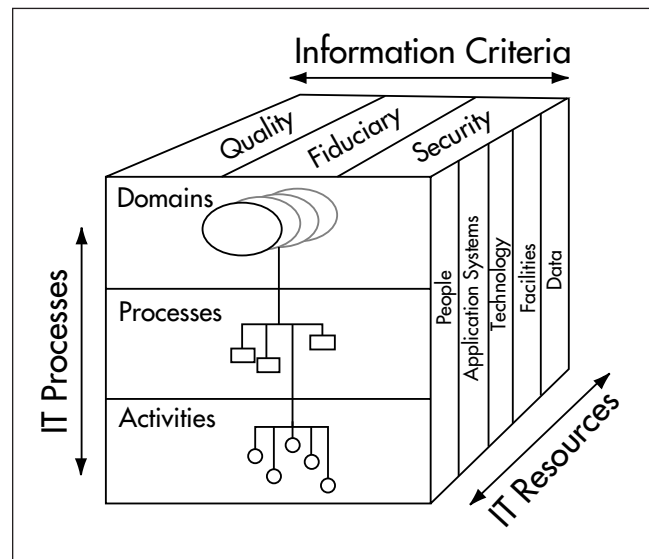
COBIT addresses the need for management and control of information and related Information Technology (IT). It recognizes that effective management of information and related IT is critically important to the success and survival of our organizations. In this global information society—where information travels through cyberspace without the constraints of time, distance, and speed—this criticality arises from the:

- increasing dependence on information and the systems that deliver this information;
- increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare;
- scale and cost of the current and future investments in information and information systems; and
- potential for technologies to dramatically change organizations and business practices, create new opportunities, and reduce costs.

For many organizations, information and the technology that supports it represent the organization’s most valuable assets. Truly, information and information systems are pervasive throughout organizations—from the user’s platform to local and wide area networks to client servers to mainframe computers. Thus, management requires increased quality, functionality, and ease of use; decreased delivery time; and continuously improving service levels, while demanding that this be accomplished at lower costs. Many organizations recognize the potential benefits that technology can yield. Successful organizations, however, understand and manage the risks associated with implementing new technologies. Thus, management needs to have an appreciation for and a basic understanding of the risks and constraints of IT in order to provide effective direction and adequate controls.

Organizations must satisfy for their information, as for all assets, the requirements for quality, fiduciary, and security. Management must also balance the use of available resources including data, facilities, technology, application systems, and people. To discharge these responsibilities, as well as to achieve its expectations, management must establish an adequate system of internal control. Thus, an internal control system or framework must be in place to support the business processes and it must be clear as to how

each individual control activity satisfies the information requirements and impacts the resources. The impact on IT resources is highlighted in the COBIT Framework together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information that need to be satisfied. Control, which includes policies, organizational structures, practices and procedures, is management’s responsibility. Management, through its corporate governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance, or operation of information systems. An IT Control Objective is a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.



### CobIT Information and IT Resources Requirements

Business orientation is the main theme of COBIT. It is designed not only to be employed by users and auditors, but also, and more importantly, by business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls. The COBIT Framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The Framework starts from a simple and pragmatic premise:

*In order to provide the information that the organization needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.*

It continues with a set of 34 high-level Control Objectives, one for each of the IT Processes, grouped into 4 domains: planning & organization, acquisition & implementation, delivery & support, and monitoring. This struc-

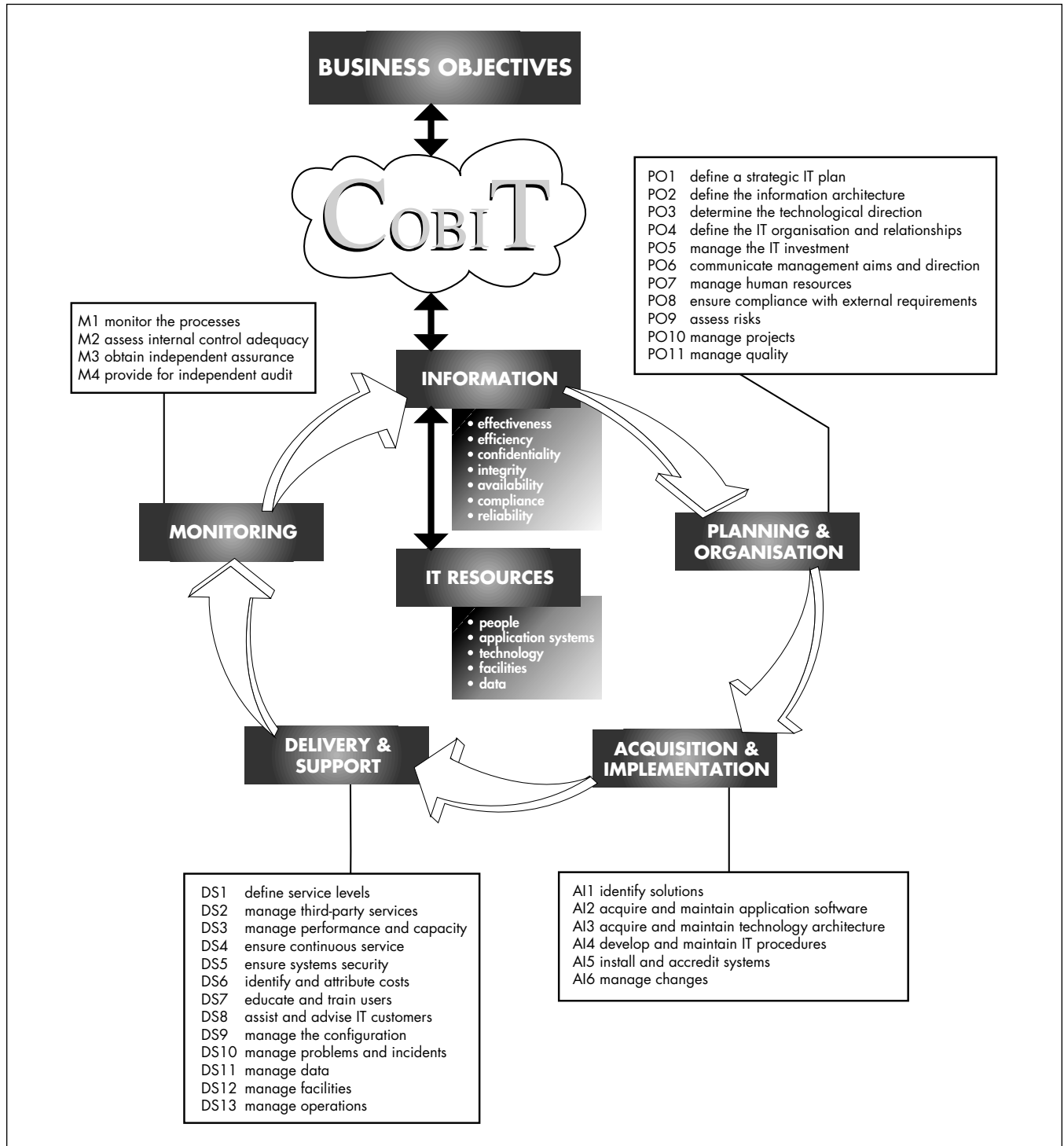
<sup>3</sup> COBIT<sup>TM</sup>, *Control Objectives for Information and Related Technology*, 2<sup>nd</sup> Edition. Information Systems Audit and Control Foundation (ISACF is a not-for-profit international research foundation), Rolling Meadows, IL, April 1998.



ture covers all aspects of information and the technology that supports it. By addressing these 34 high-level Control Objectives and with reference to the organization's policies and standards, the business process owner can ensure that an adequate control system is provided for the IT environ-

ment. In addition, corresponding to each of the 34 high-level Control Objectives is an audit guideline to enable information systems auditors in reviewing IT processes against COBIT's recommended control objectives to provide management assurance and/or advice for improvement.

### CobIT IT Processes Defined Within the Four Domains



The management of the organization needs generally applicable and accepted IT governance and control practices to benchmark their existing and planned IT environment. COBIT is a tool that allows managers to communicate and bridge the gap with respect to control requirements, technical issues and business risks. The main objective of COBIT is to enable the development of clear policy and good practice for IT control throughout organizations, worldwide. It is COBIT's goal to provide these control objectives, within the defined framework, and obtain endorsement from commercial, governmental, and professional organizations, world-at-large. **Thus, COBIT is intended to be the breakthrough IT governance tool that helps in understanding and managing the risks associated with information and related IT.**


COBIT is achieving worldwide recognition as the authoritative source on IT Governance, IT Control Objectives, and IT Audit. It is being used globally in a variety of ways by private industry, public accounting firms, governments, academia, etc. It is being used by Boards of Directors, Audit Committees, CEOs, heads of governmental organizations, CIOs, Security Managers, Information Systems (IS) Auditors, users, etc. Specifically, COBIT is appearing as criteria in reports issued by audit organizations around the world. It is being included in audit manuals, by all types of organizations in both the private and government sectors, for use in annual audit planning and performing IT audits. Similarly, accounting firms are including it in their audit procedures when auditing IT. CEOs, heads of governmental organizations, worldwide are keeping it on their desks to use as reference sources when IT issues arise and are requiring it to be included in requests for proposals for IT audits, evaluations, and reviews. CIOs are incorporating the COBIT concepts in their policies and procedures for managing IT resources. Security Managers are using COBIT's security and control tenets in developing, implementing, and maintaining their IT security policies, procedures, and programs. It is also being incorporated into classroom training in colleges and universities globally, and COBIT is being taught worldwide at Information Systems Audit and Control Association international conferences, regional conferences and seminars, and chapter meetings. In addition, the **Inspectors General Auditor Training Institute** has entered into a contract with ISACF to provide COBIT training classes at IGATI's Ft. Belvoir training facility.

## Recent Initiatives

Recently, ISACF updated COBIT by performing additional research into the secondary and newly identified reference materials. This effort resulted in significant enhancements to the existing document. The original COBIT document was based on 18 reference documents and had 32 high-level Control Objectives, whereas the 2<sup>nd</sup> Edition is based on 36 reference documents and has 34 high-level Control Objectives. In addition, the original COBIT document had 271 detailed Control Objectives, whereas the 2<sup>nd</sup> Edition has 302. The updated COBIT document also includes an implementation tool set which provides lessons learned from those organizations that quickly and successfully applied COBIT in their work environments. The tool set

**Many organizations recognize the potential benefits that technology can yield. Successful organizations, however, understand and manage the risks associated with implementing new technologies.**

includes an Executive Summary and Executive Overview for senior management awareness and understanding of COBIT's key concepts and principles. It also includes an implementation guide with two useful tools—Management Awareness Diagnostic and IT Control Diagnostic—to assist in analyzing an organization's IT control

environment. Also included are eight case studies detailing how organizations worldwide have successfully implemented COBIT. In addition, this 2<sup>nd</sup> Edition includes answers to the 25 most frequently asked questions about COBIT and several PowerPoint slide presentations, geared to different hierarchical levels and audiences within organizations. This 2<sup>nd</sup> Edition also comes in a CD-ROM version using Folio Views<sup>®</sup> which provides detailed indexing and key word searches. Furthermore, and most importantly, the ISACF Board of Directors recognized the potential significance of COBIT's impact on effective IT governance and deemed components of this 2<sup>nd</sup> Edition "open standard." As such, the *Executive Overview*, *Executive Summary* and *Framework*, with *High-Level Control Objectives*, are available for download from [www.isaca.org](http://www.isaca.org). 

---

JACK LEWIS

*Office of the Inspector General, Social Security Administration*

# The New de-Tech-tives

## *The Social Security Administration Office of the Inspector General's Experience*

**T**oday's law enforcement community recognizes that many of our investigations will be conducted in an automated environment. Through training, experience, and cooperation we are preparing ourselves to be successful in this developing arena. Often dealing with electronic crimes include the task of retrieving and analyzing digital evidence. The question facing each agency is not whether they will face the digital evidence challenge, but how to prevail. Should they formulate their own response, or rely upon other agencies for assistance. Recently, a few of the Inspectors General have chosen to develop their own ability to successfully resolve issues concerning the seizure and examination of digital evidence.

There are a number of issues to resolve when establishing a specialized unit: what is their mission, use of program management and policy, who will be selected, how will they be trained and equipped, and will there be adequate funding to cover unit start-up and continuing costs. This article highlights the experience of the Social Security Administration (SSA), Office of the Inspector General (OIG), as we established our Electronic Crime Team (ECT).

### **Mission Statement**

Although each OIG considers in their own way matters of fraud, waste, and abuse, the SSA OIG applies significant resources to investigate fraud that compromises the disbursement programs under Title II and Title XVI of the Social Security Act. The stakes are very high because SSA's programs account for over 25 percent (\$404 billion) of all Federal dollars spent. Increasingly, a Special Agent's caseload is a growing mix of investigations involving physicians, attorneys, translators, representative payees, and those who counterfeit documents to obtain SSA funds. That caseload defines the mission of the SSA OIG Electronic Crime Team: to provide technology assistance to OIG Special Agents as they conduct their investigations. Today, that mission involves the following initiatives:

- Provide appropriate training for Special Agents that will prepare them to conduct successful investigations in an automated environment.
- Assist Special Agents in the development of their criminal investigations, including the preparation of search warrants and subpoenas for electronic media (computers, computer systems, disks, backup tapes, digital diaries, and electronic organizers).

- Provide on-site field support for the execution of search warrants and initial review of electronic media.
- Provide laboratory analysis and courtroom testimony concerning the evidentiary contents of electronic media seized during criminal investigations.

In addition to the primary mission, the Electronic Crime Team is the law enforcement component of a multi-disciplined SSA response to network intrusions. The Electronic Crime Team also provides the Inspector General (IG) and the Assistant Inspector General for Investigations (AIGI) with a point of contact for the law enforcement and legal communities in matters of investigative and forensic technology.

### Program Management and Policy

The selection of a program manager for any Electronic Crime Team is critical. The manager must have sufficient technical skills to bring credibility to the Team's efforts. Additionally the manager must know, or be willing to meet with, subject matter experts and other technical managers to ensure that collaborative efforts are available to resolve technical and investigative issues. For the SSA OIG Electronic Crime Team, the program manager is responsible for daily Team operational and administrative activities. These responsibilities include the following:

- Set technical standards for the Electronic Crime Team concerning their forensic training and examination methods.
- Ensure quality control for Electronic Crime Team efforts, particularly forensic examinations.
- Routine approval authority for the conduct of computer forensic examinations and the review and

approval of all computer forensic examination reports.

- Select and procure equipment and specialized training for Electronic Crime Team members.
- Represent the IG and the AIGI at law enforcement and technical forums concerning investigations and forensic technology.

The SSA OIG Program Manager is the focal point for policy development concerning both operational and administrative issues. These issues range from who will

review electronic media to who will pay costs associated with the review. Recognizing the importance of professional computer forensic examinations, the AIGI issued the following policy statement: "It is the policy of the Assistant Inspector General for Investigations that only Seized Computer Evidence Recovery (SCERS) Special Agents from the Electronic Crime Team examine electronic media thought to be of evidentiary value. Attempts to review electronic media by those not fully trained could lead to alteration of crucial evidence. Exceptions to this policy must be reviewed with the ECT Program Manager and then approved by the AIGI or his designee."



### Selection and Training

The Electronic Crime Team is a field support unit designed and developed with the field Agent in mind. Team members must be able to participate fully in each of the

mission initiatives, including efforts to provide appropriate technology training for all Special Agents. In determining selection criteria, a decision was made to identify senior investigators who had an established history of conducting quality investigations and who had previously specialized in computer forensic support. Although the amount of work

was not yet fully apparent, it was decided that four Special Agents would satisfy our near-term requirements. Currently, the Electronic Crime Team is composed of one Assistant Special Agent-in-Charge and three Special Agents from the Office of Investigations. Two of the Team members were found within the existing staff of the OIG. The remaining two Agents were hired by the OIG specifically to participate in the Electronic Crime Team. The Team members are evenly split between OIG Headquarters and Field Divisions. The placement of Team members in the Field reflects our belief that most investigations benefit from the on-site assistance of the Team members at the time of search warrant execution. It also reinforces our belief that the forensic examination is best conducted as soon as possible, and with the active participation of the investigative case agent.

Each Agent has completed the SCERS course offered by the Financial Fraud Institute at the Federal Law Enforcement Training Center, in Glynco, Georgia. An excellent basic course, SCERS is just the beginning. Electronic Crime Team members participate in advanced training ranging from network seizures and Internet investigations, to the advanced features of operating systems such as Windows NT, UNIX/Linux, and Macintosh.

## Equipment

Computer forensic equipment for the Electronic Crime Team is used in two general areas: the field and the forensic laboratory. Flexibility is the key, and purchases were made with an eye towards the ever-increasing storage capacity of desktop computers. Four years ago a 2-gigabyte hard disk drive was sufficient for a medium-size network server. Today, mid-range desktop computers are available with 300 MHz Pentium II processors and 6.2-gigabyte hard disk drives for under \$1000. The only sure bet is that next week or next month, the computers will be faster, with more storage capacity, and still inexpensive. It is critical that all software, commercial and forensic, be purchased and licensed for the individual agency or user. The unauthorized use of software or involvement in copyright infringement can be both a criminal and civil violation. Software selections were made after a critical review of laboratory and field tests previously conducted by the law enforcement forensic community.

Electronic Crime Team members have been provided with the following basic computer forensic hardware:

- Media analysis computer (forensic laboratory).
- 17" SVGA color monitor.
- Notebook computer (laboratory and field).
- Spare, large-capacity hard drives.
- Iomega Zip and Jaz drives.
- ISA and PCI SCSI host adapters.
- Laser printer.
- 8mm tape backup unit.

- Shock-resistant carrying case.
- Uninterrupted power supply.

The following basic software toolkit was provided to each Team member:

- Original distribution media for the following operating systems: MS DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows NT, and Linux.
- Norton Utilities, file and graphic viewers, and anti-virus applications.
- Specialized forensic and recovery tools from law enforcement and commercial sources.

Although there are many software applications available, each with its unique personality, we have chosen to adopt a limited number of software tools and to exploit their full potential.

## Electronic Crime Team Costs

Hardware and software costs for each Electronic Crime Team member was approximately \$15,000. Additional start-up costs were not as apparent. Existing space was easily converted into secure forensic processing areas and Team members had already received the basic SCERS training. Ongoing costs are hard to determine because some are exam specific. One thing is sure, there will be additional costs associated with continuing education and training of Team members. Training costs are estimated to be approximately \$5,000 per year for each Team member.

Travel and per diem expenses for this program are the responsibility of OIG Headquarters and do not come out of Field Division budgets. To prepare for Electronic Crime Team travel, blanket travel orders are issued each quarter, allowing a timely response to forensic requests. Electronic Crime Team members also travel to each Field Division to participate in annual training seminars; an excellent opportunity to build trust and confidence between Team members and field investigators.

Each computer forensic examination is a unique event and may include unique expenses. To respond to these examination-specific expenses, Team members have access to accelerated buying authority through the use of the Government "IMPAC" card.

Replacement costs for major hardware components is difficult to calculate. A safe estimate is that major computers will be replaced every two to three years. Additional software, both commercial and forensic, will be required as new operating systems are encountered or new forensic examination requirements are undertaken.

## Summary

The decision to form a specialized unit to seize and evaluate digital evidence is unique for each law enforcement

agency. The SSA OIG has decided to take some modest steps to ensure that we can accomplish our investigative missions. The Electronic Crime Team has been staffed, trained, and provided appropriate equipment. The mission has been identified, and the Team members are fully opera-

tional. The amount of work required of Team members will determine if staffing stays at the current strength or increases to meet field requirements and challenges. Considering the quality of SSA OIG investigations, I believe that we will be very busy. 📧

---

GARY R. AUSTIN

Senior Information Systems Auditor, U.S. General Accounting Office

# Moving into the Next Millennium

## *Systems Auditing Capability Development for Internal Auditing*



Gary R. Austin

**T**oday's auditing professionals face considerable challenges as advancing information technology continually changes entity-wide business processes and structures. For example, open client/server systems have eliminated organizational barriers to information, forcing executive managers to expect more from their assurance providers in order to protect their entities' more accessible—and hence valuable—information. To successfully compete with other assurance providers, auditing departments must develop a survival strategy: a paradigm shift from focusing on traditional fixed financial auditing issues to focusing on dynamic critical performance issues, such as market-oriented systems, operational processes, and non-financial resources—intellectual capital, human resources, and information—designed to manage how changes are made.

Making such a shift requires gaining a greater understanding of the accounting and business information system environment(s) that—increasingly under the Chief Information Officer's (CIO) control—integrate(s) all entity processes into a coherent whole<sup>1</sup>. This article will discuss how auditing departments can adapt their audit processes to these environments in order to successfully assess the integrity, confidentiality, and availability of entities' critical performance areas.

### **Current Status**

Auditing departments encounter many problems in assessing system-based environments, including:

- Hard-copy reference tools heavily relied on in auditing currently—will be eliminated in paperless environments.
- Management can become confused by the many different organizations setting standards for auditor certifications. (E.g., IIA, ISACA, The American Society of Quality, and The International Organization for Standardization.)

---

<sup>1</sup>Gary L. Holstrum & James Hunton, *Information Systems Auditors Play a Critical Role in Shaping Future Assurance Services*, IS Audit & Control Journal, Volume III, 1997.

- Audit findings are often considered individual problems rather than symptoms of broader problems by executive management.
- Rapid change in organizations' systems makes it difficult to stay current and provide adequate coverage for all major risk areas.
- When problems are not clearly defined during systems audits, top management does not know if auditing departments or their entities' systems are inadequate.
- It is difficult for management to measure the value-added content of systems audits.

To resolve these problems, a pervasive and sustainable capability must be developed, where work processes are reengineered and staff members attain certain IS skill levels<sup>2</sup>. However, many auditing departments' efforts have met with limited success, due to the difficulty of combining general and systems auditing practices into a standard audit process. Specific audit process attributes (what to do, what to test, etc.) are not well understood, documented, and accepted as a standard best practice<sup>3</sup>. In such environments, organizational resistance to change is high and management views capability development as a technical rather than a change process issue<sup>4</sup>. Consequently, the needed understanding of integrated audit processes never takes place. Without this understanding, sustained support for learning and embrac-



ing change declines, and the reengineering effort is abandoned. When this occurs, the focus shifts to building individual versus entity-wide expertise.

The problem is magnified by the fact that—due to downsizing—today's auditing departments must accomplish more with fewer resources. In many cases, outsourcing is considered a viable option because personnel expenses are not incurred (e.g., training, pension, health, etc.). Doing so may satisfy current systems auditing needs, but strategic capability development needs likely go unmet, jeopardizing the quality of future internal auditing services.

### **Learning and Embracing Change**

To meet the challenge, a process-oriented management approach is needed. This process can be divided into three phases: unfreezing, transitioning, and refreezing existing processes<sup>5</sup>. Unfreezing is when organizations accept, establish, and foster the growth of a systems auditing capability based on current and future needs. Auditing departments apply systems auditing methods and techniques to select audit assignments to learn what can be applied successfully on a repeatable basis. Once this is understood, capability develop-

ment efforts can focus on transitioning existing audit processes department-wide. Department-wide acceptance by all management and staff leads to a refreezing phase where technical system audit processes become an integral part of the overall audit process and infrastructure. The essence is a synergy and linkage between general and sys-

<sup>2</sup>IIA Advanced Technology Committee, *Model Curriculum for Information Systems Auditing: A Knowledge Skill Set for Auditing in an Information Systems Environment*, Altamonte Springs, FL: The Institute of Internal Auditors, August 1992.

<sup>3</sup>Smith, Gordon, *Creating the Integrated Auditor* (New Jersey: ISACA, New Jersey Chapter Newsletter, Vol. 12, No. 2 – 1995).

<sup>4</sup>Tener, William T., The IIA Research Foundation, *Adapting the Integrated Audit Approach*, Altamonte Springs, FL: The Institute of Internal Auditors, 1992.

<sup>5</sup>Ibid.



tems auditing processes. Critical success factors for these changes include:

- A strong management commitment to developing the capability.
- An audit management team dedicated to capability development activities.
- Active management participation in field audits.
- A complete revamping of audit techniques and formalization of audit methods.
- A basic infrastructure of systems audit programming support.
- A strong employee willingness and ability to change.
- Use of process-based performance measures to monitor progress for improving capability.

### Systems Auditing Capability Framework

An approach that effectively embraces change process concepts is IIA's *Systems Auditing Capability Framework*, a process assessment and improvement model designed to help internal audit departments develop effective change process strategies. The framework has diagnostic and detailed self-assessment instruments designed to facilitate the process of (1) understanding a department's systems auditing capabilities and needs, (2) developing a strategy for prioritizing improvements, and (3) providing a means to periodically validate capabilities achieved. Evaluative methods used are modeled after established change process criteria and industry best practices for evaluating effectiveness of processes<sup>6</sup>. The assessment instruments are organized around a set of key process areas defined by capability maturity levels. The levels, as benchmarks, enable an internal auditing department to evaluate the status of processes actually used against defined maturity levels in achieving desired capabilities. Consistent use of this structured assessment approach will provide a firm base for reducing investment risks and for measuring the evolution of an internal auditing department's systems auditing capabilities.

The framework/toolkit can be broken into five areas that provide assessment and improvement guidance to

<sup>6</sup>Harrington, Dr. H.J., *Business Process Improvement: The Breakthrough Strategy for Total Quality, Productivity, and Competitiveness*, Sponsored by The American Society for Quality Control, New York, McGraw-Hill, Inc., 1991. Paulk, Curtis, Chrissis, & Weber: *Capability Maturity Model for Software, Version 1.1 (CMU/SEI-93-TR-24)*, Pittsburgh, PA.: Software Engineering Institute, Carnegie Mellon University, February, 1993. Rout, Terence P., *Software Process Assessment and Improvement: The SPICE Project*, IS Audit and Control Journal-Volume 1, Rolling Meadows, Illinois: Information Systems Audit and Control Association, 1995. Senge, Peter M., *The Fifth Discipline: The Art and Practice of the Learning Organization*, New York, NY: Bantam Doubleday Dell Publishing Group, Inc., 1990. U.S. General Accounting Office, *Business Process Reengineering Assessment Guide*, Version 2.0, Washington D.C., March 1997.

internal auditing departments. Each area is discussed below:

**1. Management Overview.** Detailed description of:

- Purpose and organization of the framework as a toolkit.
- Background on established process improvement criteria for defining the framework's maturity levels and common attributes for maturity or foundation building activities.
- Components of the framework—its maturity levels and key processes at each level.
- General assessment guidelines for determining how to improve an internal audit department's capability.

**2. Self-Assessment Startup.** Detailed description of preconditions and requirements for performing a self-assessment. This includes:

- Critical success factors, such as executive leadership and commitment to the self-assessment process, an action plan for improvement as a follow-up to the assessment process, and a dedicated assessment team with the requisite knowledge, skills, and abilities to perform the assessment.
- A structured work plan for the assessment process.
- Audit management considerations in initiating changes in response to assessment results.

**3. Diagnostic Assessment.** Detailed description of the diagnostic questionnaire tools and summary worksheets provided in the toolkit. This includes procedures for an assessment team to:

- Conduct a quick, preliminary assessment.
- Determine which maturity level and key process areas warrant more in-depth attention than others and establish priorities for detailed assessment work. (Note: It is important to recognize, however, that diagnostic tools are not intended to be used alone.)

**4. Detailed Assessment.** Description of detailed assessment procedures and summary worksheets provided in the toolkit. This includes procedures for an assessment team to:

- Assess an internal auditing department's ability against best practices for achieving a given maturity level's process implementation goals.
- Evaluate control environment features of key processes reviewed for fostering stability, support, and sustainability.
- Obtain an in-depth understanding of strengths and weaknesses that need to be identified in order to develop an improvement program.

**5. Process Improvement.** Detailed description of assessment procedures and a summary worksheet for assessing an internal auditing department's ability to initiate an effective process improvement program. This includes procedures for an assessment team to:

- Identify strengths and weaknesses in process improvement capabilities.
- Recommend improvements to the program.

**Framework's Maturity Level Structure**

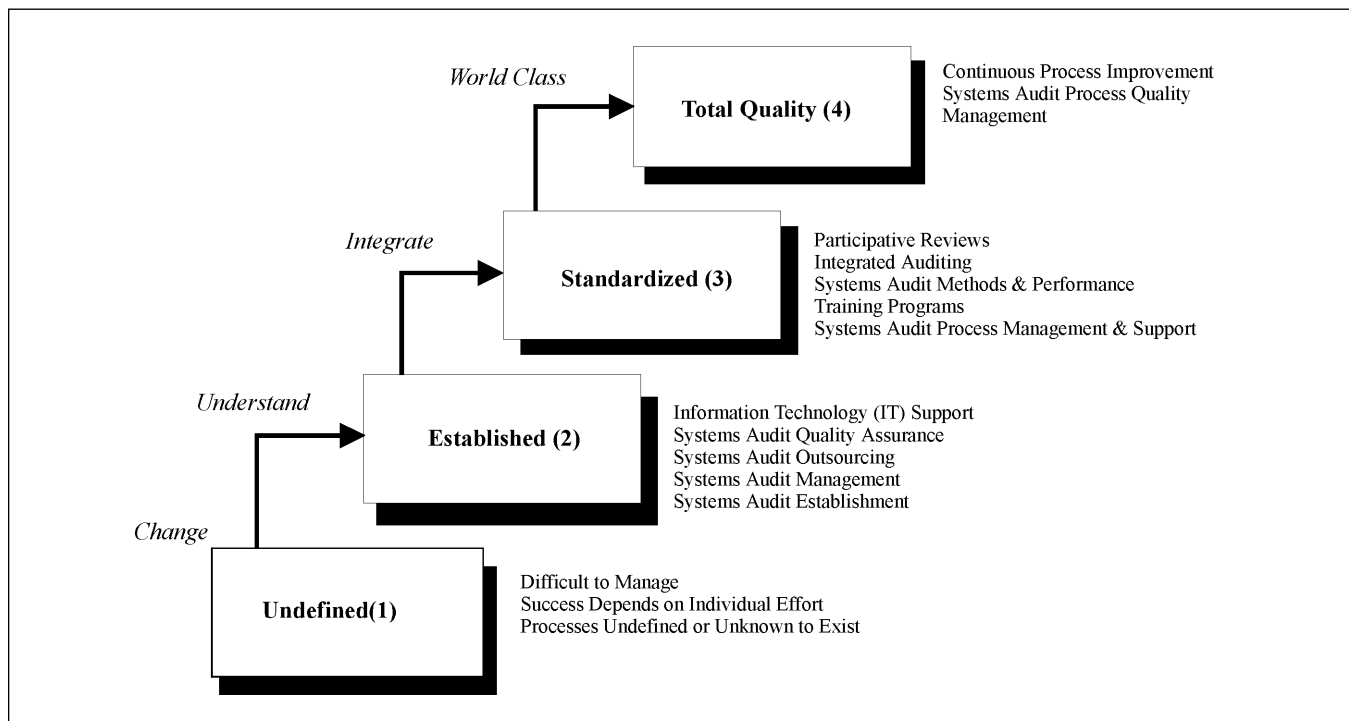
The framework identifies four maturity levels as key milestones or benchmarks for establishing a system audit capability (see figure 1). Each level has a set of key process area (KPA) capabilities and each key process is supported by a unique set of best practice attributes and a common set of control environment factors to provide institutionalized sustainability and support.

Each level achieved lays the foundation for successive levels of improvement until an audit organization attains a World Class, continuously improving capability. During the assessment, a department's systems auditing capabilities are evaluated and assessed at one of the four milestone levels, which forms the basis for future process improvement. These levels and their corresponding KPAs are defined as follows:

**1. Undefined.** Key processes for the most part are undefined or possibly not known to exist. If a capability does exist, it is based solely on individual expertise, which may be difficult to manage.

**2. Established.** A learning environment is created where (1) a stable and supportive infrastructure is established and (2) effective performance measures are applied for systems auditing processes in support of select general audit process assignments. This enables internal audit departments, with the necessary management discipline in place, to gain an understanding of systems auditing issues. The result is systems auditing practices successfully applied on a repeatable basis for audits similar in size and scope.

**3. Standardized.** Building on the understanding gained at the prior level, a pervasive integrated capability is developed in accordance with prescribed and documented standard processes. With a focal point group, a formal systems audit process management and support infrastructure is established, where improvement activities are coordinated with department stakeholders. This leads to the development of documented standard processes—a cross-functional definition of a standard systems auditing process and a total "integrated" auditing process that is tailorable, manageable, and consistently applied.



**FIGURE 1. Four Levels of Systems Auditing Process Maturity and Key Process Areas**

**4. Total Quality Management.** World-class status is attained in developing a comprehensive and pervasive total quality management system for quantitatively controlling, understanding, and continuously improving standard systems and integrated auditing processes. In this environment, a quantitative understanding of systems and integrated auditing processes exists. These attributes are enablers for continuous improvement initiatives leading to an error-free dynamic capability adaptable to future IT advances.

### Benefits and Caveats of Use

The framework as an assessment guide is intended to help audit managers develop effective and sustainable improvement initiatives. Although not a guarantee of success, the likelihood increases as an organized improvement strategy is carried out, and as improvements made for attaining a particular maturity level occur in laying the foundation for the next level. For this reason, assessments should not be considered a one-time effort. The process starts with an assessment team performing a disciplined examination that identifies the lowest level where audit practices have not been met and where problems are recurring. This establishes a baseline where improvements should proceed. For example, an assessment might show that audit management should not yet develop a standard system audit methodology if management is not actively involved in learning what technical processes best work for their organization. Subsequent assessments should assess progress in achieving desired results, before starting other initiatives.

The focus, therefore, is on resolving problems at a particular level, where each level builds a foundation for succeeding levels to create further improvements. This occurs until a point is reached where the internal audit department

is satisfied with its level of maturity, or attains a *World Class* capability of Total Quality Management.

Without attaining an institutionalized “maturity level” capability, internal audit departments can still profitably use processes described at higher levels. For example, detailed audits of general and application controls are not discussed until level three. Yet even organizations at level one can perform these activities successfully. However, capabilities developed in this manner never reach their full potential and eventually disappear, since processes without the proper foundation fail at the very point they are needed most—under stressful situations where timing and resource constraints exist. Consequently, they provide no basis for future improvement.

### Conclusion

To meet the challenges faced by today’s internal auditing departments, a process-oriented management approach is needed for learning about and embracing change created by information technology. IIA’s *Systems Auditing Capability Framework* provides an excellent way for audit departments to create synergy and linkage between general and systems auditing processes, with the potential to evolve into an integrated and dynamic “*World Class*” auditing capability. By following its guidelines and tailoring improvements to entities’ specific needs, internal auditing departments can provide professional services at the level demanded by today’s executive managers. 🏠

*This article was adapted with permission from Internal Auditing, Sept./Oct. 1998. Boston: RiA.*



---

BRIAN A. DETTELBACH

*Office of Inspector General, Department of Transportation*

## Message Massage

### *Ensuring Your Semiannual Message Doesn't Fall on Deaf Ears.*



Brian A. Dettelbach

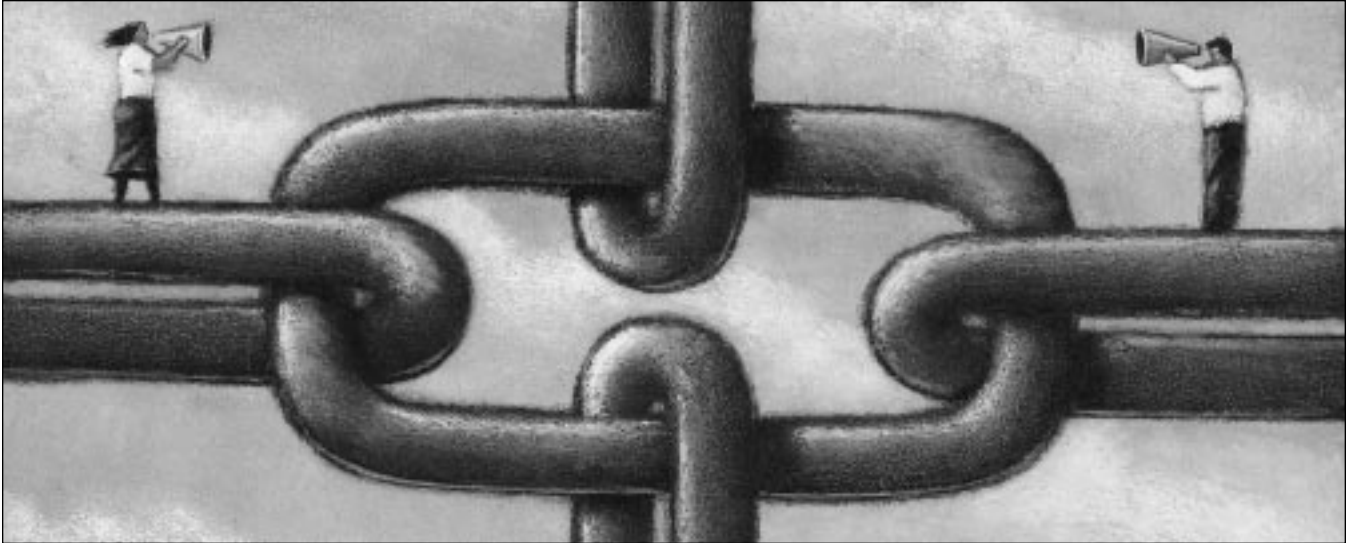
When I had the privilege of serving as Senator Glenn's Counsel for the Committee on Governmental Affairs, one day a very outspoken Inspector General (IG) of a Cabinet-level Department, then engaged in a rather nasty public dispute with the Secretary and some Members of Congress, unexpectedly resigned. It prompted inquiries from a steady stream of reporters seeking background and comments. In the middle of this frenzy, I took a call from the Majority staff of that IG's authorizing committee. They were looking for the last Semiannual Report (SAR). I invited them to come over, since we received SARs from every Office of Inspector General (OIG) as required by the Inspector General Act. Within minutes I received a similar request, this time from the Minority side of the same authorizing committee. By day's end, staff from the appropriations committee had also checked in, looking for this now—suddenly—popular SAR. Upon reflection, it struck me a bit odd that the very Congressional committees which oversee and appropriate funds for this OIG apparently had not bothered to keep any of their SARs on hand.

Having recently switched hats by going to the Department of Transportation Office of the Inspector General, I now appreciate more fully the time, effort, and resources devoted to the production of SARs. When done right, they give readers a flavor of the type of work being performed, OIG priorities, and the value added by OIG activities to the efficiency and effectiveness of agency operations. SARs can enhance Congressional oversight of the agency, its management, and programs.

Information contained in SARs can prompt interested Members and staff to request more detailed briefings on particular matters. In some cases, it may spur Congressional Members and staff to follow up directly with an agency head to resolve questions impacting OIG authority. One recent SAR, for instance, noted an IG was having difficulty gaining access to facilities where Chief Financial Officer related documents were being stored. Staff noticed this problem and brought it to the attention of a high-ranking Senator who then contacted the agency head. Voilà; full access was restored. As their most visible result, SARs can lead to Congressional hearings to heighten public awareness of an especially significant issue.

If, however, the SAR is presented with all the style and flair of the Code of Federal Regulations, it is doomed to be buried on a staffer's bookshelf, at best, or more likely, become fodder for the circular file.

Senator Glenn made it easy for staff who handled the IG bailiwick. He understood the statutory requirement that IGs report dually to their agency heads and Congress was unique in all of government. It offered Congress the chance to get an objective glimpse of



the state of the agency's program management, without the rosy tone sometimes supplied by their Congressional and Public Affairs shops. To achieve maximum potential, however, an SAR must be closely read and scrutinized. In some respects, it is akin to panning for gold nuggets. Many of our committee hearings resulted from issues first raised, in whole or in part, by SARs: Lax inventory controls at the Department of Defense, misuse of government furnished property by agency contractors, visa fraud at the State Department, NASA's lack of contractor oversight, Customs' mismanagement of asset forfeitures, the purchase and use of counterfeit and substandard parts in critical programs, and the unauthorized use of grant and contract funds. These are just but a few of the hearings where OIG involvement, whether through an SAR, a special investigation, or just an ordinary audit, was instrumental.

Committee hearings can also serve as a platform to address problems in the relationship between an IG and the agency head. Witness the recent Senate hearing highlighting the unfortunate situation at the Department of Housing and Urban Development (HUD). I also recall one of our Committee's hearings that revealed how employees and contractors of a major Cabinet agency had removed and shredded documents, literally moments before the OIG auditors arrived. Needless to say, Members on both sides of the aisle were not amused. Neither was the head of the agency when he had to offer profuse apologies to the Senators.

This article aims to help OIGs achieve maximum use of the SAR by Congressional Members and staff. I begin with one caveat, however. If OIGs rely on SARs as their sole means of communication with the Hill, they are already behind the proverbial eight ball. SARs must be supplemented by regular meetings with Hill staffers, especially to discuss recent or ongoing jobs of interest that may relate to a committee's legislative and oversight agenda. It is also a good idea to send summaries of OIG activities on a periodic basis to the authorizing, appropriations, and oversight

committee staff. They might not be read immediately or result in greater Congressional interest, but that is not the point. Hill staff do not appreciate being taken for granted, especially when an OIG they have not heard from, or seen, in months or even years—save only for the SAR—desperately needs their help.

What follows are some general thoughts and guidelines OIGs might want to consider so that SARs can receive the attention they deserve.

### Know Thy Audience

*(Or, if you have seen one SAR, have you seen them all?)*

Hill staff are notoriously harried and besieged. You can see that certain look in their eyes. They have many balls to juggle and keep in play. Each day staff receives hordes of new reports, whose ultimate fate is decided in a split second: to be discarded, filed for all eternity, or kept on the desk for follow-up. From discussions with other Congressional staff, Stephen King need not worry; SARs are no threat to any bestsellers' list. This is probably due to several different factors: confusing, overly-prescriptive, and statistically-driven statutory categories, dry writing styles with mind-numbing acronyms, and a rather staid and unintegrated approach. Most SARs do not readily lend themselves to easy reading.

### Use a broad, bold, and simple stroke

Paint the big picture. Congress has two main questions it expects SARs to address: 1) What are the major management problems within the Department; and, 2) Are IGs focusing their efforts on agency problems and programs where it matters the most?

The recent interest by House leaders for Inspectors General to provide "Top Ten" high-risk lists of major

agency issues flows from such considerations. It reflects the fact that readers often cannot discern from a SAR what these management challenges are. Thus, they resort to this type of special request.

In a similar vein, OIGs should not fear being bold and plain. Clearly state the issue up-front and out loud. Many SARs that came my way only alluded to significant issues in a rather cryptic, byzantine fashion. One needed to be an expert in hieroglyphics to fully grasp the underlying message.

We remember our shock when employees of the Internal Revenue Service were discovered to have browsed through tax returns of entertainers, athletes, and even their own neighbors. Senator Glenn's staff first became aware that this problem existed from a mere footnote referencing a regional audit by the Treasury OIG. After extensive hearings with national coverage, Congress eventually moved to outlaw this sort of "computer voyeurism."

The "big picture" should clearly highlight items of significance to Congress and the agency. Don't fuss with the minor details. If anyone on the Hill wants to pursue a particular matter, they will let an OIG know. There will be plenty of time to fill in the canvas.

## Relevance and Context

The SAR should note why Congress, and ultimately, the American taxpayers, should care if a particular program is not being properly managed. Has the program's integrity been compromised? How much money is being lost? Is there a risk or danger to public health, safety, or the environment? How vital is the program activity to the agency's mission?

The answers to these fundamental questions are not always easily found in SARs. Take time to read your own and put yourself in the shoes of a Hill staffer. Would you be able to pick out the main areas they should pursue?

While the six-month statutory requirement may help to focus OIG activities and serves a certain organizational purpose, it also makes time stand still. There is precious little continuity between SARs, no common thread to link the latest SAR with its predecessors. Nor is there any hint of what may come. What is past, at least in this case, is not always prologue.

Congress is also interested in knowing how long OIGs have raised concerns about particular programs and activities that have gone largely unheeded by the agency. How much money is involved on a cumulative or annual basis? How much might be "at risk?" Is there any danger to public health and safety? What have previous audits shown? These are key questions that transcend the six-month reporting regimen, but are vital in giving SARs some depth and perspective.

Two prominent examples suffice, although there have been others. The revelations on abuses in HUD's "Mod

Rehab" grants program caused a great hue-and-cry on the Hill and in the media over a decade ago. Members of Congress demanded to know why they had not been made aware of this scandal before it had happened. Where was the IG? Staff poured through the previous SARs and found that while references to mismanagement were, in fact, recounted, in the words of one Congressional staffer, however, "they always seemed to be buried on page 49."

Similarly, during Senate hearings on management problems at the IRS, one remembers the Senators' reaction when told by senior Treasury officials that several projects in the \$4 billion computer modernization program had just been cancelled due to operational difficulties, soaring costs, and poor management oversight. The Members pointedly asked staff: "How could we have spent hundreds of millions of dollars for failed projects? Isn't that what IGs are supposed to prevent?" Again, we reviewed several years of Treasury OIG SARs and found that, sure enough, while this had been referenced as an area of concern from time to time, it never jumped off the page.

The manner in which these deficiencies were described in the SARs also had diminished their effectiveness. The agency was usually given some credit for recognizing that problems existed and for taking corrective actions through reorganizations, new advisory boards, leadership changes, and the like. To Congressional staff, it appeared – at regular six-month intervals – that the agency was finally getting a handle on these problems. In a perfect world, staff would have time to compare the latest SAR with previous editions and get a clearer perspective on the nature and extent of challenges facing the agency. But, we all live with constraints. In these and other similar cases, it seemed that OIGs were trying to thread the needle between Congress and the agency head by saying just enough to cover themselves, but never too much that would get them in trouble. There is still a perception among Hill staff, rightly or wrongly, that OIGs tend to downplay the significance of particularly sensitive issues so as to not attract their attention – or raise the hackles of the agency. Obviously, such beliefs impact on an OIG's effectiveness and relationship with the Hill.

## Untying the Gordian Knot

Congress wants to know exactly what the agency has done to address outstanding matters and whether its actions have made a difference. The IG should present an unvarnished view, lay out current and previous OIG recommendations, and the status of corrective actions. The SAR should also identify any management or organizational barriers that inhibit the agency from implementing OIG recommendations. Most certainly, the IG should always be fair and give credit where it is due. But, IGs should also be able to state what factors, in their view, prevent these issues from being satisfactorily addressed.

Although this admission may lead some to question my sanity, I actually used to read the Audit Resolution section of each SAR. We followed-up with OIGs and the agencies on matters of special importance and ones taking years to be resolved. Again, look at the presentation of your Audit Resolution section. There is probably not much information that would enlighten a Congressional staffer as to what the issue is or its significance. Some of these decisions hold great consequence for how the agency spends tax dollars. These should be duly noted and explained. In my humble opinion, this section seemed to beg, but only inconspicuously, of course, for more Hill attention.

### **Investigations (Lawyers, Guns, and Money)**

I concede the fact that many Congressional staffers have no inkling as to what IG investigators do, how they do it, or the issues they confront. We, in the IG community, must do a better job of familiarizing Hill staff with the important contributions made to the integrity of government and law enforcement activities by our investigative teams.

An inherent drawback, surely, is the very timeliness of the material itself. That notwithstanding, we can do better. A question frequently asked was whether the matters uncovered by investigations were one-of-a-kind, isolated cases, or did they reflect larger and more systemic management deficiencies? For example, SARs are replete with cases involving contractor and grantee fraud. If there are patterns of fraud within the same program or agency activity, it certainly will be of some interest to the Hill. It is also helpful to know whether particular grantees or contractors were previously investigated for similar misuse of Federal funds, and the results. Ultimately, Congress wants to ascertain why some programs may be more vulnerable to fraud and abuse than others. What detection and prevention measures work, and which do not? Do these cases reflect a lack of qualified program managers, experienced contracting officers, internal controls, or is it a combination of factors? Moreover, if there is a way to better integrate the investigations side with program audits, especially for major program areas, it would be quite well received. Department of Health and Human Services is currently doing something along these lines with its Medicare “fraudigators” efforts.

### **A Sextant, if not a Compass**

Semiannual Reports should give some indication of not only where the OIG has been, but where it is headed. What is the game plan? What are the major upcoming audits and why are they being undertaken? Are there particular areas on which investigators are going to focus? Although not required by the Inspector General Act, this affords Congressional staff a “heads up” on what to expect that could be utilized in planning their legislative and oversight agenda.

Ask a Hill staffer the significance of the statutorily required SAR statistics and you will probably draw a blank. While these indicators do offer some ability to gauge performance, they unfortunately leave much to be desired. The different categories and definitions are not easily understood. What should be made of the fact that the number of OIG convictions are down but recoveries are up? Do fewer convictions mean an agency’s internal controls are tighter and therefore discourage contractor, grantee, or employee fraud waste and abuse? Or, is the OIG not looking in the right places? The bottom line is Members of Congress and staff want to know overall if the agency is getting better or worse at managing taxpayer funds. Qualitative improvements that have resulted in efficiency improvements or enhanced public safety and health protections, should also be noted. I realize that most OIGs are struggling to comply with GPRAs mandates but this is no bar, in the interim, of citing such successful endeavors.

### **Legislative and Regulatory Review**

This section, in my view, is the most intriguing, yet frustrating, portion of the SAR. It took some digging and persistence, but we were usually able to find glorious chestnuts. For instance, when Congress was considering certain block grant legislation, it was through a reference in this section that we were able to modify provisions on the Senate floor that would have made it more difficult to pursue and recover Federal funds misused by states and localities. On the regulatory side, we were first alerted to proposals that would have hindered OIG investigative efforts by allowing the agency the administrative flexibility to waive certain information requirements collected from its contractors and grantees.

OIGs should review this section to determine if more can be done to better reflect the kind of work and value which IGs bring to the legislative and regulatory process. This is also a chance for OIGs to go “on record” and alert Congress to proposals that may not necessarily protect the public exchequer.

### **Final Thought**

The SAR is a great opportunity for OIGs to present what they are doing, why they are doing it, and the benefits gained by public citizens. It should serve to both complement and stimulate Congressional interest in ongoing OIG initiatives. Important matters ought to be highlighted and flushed out. They should not be purposely downplayed or camouflaged. OIGs have a vital stake in making sure their SARs are accurate, candid, and comprehensive. Likewise, Congress has a responsibility to review the SARs in more than just a perfunctory manner and to ensure OIGs have the tools, access, and agency cooperation needed to accomplish the job. If we both do it right, everyone gains. 🏠



---

JAMES K. BLUBAUGH

*Assistant Inspector General, U.S. Dept of State*

## Got Any Change?

***Change is Difficult for Everyone. Here are Four Good Ways that the State Department's Office of Inspector General was able to Accomplish it.***

**A**n old Navy salt said it best—"The three scariest words in the English language are 'The Navy Way'." It's no different in the Army; the United States was the last industrialized country to give up its horse cavalry. Not to disparage our friends in the military, everyone has a tough time with change. If anything, the military is better at it than we civilians. We only have deadlines, not wars, to force us into action.

We are good at learning from others. So here are four practical examples that we've designed and implemented in the State Department's Office of Inspector General (OIG). They have helped us remedy four different problems which plague most organizations in Government today:

1. how to deal with a secretarial workforce that is increasingly underutilized and only marginally needed;
2. how to move people to those parts of the organization where they are needed the most today;
3. how to capture higher level managerial and professional skills which are critical for temporary projects or which were lost due to heavy retirement levels; and
4. how to coordinate resources throughout the organization to focus on the most important goals.

### **PROBLEM ONE**

*A secretarial workforce that is increasingly underutilized*

### **ANSWER**

*Paraprofessionals and templates*

Word processing and electronic files have made the traditional secretary position all but obsolete. Only the least demanding duties remain, and these can be filled at much lower rates of pay. So how do we deal with the talented secretary who has served for many years and is trapped in a job we no longer need? At the same time, how do we maintain the few basic functions we still require (primarily reception and correspondence quality control)?

Here's how. We started by identifying those duties being performed by middle managers which could be handled at a lower level. Foremost of these were editing (technical and substantive), maintenance of management information systems, graphic design, pre-survey information gathering, and administration. These functions were pulled together by office, and a new position description was written to cover them. By combing our processes to pull away enough of these "distracting" duties from the managers, we were able to create lower level paraprofessional (program analyst) positions for which our secretaries could apply. These new positions were usually at the GS-05/07/09 level, occasionally going as high as a GS-11.

These positions were then advertised with minimum qualifications set low enough so that most of our secretaries could compete for them. Conversely, the jobs had heavy training and skills requirements which had to be met before the new paraprofessionals could be promoted to the next grade. Most of the paraprofessionals were chosen at the GS-05 level, which meant that they had to drop back in grade in order to be given an opportunity to move forward.

The former secretaries selected for these new positions were looking for a new challenge. The secretaries not selected were reassigned to our most critical locations, which for many of them was a step up in hierarchy and challenge of work. The resulting vacant secretarial positions were abolished.

In order to ensure that correspondence coming forward for the IG's signature is prepared according to our requirements, templates were designed and placed on the computer word processing file. The templates not only preset style and format, but they provide helpful hints for preparation of the document. These templates have been a bonanza, shortening turnaround time and providing uniformity.

When the dust settled, we had abolished 17 secretarial positions. After adding in the cost of the new paraprofessionals, we still achieved a savings of nearly \$200,000 per year.

The end point is that most of our offices do not now have a secretary. In order to ensure that these remaining offices still have clerical help when needed, each paraprofessional is expected to provide as much as 20 percent of his/her time performing clerical support. This is usually more than enough to provide adequate phone coverage and assistance in such things as ordering supplies.

The individuals chosen for the paraprofessional positions have proven themselves to be highly motivated, and they have applied themselves to their new duties and to the training required with a renewed vigor. They are now performing those functions which truly make them crucial and indispensable, and for the first time in years, they feel like and act like they are critical members of the team. The managers who no longer have to perform basic editing and administration are the happiest of all.

## PROBLEM TWO

*Moving people to those parts of the organization where they are needed the most*

## ANSWER

*An annual rotation policy*

When we merged with the USIA's Office of Inspector General, we became the first OIG to cover four Federal agencies (State Department, U.S. Information Agency, Arms Control and Disarmament Agency, and Broadcasting Board

of Governors). The immediate problem we faced was an extreme case of poor distribution of employees. Duplicate management positions existed at all levels and too many auditors and investigators were lumped into areas where they were not needed.

All organizations have problems in assigning people where they are required most. Our

merger brought the problem to critical proportions. It forced us into more radical action. We needed to build, within the OIG, an integrated and interdisciplinary workforce with cross-cutting skills. A number of critical functions had to be staffed by moving people to them from areas where their skills were in surplus.

Our solution was an annual rotation exercise. The first rotation opportunity took place a few weeks after the merger occurred. During a three-week period, employees could "bid" on any job in the organization for which they were qualified. They also could be more general and request an area elsewhere in the OIG where they would like to be transferred.

We were surprised when 25 percent of our employees participated in the first exercise, but we succeeded in ensuring that 90 percent of them received their first or second choice. Now that the program is fully established, it appears to be stabilizing at lower levels. During our most recent



rotation exercise, 10 percent of our employees participated and half of them received their first or second choice.

The rotation exercise is a supplement to normal competitive selection processes, not a replacement for them. While it is only one of several mechanisms for providing employees with the skills necessary to successfully meet the challenges of a multidisciplinary work environment, it provides participants with a broader perspective of the working environment, enhances promotion opportunities and, at the same time, provides each office with the talent most necessary to tackle and resolve increasingly complex problems.

What did it do for us? We have a better trained work force, fewer areas of critical need, and, as a bonus, we have happier employees.

### PROBLEM THREE

*Capturing higher level managerial and professional skills which are critical for temporary projects or which were lost due to heavy retirement levels*

### ANSWER

*Fast-track contracting*

When it comes to change, the Government is at a disadvantage. Our employees are hired for the long term, selected for skills which will benefit us in performing our required duties. Unlike the private sector, it is difficult for us to identify and hire temporary employees or contractors in time to meet our special needs. It is unrealistic to expect that our staff of generalists will always have the array of detailed skills which are needed only occasionally. For example, when we inspected our medical bureau, we required the services of at least two highly regarded medical professionals with no ties to the State Department. Due to the time it took to find them, recruit them, and complete the paperwork, we couldn't get them on board in time to help us.

The problem is exacerbated now that such a large percentage of our most senior employees have retired. They took with them their experience, their expertise, and their institutional memory. It is understandable that, after 30 years or more of Federal service, these former employees are not immediately replaceable. We will eventually train others, but how do we recapture that lost expertise in the meantime?

The solution was to develop a contracting mechanism that could react quickly and broadly to a wide range of needs. We did it by taking advantage of changes in technology and by predefining scopes of work, job duties and skills.

Contracting is usually a lengthy and expensive way to acquire talent. But the alternatives are often not better, and certainly not efficient. We have been using a complex system of retired foreign service officers on a WAE (when

actually employed) appointment. This system is cumbersome—we keep nearly 100 temporary people on the OIG rolls alone in order to meet all the expertise needs of reviewing our four agencies. It is costly—we pay a range of employee benefits, must renew appointments every 90 days, must maintain and sign time and attendance records for all of the employees whether they work or not, and must expend our FTE on them. There is a shortage of these workers, such that bureaus in the Department are constantly “borrowing” staff from each other. It locks us into pre-established salary rates, regardless of the work assigned. There are income limitations which are mandated by law and which must be handled and monitored. Finally, it locks us into a small elite corps of foreign affairs specialists, which forces us to choose not what we need, but the closest fit. In other words, if all you have is a hammer ...

After a year of working with lawyers and contracting officers, the Department now has an indefinite quantity of contracts with a firm specializing in both Personnel and ADP services. We defined a number of labor categories (e.g., three different levels of Program and Management Analyst, two levels of Intelligence Analyst, a Network Administrator, and several others) which included the expertise required, the deliverable expected, and the duties to be performed. Additional labor categories can be easily added as needed.

To get contractor help, it is only necessary now to call up the vendor via modem and click on the labor category that is wanted. Once the category is chosen, a second screen appears detailing a list of skills needed (such as visa fraud or narcotics expertise). The manager will typically identify 2-4 skills. This information is entered, the vendor replies within minutes with the names and background of those individuals who possess the background and skills, and the manager selects.

Although the process has a high degree of electronic automation, the contractor is always to be available on a personal basis to discuss a task order or assignment.

Because the scope of work, job duties, deliverables and skills are all predefined, the Government manager need identify only the title, timing and location of the job to be performed and any special considerations. The time it takes to acquire contractor assistance is now a small fraction of what it used to be.

The contract gives the OIG an enhanced capability to handle unplanned reviews, provide special expertise to our inspection and audit teams, bring in specialists (disarmament experts, refugee specialists, statisticians, methodology experts) to provide on-call advice, handle large one-time efforts, and manage around attrition problems.

The contract allows any office in the Department to acquire staff at lower rates than through the WAE process by specifically tailoring the grade to the job. Presently, if the WAE officer is a GS-15/10, he/she is paid at that rate

regardless of the work. Every office in the State Department is able to use the contract to meet special or temporary needs; access to a temporary workforce is no longer a tool available only to the foreign service aspects of our work. The contract permits offices to use multi-functional teams without disrupting the work of other units. By more properly aligning hourly rates to the job at hand, a contractor can provide the services at lesser cost.

Now, finally, we have open to us the same option which is available to every American private sector firm—the ability to acquire talent from the entire labor pool.

#### **PROBLEM FOUR**

*Coordinating resources throughout the organization to focus on the most important goals*

#### **ANSWER**

*Core groups*

This is our newest venture. In simple terminology, it is nothing more than “keeping our eye on the prize.” Like any complex organization, the OIG sometimes finds it difficult to deliver its product in the most efficient and effective way. For example, within a brief period of time, we might have 1) an audit being conducted on the use of aircraft for counternarcotics, 2) a series of inspections in countries where counternarcotics are a major U.S. policy priority, and 3) a review of law enforcement coordination overseas, including in the narcotics area. When completed, each piece will stand on its own as a valuable study, but unfortunately nowhere will we have a complete coordinated picture of counternarcotics efforts in the Department.

To overcome this deficiency, a core group concept was developed to get us beyond seeing only the snapshot and into viewing the big picture. Core groups are led by one of

our most senior officers and bring together employees from throughout the OIG, each with different skills. Each core group focuses on one of the five strategic goals of the OIG. They meet as a unit and plan the work that needs to be accomplished in order to meet their particular strategic goal.

The core group plans, tasks, assigns resources, monitors progress, and contributes to the appraisal of individuals assigned to it. The core groups have been given the authority to accomplish their mission, and to make those changes in work processes and policies that will enable them to accomplish that mission. The concept behind the group is to bring the full range of OIG skills and expertise to bear in addressing problem areas in a coordinated fashion, rather than reviewing issues in isolation.

At this point, while we still expect most of the OIG work to be handled by existing offices and divisions, various methods are being tested to determine how the traditional offices will work with and respond to the core groups. One way is for the core groups to “contract” with each office’s management to do specific tasks. The core groups allow us to eliminate hindrances, provide products more quickly, and produce results, without any additional management layers.

**THESE FOUR NEW OPERATIONAL METHODS** are working for the OIG. They cost next to nothing to implement (other than the stress that comes with any change). They have been well received by both management and staff. The improvements these operational changes have brought in efficiency, effectiveness and staff morale have been dramatic. And just like loose change, they are there for others to pick up and use.

By the way, if you improve on them, give us a call and tell us what you did. We’re always interested in finding a better way. 🏠

# Rethinking Leadership

*Too few leaders understand the depth of our craving to be part of something larger and to do jobs with meaning.*

OUR ORGANIZATIONAL mythology is out of sync with our reality. We cling to the myth of the omnipotent leader, the larger-than-life individual who can solve every institutional problem, however daunting. We continue to believe in the CEO as corporate Hercules, even as we read cautionary tales almost daily of once-lionized leaders who have failed spectacularly and been replaced after briefer and briefer tenures by angry boards.

Yet all of us who work in business, industry, education, or government observe it and know that, in terms of the organization, the Lone Ranger is dead. The world in which an individual leader, however gifted, however tireless, can save an enterprise single-handedly no longer exists. I suspect that the notion that great institutions are lengthened shadows of individuals has always been an exaggeration, if not a lie—a reflection of our romantic yearning for gods and heroes.

But the problems and challenges of corporate life today dwarf any individual, even those as wildly successful as Walt Disney Co.'s Michael Eisner or Microsoft Corp.'s Bill Gates. In a world of increasing globalization and ever accelerating change, even great leaders are not enough. We need both Great Groups and great leaders, even teams of leaders, if only because—as one wise observer of humanity expressed it, “None of us is as smart as all of us.”

To a large degree, our growing recognition of the need for a new, more collaborative form of leadership results from the emergence of intellectual capital as the most important element in organizational success. In the winning enterprises of an earlier time, the leader could control all the assets. But today's most successful companies live and die according to the quality of their ideas. And ideas are different from equipment and other physical assets. Ideas are like butterflies—wonderful but elusive. Moreover, the people at the top of the chart have no lock on them. Great ideas can come from anywhere in the enterprise, and they inevitably shift power to those who have them.

Recently, co-author Patricia Ward Biederman and I studied seven extraordinarily successful collaborations for our book, *Organizing Genius*. These Great Groups, as we called them, had each changed the world in some significant way. Each had made what Steve Jobs liked to call “a dent in the universe.” Disney Feature Animation had created a new art form with *Snow White and the Seven Dwarfs*. Xerox Corp.'s Palo Alto Research Center (PARC) and Jobs' Macintosh team at Apple Computer had created the first user-friendly computer. The Manhattan Project had made the atomic bomb, a gadget, as the

team called it, that unquestionably changed the world, for better and for worse.

We found that all seven of our Great Groups had important commonalities. Each believed it was on a mission from God. Each was filled with greatly gifted people who wanted to be working on their particular project more than anything else in the world. Each was made up of sometimes delusional optimists—people who didn't know the meaning of the word "impossible." Each group believed it was involved in a mortal struggle against a Goliath-like enemy (the Axis powers in the case of the Manhattan Project, IBM for the makers of the Macintosh). Each had become a world unto itself, a place with its own language, jokes, rituals, and, in the case of Apple, its own T-shirts. And, perhaps most telling, each was filled with people having fun.

We also found in these Great Groups a new paradigm for achieving great things—one in which a great leader or leaders devote themselves to unleashing the genius of their colleagues. Let me emphasize that none of these was a leaderless team. Instead, they constitute a new kind of organization, teams in which each member of the group, including the leader, is needed to create the collective magic.

Whenever I talk about creative collaboration, I find the audience has the same response. They are both exhilarated at the thought of being part of a Great Group and depressed that their own groups fall so short of the mark. It is no accident that the walls of so many of today's workplaces are decorated with the cynical (albeit hilarious) musings of industry Everyman Dilbert. Too many modern workers regard themselves as wage slaves, and too many workplaces appear to be places of pain, not passion, peopled by individuals who see themselves as underutilized and undervalued.

How can we change that and turn every group into a great one? First, we have to take a page from the book of the inventors of the PC and other extraordinary innovators and believe that it can be done. Great Groups always have godlike aspirations. Alan Kay, one of the scientists at PARC, "dealing lightning with both hands," recalls that he and his colleagues wanted to achieve far more than they actually did. He, for instance, was trying to develop a laptop computer easy enough for a child to use, more than 20 years before such devices were first produced commercially. Greatness is impossible without willingness to take epic risks or, as hockey great Wayne Gretzky reminds, "You miss 100 percent of the shots you don't take."

There is a compelling reason for learning the secrets of these extraordinary groups. I am convinced that the key to competitive advantage into the next century will be the capacity of leadership to create the social architecture that generates intellectual capital. Success will belong to those who unfetter greatness within their organizations and find ways to keep it there.

Others obviously think so, too, as evidenced by the increasing number of companies that are building education

into their programs. Andersen Consulting now spends 6 percent of its annual revenue on education, requiring every professional employee to take at least 130 hours of training. Intel Corporation spends \$3,500 per person per year on education. General Motors and others have named vice presidents for knowledge services. This institutionalization of education is not some fringe, feel-good benefit. It is tangible recognition that education gives the biggest bang for the corporate buck. According to a recent study conducted by the University of Pennsylvania, companies that invest 10 percent more in education see an 8 percent increase in productivity. Upping capital expenditures by 10 percent boosts productivity by only 3 percent.

But a creative, well-educated workforce is not the only ingredient in a Great Group. Leadership is also a crucial element. I have always believed that leadership is, above all, a question of character. Ironically, character is always the last criterion used to evaluate corporate leaders, who are

**A key attribute of this new kind of leader is the ability to generate and sustain trust. Largely as a result of downsizing, the level of trust in the workplace is at its lowest ebb ever.**

usually judged on such relatively easy-to-assess but far less important criteria as technical competence, people skills, track record, taste, and judgment. The question of character is more important than ever in the age of information. Today's leaders must not only have the stature to attract top talent—they must have the kind of character that

retains it. Talented people have options. They can walk out the door at any time—to go to a competitor, to become a competitor. In this environment leaders don't automatically command respect. They have to earn it.

A key attribute of this new kind of leader is the ability to generate and sustain trust. Largely as a result of downsizing, the level of trust in the workplace is at its lowest ebb ever. Terrible alienation exists in today's plants and offices, with corporate leaders tending to regard employees not as the company's treasure, but as a fiscal liability and employees feeling the hopelessness of poet John Milton's Samson, "eyeless in Gaza, at the mill with slaves."

The only great work being done in many businesses today is that of entrepreneurial individuals who are using their employers' fax machines and other resources to craft their next job—a high anxiety activity that has been dubbed "wing-walking." Only a leader who inspires trust can get such workers off the wine and focused on the task that the organization deems important. Such a leader sends the message that "We are all in this together."

One way true leaders accomplish this is by imbuing work with meaning. The late Richard Feynman, the irrepressible Nobel Prize-winning physicist, used to tell a wonderful story that illustrates how profoundly meaning can transform work.

Among Feynman's tasks during the Manhattan Project was supervising a group of technicians who had been brought to Los Alamos, NM, from all over the country to do calculations on primitive computers. The work involved doing energy calculations and other tasks crucial to the success of the project, but, unlike Feynman and the other physicists, the technicians were kept in the dark about the true nature of the project or even what their calculations meant. They did what they were ordered to do—process one number after another—but they did it slowly and badly. And then Feynman prevailed on his superiors to lift the veil of secrecy. J. Robert Oppenheimer talked to the technicians, explaining how important it was to build the bomb before the enemy did and their vital role in that effort.

As a result, the men were completely transformed. They found new, better ways of doing the work. They invented new programs. They worked through the night. Ever precise, Feynman determined that the group worked nearly 10 times as fast after the task had been imbued with meaning.

Great leaders can bring about that kind of transformation. They have a vision, and they have the ability to articulate that vision in a way that makes other people want to sign up, too. Oppenheimer had that talent, but so do the best corporate leaders today. Sears, Roebuck & Co. CEO Arthur Martinez has transformed that once-failing retail giant by persuading employees that they are a crucial part, not of a mundane comeback effort, but of one of the greatest adventures in business history. CEO Herb Kelleher has made Southwest Airlines, wildly successful by enlisting employees on a crusade, not to sell bargain airline tickets, but to give everyone a precious gift—the freedom of travel.

Knowing that people would rather be on a crusade than simply at work is one of the gifts of the kind of leader who creates and sustains a Great Group. The ability to enlist others is not some simple rhetorical trick. If it were, the bland mission statements cranked out by most corporations would actually inspire workers, instead of infuriating them, as they typically do. The ability to inspire reflects a pro-

found understanding of human nature. People want to do good work. They want the hours they spend in the workplace to mean something more than the sum of the objects they produce.

When I think about leaders of truly Great Groups, such as Bob Taylor at PARC, I'm reminded of the story about Queen Victoria's two great prime ministers, William Gladstone and Benjamin Disraeli. Someone once observed that when you had dinner with Gladstone, you came away thinking he was the wittiest, most intelligent, most charming person you had ever met. When you dined with Disraeli, you were sure you were the wittiest, most intelligent, most charming person ever. Leaders in the tradition of Disraeli, Oppenheimer, and Taylor allow their groups to become great, and they also find their own greatness in the group.

Such leaders have contagious optimism. They make employees feel that they can accomplish anything. They also understand the truth of playwright Noel Coward's observation that "work can be more fun than fun." The workplaces they create are productive because they are filled with people who are enjoying the intrinsic rewards of working well. We love to problem solve. It's the task we evolved for. We especially love to do it in partnership with others whom we respect.

The longing for community is born in us. Too few corporate leaders understand the depth of our craving to be part of something larger, and even fewer understand how to tap that longing to turn individual workers into a cohesive, productive group. And yet it is only in such groups that the increasingly complex work of the modern corporation can be accomplished. Allowed to flourish, people spark greatness in each other. As Italian author Luciano De Crescenzo said so beautifully, "We are all angels with only one wing. We can only fly while embracing each other." 🦋

Warren Bennis is a distinguished and founding Chairman of the Leadership Institute at the University of Southern California's Marshall School of Business and co-author of *Organizing Genius* 213-740-0766.

*Reprinted with permission from the Executive Excellence February 1998 issue.*





---

KELLY A. SISARIO

*Inspector General, National Archives and Records Administration*

# Who Reads the Journal of Public Inquiry??

*Lots of People!!*



Kelly A. Sisario

Just a few years ago, a small group from the Inspector General community decided to produce a publication which we all now know as *The Journal of Public Inquiry*. While the original audience for the Journal was the Inspector General community, the publication was well received and distribution grew to include Congressional Offices, Assistant United States Attorneys, FBI Special Agents-in-Charge, and some educational institutions. Now, over 2,500 copies of the Journal are printed for distribution.

This year, we confirmed that there is another audience which has access to the Journal through the Federal Depository Library Program (FDLP). Whenever the government produces a publication which is of general interest to the public, that publication is placed on a list and made available to libraries through the FDLP. Under this program, the Government Printing Office (GPO) provides the selected government information products, at no cost, to designated depository libraries throughout the country. From a large inventory, each library selects the government publications they want to have available at their facility. These depository libraries, in turn, provide local, no-fee access to the public.

Federal depository libraries are located in nearly every congressional district throughout the United States and its territories. Currently, there are 1,363 depository libraries in the program, categorized as follows:

General Academic Libraries	50%
Public Libraries	20%
Academic Law Libraries	11%
Community College Libraries	5%
State and Special Libraries	5%
Federal and State Court Libraries	5%
Federal Agency Libraries	4%

I recently met with Ms. Robin Haun-Mohamed, Director of the FDLP. She explained that the GPO staff considers demand to be very high when a publication is requested by 600 to 700 libraries. Currently, 1,062 libraries are selecting the *Journal of Public Inquiry*. This is a significant number and demonstrates the broad interest in our publication. Congratulations to the staff and contributors of the Journal!!

