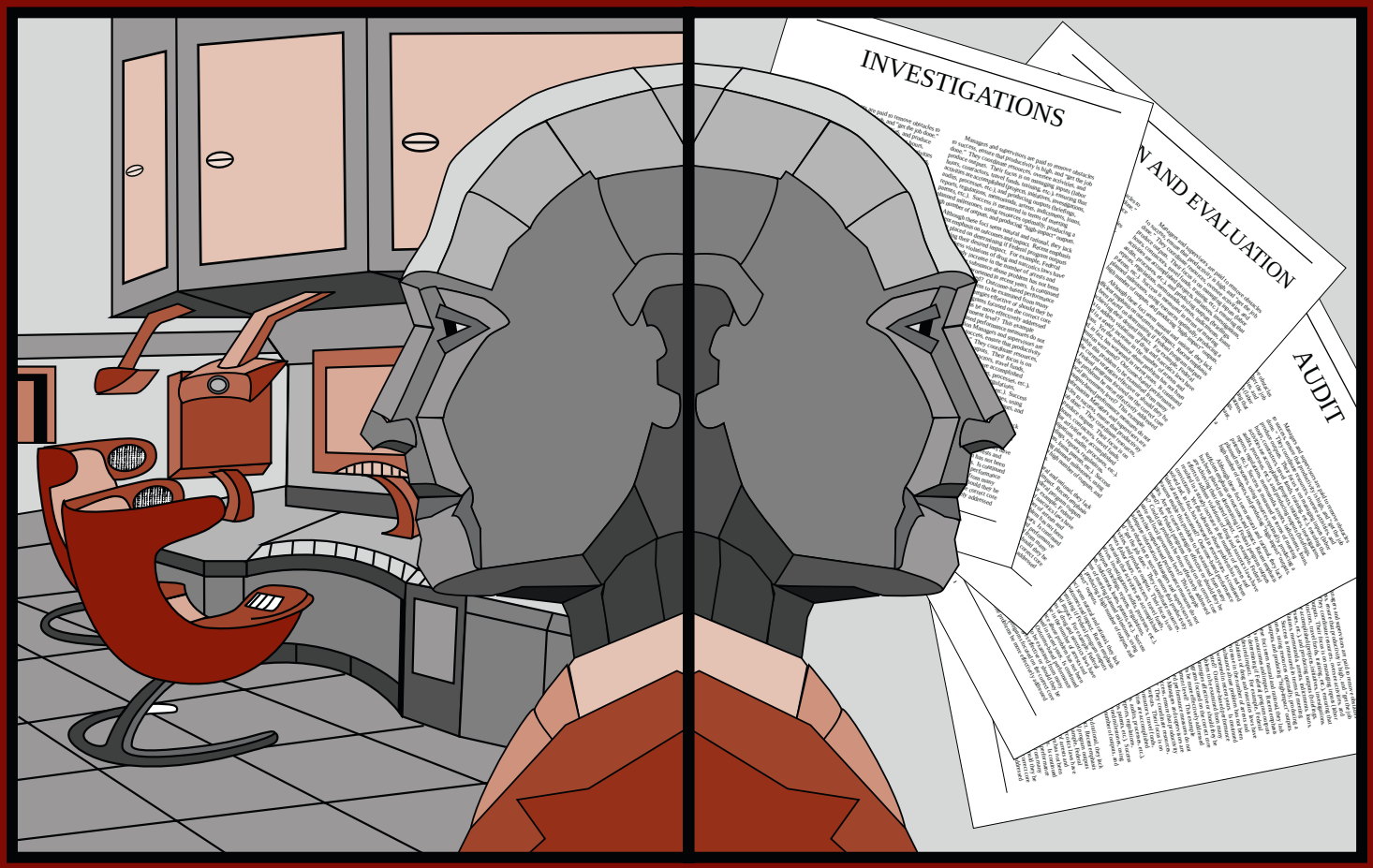
The JOURNAL OF PUBLIC INQUIRY

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES



A Forward Look...

FALL/WINTER 1997

The Journal of Public Inquiry

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, Social Security Administration OIG
Wendy Zenker, Office of Management and Budget

Staff

Editor

David C. Williams, Social Security Administration OIG

Editorial Services

Karen M. Shaffer, Social Security Administration OIG
Agapi Doulaveris, Social Security Administration OIG

Printing

Frederick Watson, Department of Defense OIG

Public Affairs

Robert S. Terjesen, Department of State OIG

Design & Layout

Automated Graphic Services, Nuclear Regulatory Commission 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, Social Security Administration, Altmeyer Building, Suite 300, 6401 Security Blvd., Baltimore, MD 21235.

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.

The JOURNAL OF PUBLIC INQUIRY

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

Table of Contents

IG Gate – Investigating Major Scandals:

The role of the Inspector General (IG) has evolved in a variety of ways over the past 20 years. Although the media has focused on the Independent Counsel's role in investigating major scandals, IGs are playing an expansive and important part in these cases.

Part II: The Nuts and Bolts

by Michael R. Bromwich and Glenn A. Fine

In the following article, the second of a two-part series, the authors discuss the dynamics and mechanics of conducting major scandal investigations.

Michael R. Bromwich, Inspector General, Department of Justice

Glenn A. Fine, Director of Special Investigations and Review Unit, Office of the Inspector General, Department of Justice

Over and above the normal investigations, audits and inspections undertaken by the Department of Justice's (DOJ) Office of the Inspector General (OIG), we have been called upon over the last 2 years to undertake an increasing number of special investigations. These investigations have arisen largely in response to particularly serious allegations that gained the attention of top DOJ officials, Congress, the media, and the public. Within our office, we refer to these high-profile major investigations as special investigations, or "specials." By this label, we do not mean they are more important than the core matters our divisions handle every day. Rather, we recognize that these investigations require particular attention because they typically last longer, involve complicated issues, demand more resources, and command greater public attention.

Over the last 2 years, we have conducted eight special investigations:

1. *The DOJ's Handling of Reports of Certain Violent Crimes in Guatemala.* This classified review was conducted at the request of the congressional intelligence committees and the President's Intelligence Oversight Board. We examined what DOJ employees knew and did regarding certain highly publicized crimes against United States citizens in Guatemala, including the murder of innkeeper Michael Devine. Our review was in coordination with related reviews conducted by the IGs of the Central Intelligence Agency (CIA), the Department of State, and the Department of Defense (DOD).

2. *Allegations of Racial and Criminal Misconduct at the Good Ol' Boy Roundup.* This review involved investigating allegations made public in June 1995 that Federal law enforcement officers participated in racist, criminal, and other kinds of misconduct at annual gatherings in Tennessee known as the Good Ol' Boy Roundup. The Department of the Treasury OIG performed a similar review. We conducted an intensive investigation of these allegations, eventually interviewing over 500 witnesses and writing a 220-page report that reconstructed the events at the Roundup over a 15-year period.

3. *The Alleged Deception of Congress: The Congressional Task Force on Immigration Reform's Fact-finding Visit to the Miami District of INS in June 1995.* We investigated allegations that senior Immigration and Naturalization Service (INS) officials had deliberately deceived a delegation from the Congressional Task Force when it reviewed INS operations at Miami International Airport and the Krome

(continued on page 2)

detention facility in June 1995. The allegations included charges that, just before the delegation arrived, aliens were moved out of secured areas, transferred to other facilities, sent on bus trips for the day, or released. After interviewing more than 450 individuals, we issued a 196-page report substantiating that INS management in Miami intentionally misled the visiting congressional delegation.

4. *The DOJ's Response to the Zona Rosa Murders*. In 1996, at the request of the Senate Select Committee on Intelligence, we examined the actions of DOJ employees in response to the 1985 murders of four United States Marines and two other United States citizens in the Zona Rosa district in San Salvador, El Salvador. Our review was part of a Government-wide inquiry conducted in coordination with the IGs of the CIA, DOD, and the Department of State.

5. *The Federal Bureau of Investigation (FBI) Laboratory: An Investigation into Laboratory Practices and Alleged Misconduct in Explosives-Related and Other Cases.* We investigated allegations of impropriety and faulty forensics in certain sections of the FBI Laboratory, primarily relating to bombings and explosives cases. Our review, involving some of DOJ's most significant prosecutions, was assisted by a panel of five internationally respected scientists with expertise in the operation of scientific laboratories.

6. *A Review of the FBI's Performance in the Identification and Apprehension of Aldrich Ames.* Initiated in response to a request from the House Permanent Select Committee on Intelligence, this classified report evaluated the FBI's response to the loss of those intelligence assets caused by the espionage of Aldrich Ames.

7. We are currently conducting a review of Operation Gatekeeper, a major INS initiative designed to stem the flow of illegal immigration from Mexico into the United States along the San Diego border. Among other allegations, we are investigating whether INS employees were ordered to falsify and alter reports to ensure that Operation Gatekeeper appeared successful.

8. We are currently conducting a review of allegations that in the 1980s the CIA was involved in the importation of crack cocaine into the United States by supporters of the Nicaraguan Contras. In coordination with the CIA IG, we are examining what DOJ officials knew and did regarding these allegations.

Each of these reviews has involved different issues and presented distinct challenges. However, in the course of handling them, we have learned certain lessons from our mistakes and successes. And each has taught us valuable lessons about how to conduct large-scale special investigations. What follows are some general observations about the procedures and techniques we have used to conduct these large-scale, special investigations.

Staffing and Supervision

The initial and perhaps most difficult task is the selection of the team to conduct the investigation. The selection of a team leader or leaders is critical. We have found that in a department run by lawyers, it is desirable for at least one of the team leaders to be a lawyer. These investigations often require the rendering of difficult legal judgments. For example, in the Zona Rosa review, we had to assess the thorny legal questions about whether prosecutors had sufficient admissible evidence to bring a case against the alleged perpetrators of the murders. In the FBI Laboratory review, we evaluated difficult issues concerning the appropriate standards for reporting the results of forensic examinations. In the Guatemala review, we addressed the potential application of the terrorism statute to the facts known to the prosecutors. Our ability to conduct these inquiries and render the difficult judgments that they called for was aided by having lawyers who were experienced investigators and prosecutors in critical positions on the investigative team.

To lead these special investigations, we have assigned Special Investigative Counsel from our Special Investigations and Review Unit (SIRU) or Assistant United States Attorneys (AUSAs) detailed to the OIG. Reflecting the importance we place on these special investigations, SIRU is located within the front office of the OIG and reports directly to the IG. In some cases, the special investigations have been jointly led by attorneys and senior investigators from our Investigations Division. In the Miami INS review, for example, the team was led by an AUSA detailed to the OIG from the United States Attorney's Office, Southern District of New York, and by the then-Assistant Special Agent-in-Charge (ASAC) of our Washington, D.C. Investigations Field Office. This ASAC had extensive experience in investigations involving INS practice and procedures, which was invaluable to the review.

The resources necessary to staff these projects adequately have placed enormous strains on our other important functions. The number of people assigned to these "specials" ranged from approximately four in the Zona Rosa review to 15 full-time on the Miami INS review. To select the investigators who will serve as the investigative backbone of these efforts, we have relied on the Assistant Inspector General in charge of the Investigations Division. He has demonstrated his commitment to the success of these special investigations by recruiting some of his most outstanding agents, regardless of whether their assignment to the investigation might create hardships in specific field offices and in the Division generally. In general, the agents recruited for the investigative teams have extensive experience in handling both criminal and administrative matters within DOJ. Because continuity is so important on these special investigations, the agents are normally assigned to the special investigation for the duration of the project, reporting directly to the team leaders.

We also include on the investigative teams top personnel from our Audit and Inspections Divisions, who bring distinctive skills and techniques to the projects. For example, in the Miami INS review, auditors thoroughly examined historical INS data to determine whether the pattern of release of detainees from the Miami INS facilities just before the visit of the congressional delegation was inconsistent with normal practice. This painstaking review, examining raw data rather than the summaries provided to us from the INS, demonstrated that the INS had substan-

tially deviated from its normal practice. In the Good Ol' Boy review, inspectors conducted an important telephone survey of people who had attended one or more Roundups to determine whether they had any information concerning the allegations of misconduct.

When appropriate, we have reached outside our office for qualified personnel to work on the specials. Because the FBI Laboratory review involved highly technical scientific analysis, we assembled a team of renowned forensic scientists from around the world to assist our lawyers and investigators. The commitment of time they gave and the magnitude of their contribution substantially exceeded our expectations. They attended many of the interviews of Laboratory examiners, took an active role in questioning many of these witnesses, and participated fully in the preparation and review of our final report. In the Ames review, several FBI agents who had extensive experience in counterintelligence matters (but who had no involvement with the Ames case) were detailed to our team. They provided valuable guidance and insight into the often arcane world of foreign counterintelligence. In each of these reviews, however, we made clear from the outset that the team members reported to the team leader and to me, not to their normal supervisors or agencies.

These specials were supervised directly by me and the front office of the Inspector General, rather than in one of our regular units. I along with my immediate staff--the Deputy Inspector General, the Director of SIRU, and my counselor--were closely involved in monitoring and overseeing these reviews. In supervising these matters, I was regularly briefed on their progress at regular intervals. For example, in the Good Ol' Boy investigation, I met every week with the team leader and team members to learn about the status of the investigation and to address any problems that developed. In the Gatekeeper review, which is based in San Diego, I schedule a conference call with the team once a week. In the FBI Laboratory review, at critical times we assembled the lawyers, scientists, and investigators to review the progress of the investigation.

Investigative Steps

The initial step in these special investigations has been the difficult and unglamourous task of obtaining and managing the vast quantity of relevant documents. We cannot overemphasize the importance of this step, and its impact on the success of the projects. In most of these reviews, we sent broad document requests to all DOJ components and offices that might have relevant documents. We initially asked each component to identify and secure any documents responsive to the request and to designate a responsible official to ensure a timely and complete response to the request. When we learned the scope and general substance of the documents, we made arrangements to obtain those we deemed relevant.

Rarely did we get from every component all the relevant documents on the initial request. We often went back again and again to the responsible officials, clarifying how they searched for documents, seeking more documents, ascertaining the component's document retention practices, and ensuring that all those within the component who might have relevant documents responded to the request. In the FBI, for example, the Office of General Counsel plays an invaluable role in identifying and locating critical documents within the FBI and securing them for us. In some components, the internal inspections divisions, such as the Drug Enforcement Administration's Inspections Division, perform this useful role.

To obtain documents from Government agencies outside DOJ, we have had good success working through other IGs. For example, in the Guatemala, Zona Rosa, and Contra-cocaine reviews, we have sought critical documents from the CIA's Directorate of Operations. The CIA IG was instrumental in identifying and obtaining those documents for us, despite initial opposition from elsewhere within the CIA to providing these documents to an outside entity. When necessary, we have received support from the Attorney General and the Deputy Attorney General in obtaining necessary materials.

Organizing the mass of documents we obtain is vital to the orderly progression of our investigations. We have found it useful to designate an executive officer in charge of the documents. That person is responsible for logging in all documents by source and date of receipt, "Bates" stamping each page with an identification number, and organizing the documents in files. In the FBI Laboratory review, a member of our Inspections Division oversaw this critical task and ensured that the key documents were provided to the lawyers and scientists who needed to see them. The job was particularly difficult and critical because at various phases of the inquiry our lawyers were in Chicago, Phoenix, and Seattle, and our scientists were in Virginia, New Mexico, Canada, and Northern Ireland. The executive officer became the nerve center for the entire effort.

In several of the "specials," we created computerized data bases to facilitate use of the documents. For example, in the Good Ol' Boy review, personnel from our Audit Division created a data base that included the Bates number of each document, its date, and some information regarding its content. Before interviews of any witness, the data base could be searched for all documents with information relevant to the person being interviewed. The data base was also critical in the report-writing phase of the investigation, where detailed information on individual misconduct at each Roundup or each incident of misconduct could be retrieved. In this review, we also created a data file for each person we identified as having attended one or more Roundups, whether that person had been interviewed, and other pertinent information relating to that person. This system was critical in managing and tracking the 500 interviews that were conducted.

In the Miami INS, the Good Ol' Boy, and the Gatekeeper reviews, we conducted large numbers of interviews of line personnel to determine whether they had any information on the core allegations. For these

(continued on page 4)

interviews, we developed standardized questions for our investigators. Each interview was different, however, and the investigators used the standardized questions as a checklist to make sure they covered the basic topics, rather than as a script to which they became slaves.

In every interview, we consistently try to have at least two team members present. After an interview, one of the team members is responsible for drafting a Memorandum of Interview (MOI), which the team leader reviews before it is finalized. In several of the specials, we created computerized data bases containing all the MOIs. As a result, any team member could search the contents of other MOIs for information. For example, the MOIs could be searched for references to particular people or incidents that were relevant to an interview. In addition, when an investigator was traveling and needed to access information from an MOI, the investigator could search the computerized data base remotely.

For a small number of interviews of key witnesses, we either tape record or arrange for a court reporter to be present at the interview. In the FBI Laboratory review, for example, the interviews of key Laboratory examiners were recorded and transcribed so that the scientists who were not present at the interviews could review exactly what the witnesses had said.

Report Writing and Distribution

There is no magic to the tedious and difficult process of synthesizing masses of information into a coherent, readable report. We have found it helpful to review the report-writing in stages, first in outline, then in draft, and then in final form. Members of my front office and I try to review each stage of the report-writing process carefully, from the outline phase to the draft to the final product.

We strive in all of our reports to make sure they are free from any factual errors. To ensure this, we have in certain cases sent the draft report to key individuals or components to review for any factual inaccuracies contained in the draft report. We give these reviewers a very short turnaround time and discourage arguments about the conclusions reached or judgments rendered in the report. Rather, we ask whether anything we have written is factually incorrect. Very few factual inaccuracies have been brought to our attention as a result of this process.

The reports have generated significant interest from Congress and the public. Prior to the completion of our reports, we have sought to keep authorized oversight committees apprised of the status and progress of our investigations, while steering clear of providing conclusions that might still be subject to change. Once the reports are complete, we provide them to the oversight committees, with an offer to brief members and staff on our findings and conclusions.

Conclusion

Special investigations present special challenges and opportunities for IGs. Because the level of public, media, and congressional scrutiny given to these efforts is so high, they play a significant role in shaping the reputation of an OIG. And in an era in which we all fight for the resources we need to do our jobs, they may play a disproportionate role in determining the level of appropriations Congress approves. The techniques we have developed in staffing special investigations, gathering relevant evidence, conducting interviews, and preparing our reports have given us confidence that we can meet even the most difficult and complex investigative challenges and produce authoritative reports that generally command respect even from demanding congressional and media audiences.❑

Postcards from the Edge: IGs' Predictions of the Future of the Offices of Inspector General

Introduction by David C. Williams

David C. Williams,
Inspector General,
Social Security Administration

When I think of the future and what it will bring to our community, I imagine Government being substantially more interesting, in a world!illed with increasing risks. I see the community making choices that will either make us vital guides and guardians or obscure observers. Our investigators will keep pace with change and protect vital Government services. Our auditors and inspectors will inform the great debates and develop insightful and innovative designs for efficient and effective governance. Or they won't.

I can easily imagine some landscape features before us. Straight, clear pathways lead to them from where we presently stand. Other features are more blurred with their hopes and their dangers masked. Certainly the easiest feature of the landscape to identify is cheap, plentiful. . .and vulnerable communications and electronic services.

The Information Age is opening enticing frontiers to us, immersing us in vast amounts of knowledge and exposing us to new ideas at a fantastic mental velocity. The Information Age has a darker side though. Hackers, corrupt employees and professional criminals are also drawn to computers and electronic services. Sleek imaginative crimes in cyberspace follow each new innovation like tails of comets. Electronic crimes have certain unique features for criminals that make them unusually attractive. Computers are essentially dumb and will hand over a fortune to someone, without ever saying "what am I doing?" or "hey, wait a minute!"

The primary pathway for communication services is the Internet. The Internet has few security features and was conceived to have none. It was a device to freely share ideas among scientists and engineers with strong morals and high ideals (mostly). Criminals and pranksters can either remain anonymous or even pose as someone else while sitting safely at a university or library computer or from the comfort and privacy of their own homes or by threading calls through third parties. The Rules of Evidence used by criminal Courts do not anticipate how to handle electronic impulses as evidence or to judge reliability of such evidence.

Hiding one's identity is a central feature in most criminal activities, while stealing the identity of another real person has many added advantages. I expect more identity thieves to be on the prowl for account numbers, false birth certificates, false driver's licenses and Social Security cards. A false identity is the gateway crime for most other electronic service delivery and computer crimes or hackers pursuing the eternal quest for a dial tone.

I would also expect increased heavy traffic involving credit card theft now and smart card theft schemes in the near future. Credit cards and smart cards have a double value. They are both forms of identification and sources of funds.

I believe that there will be an increase in computer sabotage cases and computer espionage cases. With the exception of the defense and intelligence agencies, the focus of our community will be on commercial espionage. Corporate criminals will access proprietary information and competitor bids. Corrupt employees will download and e-mail insider information to co-conspirators across the city or across the world.

Because computers are essentially dumb creatures, criminal acts once initiated successfully can result in huge financial losses, and the compromise of voluminous amounts of sensitive data. If the compromise is great enough, entire sectors of electronic service delivery might need to be withdrawn until our defenses catch up with the emerging security threats.

Investigators aren't entirely cursed by the computer age though. We can play too, and I imagine that we will. Investigators have tremendous capacity at their fingertips to research suspects without leaving a trail and to cross-match massive data bases to target suspicious transactions and other connections. Government security officers and investigators can surveil or monitor computer entries by employees, capturing and isolating anomalous behavior for later investigation or instant apprehension. Employees can be sorted by job series and traced through personal identification numbers (PIN). Data access patterns inconsistent

(continued on page 6)

with certain job series can be identified and traced. Computers can also identify unusual volumes of queries or trends in the lopsided exercise of discretionary decision making.

Investigators have wonderful undercover opportunities as well. The same secrecy and anonymity that cloaks criminals can cloak undercover police. Whole investigator squads can pose as a single undercover operative or lurk among members of electronic crime gangs as they communicate. I believe there are terrific electronic surveillance capabilities on the Internet. Photographic images can be captured and transmitted over the Internet or through wireless communication to the locations of your choice. The same is true for communication intercepts. You can conduct surveillance activities with your laptop at your desk, in your auto or on the street. Pen registers installed on a single phone line can rapidly identify whole electronic criminal gangs corresponding with one another to commit crimes.

I also see the emergence of audit teams focusing entirely on defensive and pro-active computer security measures.

For better or worse, as Americans become dependent on electronic communication and service delivery, it will be possible to demand that suspects come to our offices for interviews rather than experience disruption to these increasingly essential services. Like each of us, criminals may become very dependent on communication and electronic services, and may routinely surrender for arrest rather than cope in a world cut off from vital services. This may be a welcome development as violence against police becomes more commonplace.

I expect other types of criminal activity will arrive with the new millennium. As retirement ages are driven upward, we can anticipate a sea of phony disability claims from people simply tired of working.

Moving beyond auditors and investigators, I anticipate that our semiannual reports will be discontinued in favor of online comprehensive IG reports with hypertext capability to access actual audits and perhaps our performance and results data and budget requests.

As we become weaned from bigger is better mentalities, Congress will trust us with simple capital budgets that are silent on FTE levels. IGs will decide whether to do certain tasks with contractors or purchase services rather than maintain the service capability using Federal employees. Most of our big initiatives will be financed as investments in which we promise reductions in Government outlays in return for relatively small investments in our savings and fraud reduction proposals.

I see IGnet moving much more adeptly into specialized chat groups that focus on audit and investigative problems and opportunities. These "members only" groups can tackle important tasks in the manner that Government scientists first envisioned for the Internet.

Big finish! As I look into the next century I see two views of the IG community. The first is one in which we continually position ourselves to advantage the community for change. We play key roles in emerging issues and aggressively step up to bat for new roles as guardians of an electronic age.

The second possibility is that we barricade ourselves in and suspiciously monitor agencies as they grapple with the future. For many of us addicted to formula audits and stale investigative techniques, "monitoring the agency" will be a euphemism for standing on the sidelines as horrified observers to a rapidly changing scene for which we are ill prepared.

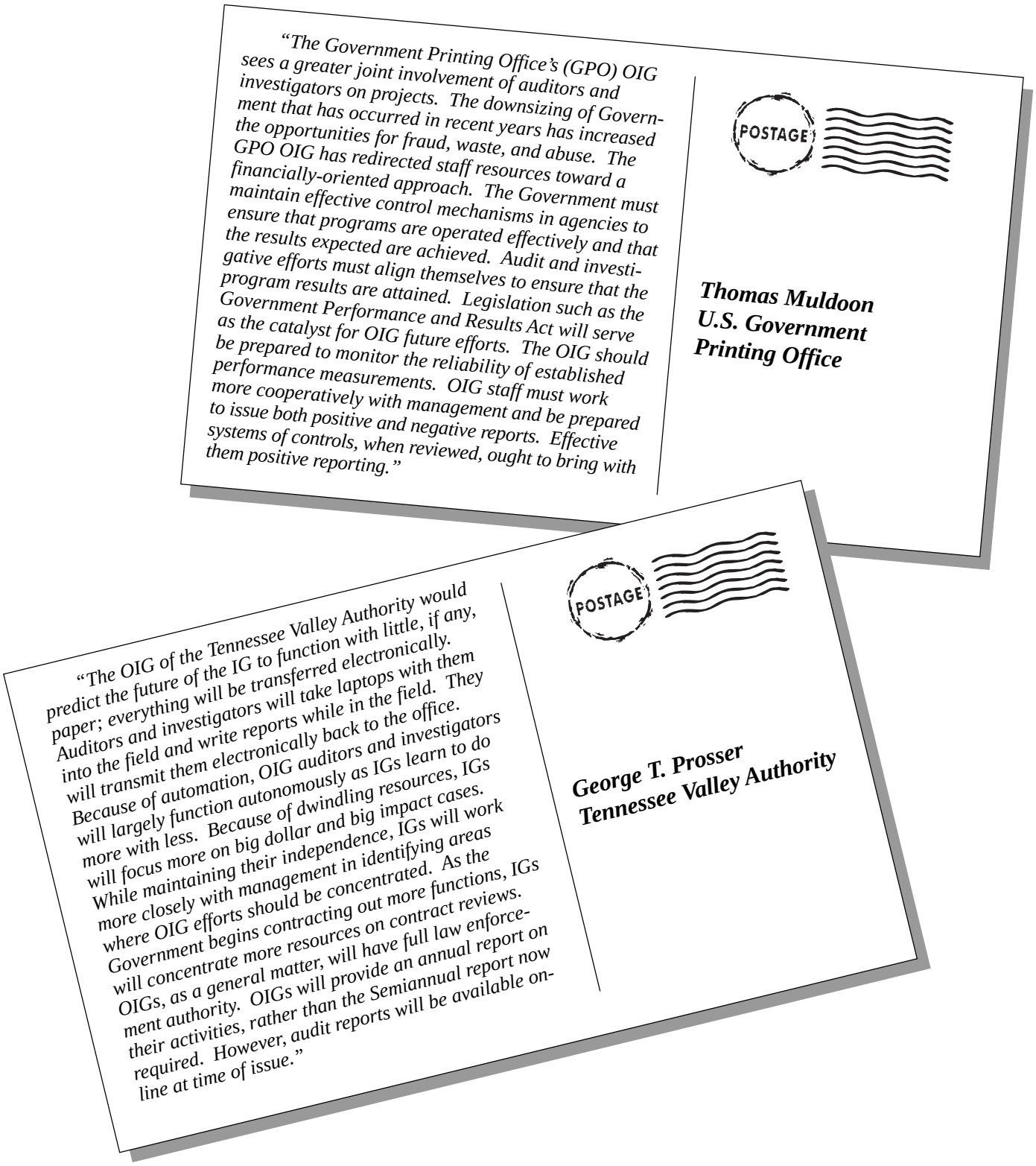
I am confident that we can trade on the trust and good will that we have established with Congress and the Executive Branch to play a key role if we wish and if we have developed the capability. Our neutrality and honest competence will be highly prized in the coming age of rapid change that will be so difficult to understand. We can inform the important debates and strike effectively at criminal threats to vital Government services.

This was a fun article to write and I invited other Inspectors General to share their own glimpses of the future. I think you will enjoy having a look at these other "Postcards from the Edge."❑

Predictions: Inspectors General of the PCIE and ECIE Communities

(continued on page 8)

Postcards (continued)



"The Office of the Inspector General of the future will need to come to resolution with the issues now facing the community. With this in mind, I predict that the following will take place in the future:

I. First, I believe that IGs will better learn to balance pro-active intra-agency activities, which are prescribed by the National Performance Review, with statutory compliance responsibilities. While some OIGs may have been perceived as having abused their legally mandated authorities in the past, others I feel are now near to working too closely with their agencies on issues of policy. It is not wrong to find that mismanagement or abuse exists and to report that finding; that is our primary job.

II. I also think that more IGs will establish an evaluation and inspections unit within their offices as a way of providing pro-active assistance without becoming involved in developing agency policy. I personally have utilized such a unit to provide technical assistance to the agency without becoming too closely associated with the policy issue decisions we are prohibited by law from helping to formulate.

III. To prevent any impression of undue agency influence on the decisions of the IG, it is essential that future IGs be able to submit their annual budget requests directly to the Office of Management and Budget without what could be seen as politically based review and modification from the agency. The trust we enjoy in the Federal community comes from an aura of being beyond political influences.

IV. In the same vein, IGs must understand that if adversarial situations come about as a result of us doing what is right – it's OK.

V. To prevent an appearance of undue influence from management, it must be understood that IGs in the future do not receive monetary awards from the agency.

VI. Finally, I feel that the entire Federal IG community will become more public relations oriented to ensure that the press, Congress, and the American taxpayers understand the IG role and how this role is critical to safeguarding Federal programs."

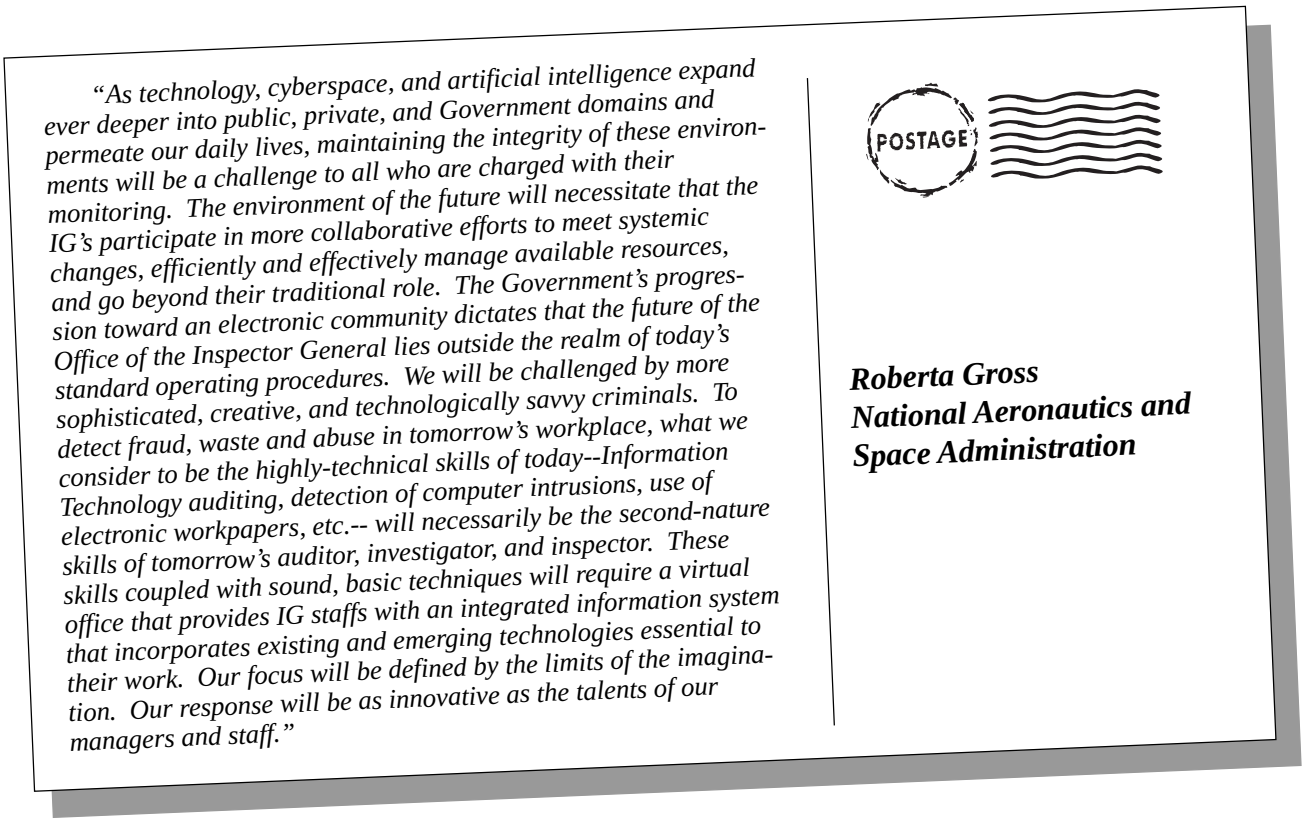
Patrick E. McFarland
Office of Personnel Management

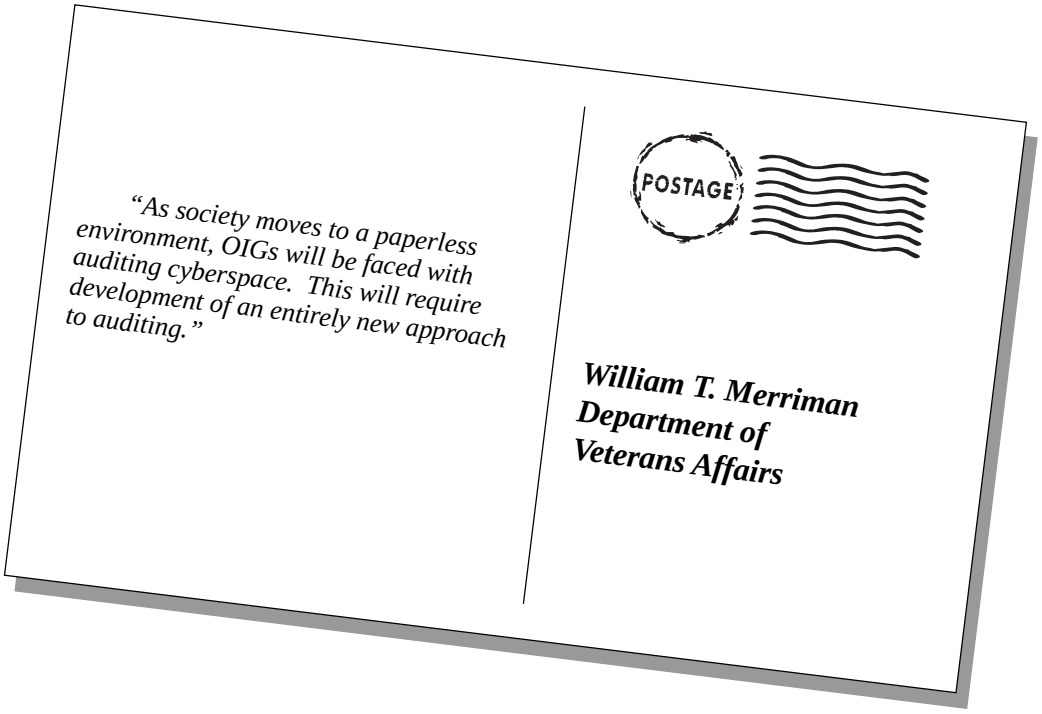
"The Office of Inspector General of tomorrow will be technologically adaptive - both internally and externally. That is, OIG staff will operate from virtual offices with immediate access to data in the organization and access to approaches as well as results from audits, investigations and studies of counterparts and others in both the public and private sectors from computers that attend the individual more than a location. Groupware will be used for workpapers as well as management information; we will have to watch out for the negatives of institutionalization and strive to be at the forefront in showing the way through expertise and forward thinking rather than the traditional follow-up role; and continue to emphasize integrity and capability as the top criteria for employment with an OIG. Challenges will (present in dealing) with the proliferation of information and attendant misuse of that information."

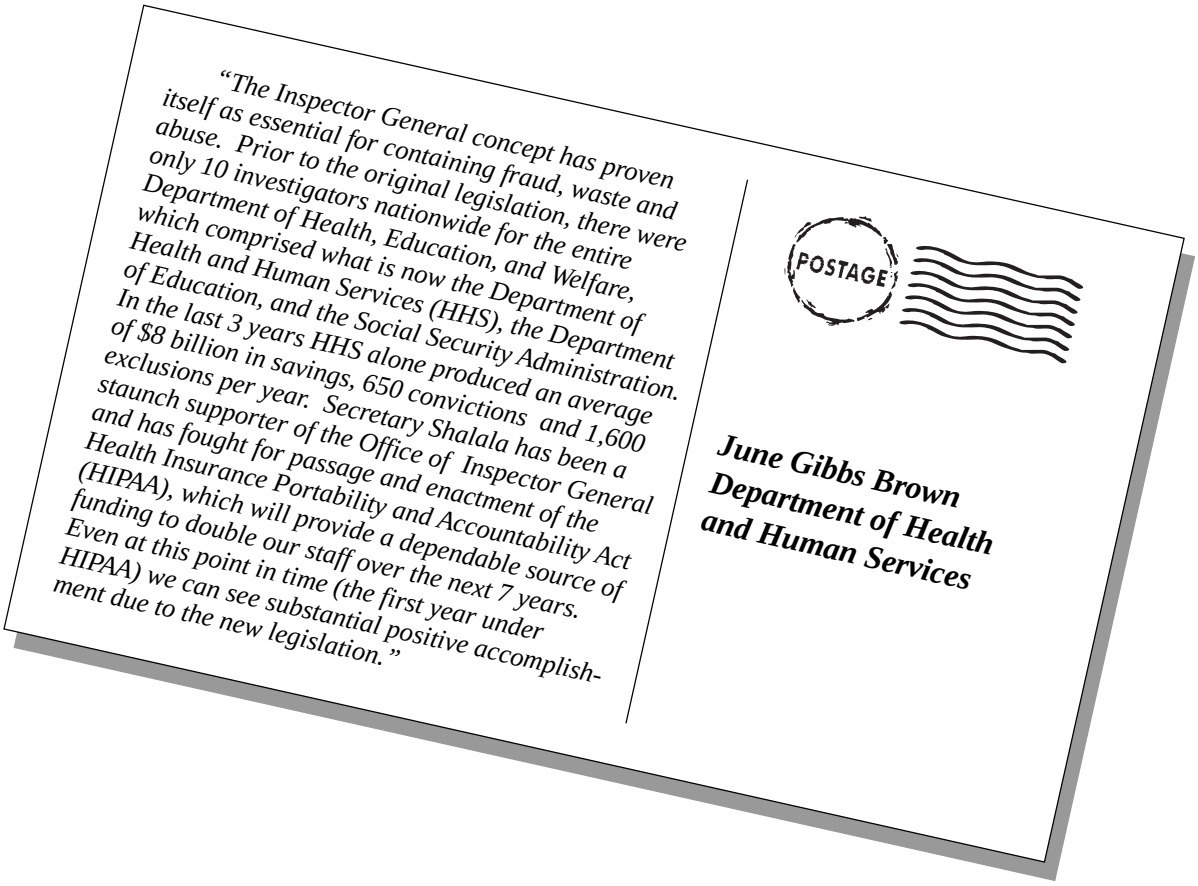
Brent Bowen
Federal Reserve Board

(continued on page 10)

Postcards (continued)

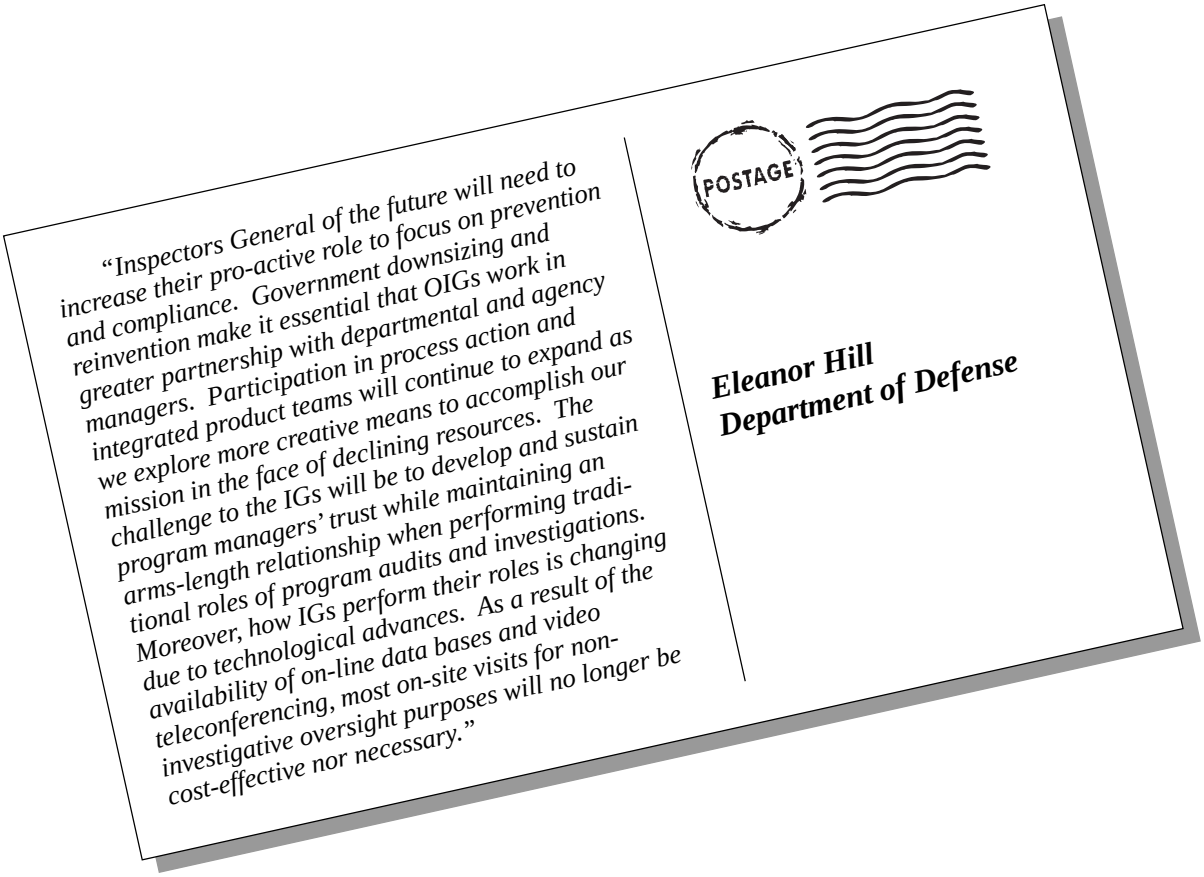






"The Inspector General concept has proven itself as essential for containing fraud, waste and abuse. Prior to the original legislation, there were only 10 investigators nationwide for the entire Department of Health, Education, and Welfare, which comprised what is now the Department of Health and Human Services (HHS), the Department of Education, and the Social Security Administration. In the last 3 years HHS alone produced an average of $8 billion in savings, 650 convictions and 1,600 exclusions per year. Secretary Shalala has been a staunch supporter of the Office of Inspector General and has fought for passage and enactment of the Health Insurance Portability and Accountability Act (HIPAA), which will provide a dependable source of funding to double our staff over the next 7 years. Even at this point in time (the first year under HIPAA) we can see substantial positive accomplishment due to the new legislation."

June Gibbs Brown
Department of Health and Human Services



"Inspectors General of the future will need to increase their pro-active role to focus on prevention and compliance. Government downsizing and reinvention make it essential that OIGs work in greater partnership with departmental and agency managers. Participation in process action and integrated product teams will continue to expand as we explore more creative means to accomplish our mission in the face of declining resources. The challenge to the IGs will be to develop and sustain program managers' trust while maintaining an arms-length relationship when performing traditional roles of program audits and investigations. Moreover, how IGs perform their roles is changing due to technological advances. As a result of the availability of on-line data bases and video teleconferencing, most on-site visits for non-investigative oversight purposes will no longer be cost-effective nor necessary."

Eleanor Hill
Department of Defense

(continued on page 12)

"The future Office of the Inspector General can expect Federal programs that are administered in a decentralized environment, with fewer controls, less guidance and documentation, and reduced management levels and resources. Directives will be severely reduced or eliminated. Multiple supervisory levels, which in the past were thought to help ensure quality performance and prevent loss and abuse, will be eliminated. Fewer transactions will be recorded on paper (which has provided the audit trail in the past) as electronic transactions become the norm. The role of auditing will change as we move toward verifying the validity of measurements and outcomes and performing return-on-investment analyses to judge the value of operations. With fewer controls, more electronic exchanges, and increased pressure to show measurable results, the opportunity and motivation for fraud may increase—while evidence may become more hidden or unobtainable. If delegation of authority from the Federal Government to State and local counterparts continues, both accountability for resources and responsibility for results may become diffused. IG reports must be short, direct and clearly demonstrate pay-off value to management. As OIGs are also downsized auditors and investigators must work together more closely to leverage remaining resources, and there will need to be a greater homogenization of skills within and among OIGs. The need for audits and investigations has never been greater than in this changing environment, and OIGs must be willing to respond with creativeness and flexibility."

Nikki Tinsley
Environmental Protection Agency

"Leadership in the IG community will pass to those organizations staffed by dynamic agents of positive and meaningful change, with a viable commitment to our core mission of detecting and preventing fraud, waste, and abuse and promoting the effectiveness and efficiency of Government programs. Our change agents will be recognized for solid knowledge of public administration and management, in general, and in-depth understanding of their own agencies' programs and complex internal and external operating environments. The staff of the premier OIGs will also demonstrate exceptional skills in interpersonal communications, analysis and evaluation, and advanced technologies. Through direct staff resources or contracting, the OIGs will have access to expertise in technical fields of particular significance in their agencies, such as medicine, aerospace, or construction. A renewed focus on the core legislated mission of the IGs will be accomplished be transferring resource-intensive peripheral responsibilities, such as the auditing of financial statements to the Chief Financial Officer and reviewing these activities in line with other priorities. Without compromising independence, our future change agents will perform a greater number of projects in a customer-focused, interactive mode, flexibility drawing upon the pertinent methodologies of a variety of professional fields and working in multidisciplinary teams of auditors, investigators, evaluators, technical specialists, and program officials. The foremost standard of professionalism will be the USEFULNESS of our products as catalysts for significant and meaningful improvements to the quality, efficiency, and integrity of Government programs."

Hubert N. Sparks
Appalachian Regional Commission

"The future of OIG at the Equal Employment Opportunity Commission (EEOC) is assured if we continue the transition into multi-disciplined teams; establish partnerships with other OIGs and some internal Agency offices to assist in our work; utilize contractors for the routine audits, inspections and investigations; and make use of cyber technology to work smarter to accomplish OIG's mission. In my opinion, "traditional" audit work is only as important as the impact and interest it generates within the Commission. Our future must incorporate our "watchdog" role with that of management consultant. We must be on the forefront of improving the processes that are critical to EEOC's mission. We've recently reviewed small pieces of the discrimination charge process and the procurement of litigation support services. Our analysis of these areas assisted management by improving controls and procedures in the real "bread and butter" areas. Finally, we must continuously evaluate and measure our own performance to determine whether we are adding value to the management of EEOC's limited resources and the improvement of its programs."

Aletha L. Brown
U.S. Equal Employment Opportunity Commission

"Inspector General offices and management have forged a closer partnership. The partnership is natural in that both had the same goal, and both were continually urged to work more closely together. Scarce resources have impacted the offices and agencies. Some matters that were once audited and investigated by the Office of the Inspector General are now referred to management for inquiry and resolution. The need to manage agency as well as audit resources has changed assessment yardsticks. Management looks for audits to focus more on effectiveness of their operations than on compliance. Because performance is now measured in effective solutions, audits now focus on the indicators of success. The outlook and the composition of the Inspector General workforces have changed: investigators focus on prevention as well as prosecution, and auditor groups have evolved beyond staff assessing financial compliance to teams with the skills and experience to handle the more broadly based evaluations."

Luise S. Jordan
Corporation for National Service

Are We Ready for the Electronic Parade: Electronic Benefits Transfer

by Roger C. Viadero and James R. Ebbitt

By Roger C. Viadero, Inspector General, Department of Agriculture

James R. Ebbitt, Assistant Inspector General for Audit, Department of Agriculture

What Is Electonic Benefits Transfer?

From Red Tape to Results, issued by Vice President Gore's National Performance Review in September 1993, called for using similar to electronic funds transfer technology to develop rapidly a nationwide system to deliver Government benefits electronically. This is referred to as Electronic Benefits Transfer (EBT) and is defined as "the automation of benefit authorization, delivery, redemption, and settlement processes through computers, plastic cards, and telecommunications technology which results in the elimination of paper coupons or other paper delivery systems." The Federal EBT Task Force was chartered in November 1993 to meet this challenge. Its goal was to make EBT available nationwide in the fullest sense--one card, user friendly, with unified electronic delivery of Government-funded benefits under a Federal/State partnership.

In 1994, the Federal EBT Task Force identified a number of Federal and State programs where EBT could be used to deliver benefits. In cases where benefits are paid in cash, the objective is to convert to EBT cases where recipients did not have bank accounts and could not receive their benefits via direct deposit. In the case of the Food Stamp program, the objective is to eliminate paper food coupons and substitute EBT cards which could then be used to purchase food. The task force identified the following programs where EBT could be used: Food Stamp program; Aid to Families with Dependent Children; Supplemental Security Income; Old-Age, Survivors, and Disability Insurance (Social Security); unemployment insurance; Veterans Affairs compensation; Special Supplemental Nutrition Program for Women, Infants, and Children (WIC); Federal and military pensions; and Railroad Retirement benefits. In all, it was estimated that $111 billion in annual benefits could be delivered using EBT.

The U.S. Department of Agriculture's (USDA) Food and Consumer Service has been at the forefront of EBT development. This article will focus on USDA's experience with EBT and will examine the issues and challenges facing the Office of Inspector General (OIG) in auditing and investigating aspects of EBT. We believe that our experience can provide insight and valuable lessons learned for other OIGs as EBT becomes more prevalent in the delivery of Federal benefits.

Perspective on EBT at USDA

In October 1977, Congress amended the Food Stamp Act which authorized USDA to seek alternative methods for program benefit delivery by relying on data processing equipment and computer technology. The Food and Consumer Service funded and arranged an EBT system demonstration project in Reading, Pennsylvania, beginning in 1984. Other demonstration projects followed in 1987 and 1988 in Iowa, Maryland, Minnesota and New Mexico. In 1990 the Food Stamp program was again amended authorizing on-line EBT systems. The 1996 Welfare Reform Act mandates EBT for food stamps by 2002.

The objective of the Food Stamp program, from its inception in the 1960's, was to help eligible Americans obtain an adequate diet. Food coupons were developed to deliver program benefits with the idea that they could only be used to purchase food. To make this concept work, the USDA's Food and Consumer Service authorizes stores to accept food coupons. The authorized stores receive redemption certificates which permit them to deposit food coupons at a banking institution and receive credit to their bank account for the face value of the coupons. Stores, to be authorized, are to offer a defined variety of staple foods, or have 50 percent or more of their total sales in staple foods, and agree to only accept food coupons for food.

Trafficking in food stamps quickly emerged as a problem because some recipients did not want their benefits in food and some authorized stores were willing to sell non-food items, as well as exchange coupons for cash at a discount. Middlemen also traded for coupons, again at a discount, for items such as drugs, guns, electronic equipment and cars. Middlemen then found authorized stores that were willing to accept the coupons for cash, at a discount. Food coupons became a secondary currency on the streets. The Food and Consumer Service estimated that of the $22 billion issued in Fiscal Year 1993, over $815 million was trafficked. The OIG testified that trafficking and related fraud was in excess of $1 billion.

(continued on page 16)

EBT could eliminate other program costs associated with food coupons, such as the printing of food coupons, distributing them to the States and issuing agents, issuance to recipients, and the cost to redeem the coupons through the banking system and the Federal Reserve. The OIG has been supportive of EBT to issue program benefits because it eliminates food coupons from serving as a second currency, as well as the middlemen in trafficking schemes, and it reduces program costs. As we will discuss later, it also provides a powerful tool to better identify stores and recipients who may be trafficking.

Successful EBT Requires Partnerships

To make EBT systems work, partnerships had to be developed. Except for State general assistance programs, the programs where EBT is to be used are funded all, or in part, by the Federal Government. In several cases, State agencies administer the programs under agreements with the Federal funding agencies. In addition, since EBT systems are to use existing private systems to the extent practicable, the partnerships include private processing companies who operate EBT systems and private banks that move funds and settle accounts. In some cases, processors and banks are one and the same. Each of the partners plays a role in making EBT work.

Using the Food Stamp program as an example, program benefits are funded entirely by the Federal Government. USDA sets program policy, provides general oversight and monitoring of program operations, authorizes stores to participate, and receives reports accounting for store redemption activity and the draw down of Federal funds. The Food and Consumer Service enters into agreements with State agencies to administer the program. State agencies determine eligibility and issue program benefits. Since EBT is an issuance function, States enter into agreements with private processors to carry out the issuance function, with approval of the Food and Consumer Service. States issue EBT cards and allow recipients to select personal identification numbers.

The processor receives electronic information from the State agency telling it which recipient accounts to establish for the month and the benefit amount. The processor installs Point of Sale terminals in authorized stores so that stores can communicate with the central data base and determine whether recipients are authorized and the account balances available will cover the transaction. In some cases, stores had an existing EBT-type relationship with a processor other than the one selected by the State (a third-party processor). Rather than install duplicate equipment, the State's EBT processor enters into an agreement with the third-party processor. This permits the store to continue using its processor, but it is now able to communicate with the State's EBT processor's central data base and receive settlement for food stamp EBT transactions. The processor also settles individual store accounts for cumulative food stamp transactions. This is accomplished by drawing down Federal funds and using a private bank to move funds to the stores' banks and then into the individual store accounts.

States are rapidly moving to implement EBT systems for the Food Stamp program and a number of other targeted programs. Two technologies are used currently to make EBT work: on-line and off-line systems. On-line systems use existing debit card technology with information maintained on a central computer system. The card is used to access information, including the account balance. Off-line technology uses "smart" cards. The card contains a microcomputer chip which stores information including the available account balance. Currently, 19 States have operational on-line EBT systems; 2 States have operational off-line EBT systems; 24 States have selected EBT processors and are in the process of approving contracts and implementing Statewide systems; and 3 States have issued requests for proposals.

In addition to the Food Stamp program, WIC program benefits are being issued using an off-line EBT system in selected counties in Wyoming. Fourteen States are issuing Aid to Families with Dependent Children and two issue some direct Federal benefits. Ten States are using EBT to issue a number of State program benefits.

Investigative and "Alert" Monitoring of EBT

While the EBT card has not eliminated illicit trafficking by authorized stores and recipients, EBT-generated records have enabled OIG to better monitor and analyze sales and redemption activity. As a result, OIG can target stores that may be trafficking. There is more data pertaining to EBT transactions, compared to the food coupon issuance systems and it is readily available in electronic format. A valuable benefit of this involves the ability to identify the food stamp recipients who are involved in benefit trafficking activities. In contrast to paper food coupons, which lose their ownership identity immediately upon being used in a transaction, EBT benefits are attached electronically to the recipient. When the benefits are redeemed, they are stored on the computer system showing when and where the benefits were used. Once we identify a store where trafficking is occurring, we are also able to identify recipients who appear to be involved in the scheme. This information has become extremely valuable during the course of our investigations of stores, as well as providing key evidence to allow for criminal prosecution and/or administrative (program) disqualification of the recipients.

The first criminal investigation of trafficking in EBT food stamp benefits occurred in Reading, Pennsylvania (the site of the first EBT pilot project) in 1991, and resulted in convictions of 2 store owners and over 140 recipients who sold their benefits at the store. Since EBT started, we have initiated 199 EBT-related investigations, resulting in 261 indictments and 198 convictions, and monetary results of nearly $4.5 million.

An example of our EBT investigative work involved our investigation of a small convenience store owner in

Baltimore, Maryland, who pled guilty to trafficking over $700,000 in EBT food stamp benefits during an 18-month period. He subsequently was sentenced to 2 years in prison and was ordered to pay restitution of $250,000 to the USDA. In addition, over $92,000 from the proceeds of these illegal transactions have been seized by or forfeited to the Government. Store employees admitted to our investigators that the store owner instructed them to add $3 and change to all trafficking transactions at the store. This was done in an attempt to disguise the trafficking pattern so the EBT system would not show even-dollar transactions at their store, one of the tell-tale signs of trafficking. During our investigation we reviewed all transactions which exceeded $20 and determined that 92 percent of these, totaling over $745,000, included the additional $3 charge.

Based on the success OIG had in using EBT data to identify stores and recipients suspected of trafficking, the Food and Consumer Service hired a contractor to develop an automated system that would be capable of doing similar reviews on a nationwide basis. The system, Anti-fraud Locator for EBT Redemption Transactions (ALERT), was developed using OIG's experience and input. ALERT has been tested using EBT data from several States, and after modifications based on the testing, is being used successfully for a number of States where EBT systems for food stamps have been implemented.

Not only has OIG been supportive of EBT, we have taken an active role in monitoring and reviewing EBT systems used for the Food Stamp program. In doing this, OIG identified key EBT operational areas that need to be reviewed: automated data processing (ADP) security; program benefit issuance and redemption; reconciliations between a State, its EBT processor, and Federal agencies; EBT settlement between the Department of the Treasury, the EBT processor, and the authorized stores; and EBT reporting, both financial and management.

During the last 2 years we led a work group under the auspices of the President's Council on Integrity and Efficiency. The work group issued a report entitled, "Implementing the EBT System: A Report on the Current Status of Control Systems," which describes EBT implementation in nine States, and a report to the Food and Consumer Service on issues that need to be addressed at the national level. Overall, our audits have concluded that EBT systems used for the Food Stamp program are working. Program benefits are being issued to the right people in the right amounts, and settlements among the parties are being made on a timely basis. There are, however, some issues that need to be addressed.

EBT Issues to Address

With the available transaction data in EBT systems, the ALERT system is capable of identifying retailers and recipients suspected of trafficking. The down side is that there are large numbers of retailers and recipients that Federal and State agencies need to deal with but there is not a plan in place as to how this will be done. An example of the numbers comes from analyses run in Baltimore, which identified over 7,000 suspect recipients.

Reconciliations between letter-of-credit draw downs for settlement and reported EBT transactions were not always made even though there were substantial differences that needed to be researched and resolved. There were also inconsistencies between States in how settlements with retailers were made. The impact of this will be felt as States begin to interact.

Some EBT processors are banks, and in at least one case the EBT accounts were co-mingled with other accounts maintained by recipients. We will need to ensure that auditors and investigators have access to financial records maintained by banks as defined by the Right to Financial Privacy Act of 1978.

While the Food and Consumer Service has developed a nationwide system to detect suspected trafficking, consideration needs to be given to whether similar control measures are needed at the State/EBT processor level. The Food and Consumer Service used South Carolina as a test project area for the EBT processor to run analyses for suspected trafficking. The project had good results and may be particularly suited for recipient cases since States have dealt traditionally with these types of cases.

Current record retention requirements are 3 years, yet criminal statutes typically have a 5-year statute of limitations. EBT-related records need a retention requirement consistent with the criminal statute of limitations. Most, if not all, States have statutes that define food coupon trafficking as a State offense. Similar State statutes are needed to define EBT card trafficking as a State offense.

Specific requirements for protecting private data in EBT systems have not been defined and provided to States and their EBT processors. This also is true for third-party processors. Specific requirements are contained in the "Federal Information Processing Standards Guidelines for Computer Security, Certification and Accreditation," and our recommendation is that these be adopted and required of the States and their EBT processors. State contracts with EBT processors need to provide that Federal and State representatives, such as auditors and investigators, have access to EBT processor records.

Once EBT systems were up and operating, reviews were not made to determine who had access to systems, what that level of access was and whether it was still needed. In some cases employees had high access levels, yet supervisors or another second party had not reviewed the level and determined it was needed. In one case, out of 1,600 active log-on identifications for the EBT system, 233 were assigned to employees who were no longer authorized access to any other State ADP system.

Federal guidelines require States to maintain an ADP security program which includes data and personnel; however, this has not been well defined and has not been passed on to the EBT processors through the contracts. It involves such things as employee security clearances,

(continued on page 18)

security training, and accepted security practices. Two of the three processors we reviewed did not have a security program which addressed these areas.

Certification standards for third-party processors have not been established. Multiple third-party processors are being used in each State where EBT is operational and the approaches in each State to certify them have varied widely.

There were discrepancies between the authorized-store data base maintained by the Food and Consumer Service and that maintained by the EBT processor. Stores that were no longer authorized continued to transact EBT business. This resulted from communication problems on the part of the Food and Consumer Service, as well as the EBT processors.

There are multiple Federal and State audit groups that have a need to audit EBT processors because the processors are private parties performing financially-related functions that affect Federal and State financial statements. The reality is that relatively few EBT processors have the EBT business. We need a coordinated approach to obtain audit coverage at EBT processors to avoid multiple audit groups converging on the processors.

We have recommended that the contracts with EBT processors require that the processor obtain audit coverage under Statements on Auditing Standards (SAS) 70 requirements. The President's Council on Integrity and Efficiency has assigned us to chair an EBT task force project to develop agreed-upon procedures and relevant tests of controls that the processors' auditors would apply under SAS 70 coverage. Participants on this task force include representatives from Federal, State and private audit organizations.

Conclusion: Are We Ready-- You Bet!

With over $111 billion in program benefits slated to be issued through EBT and over $24 billion of that in Food Stamp and WIC program benefits for the USDA, we must be prepared to review these systems and communicate to managers whether they are functioning properly. In addition, we must assess whether these systems can aid us in better carrying out our audit and investigative responsibilities. We have been able to accomplish this by involving ourselves in EBT systems as they were tried as pilot projects and then being ready to review them as they were rolled out as full-fledged issuance systems. We have met the initial challenge and as a result we believe we are in a good position to fulfill our mandated role.❑

Pros and Cons of EBT

Overall, our assessment is that EBT is a good thing and OIG has been fully supportive of using it to issue program benefits. However, we believe it is a useful exercise to review the pros and cons as we viewed them in arriving at our conclusions.

Pros

Paper food coupons are eliminated, thus eliminating associated costs to print, store, ship, issue, redeem, and dispose of them. In addition, a second currency is no longer available and the middlemen who often trafficked in food coupons can no longer do so.

Recipients, retailers, and banks generally prefer EBT cards over food coupons. Retailers and banks realize savings because they no longer have the labor-intensive task of handling the food coupons. Recipients no longer have to make the monthly trip to the issuing agent to obtain their food coupons.

Data are now available to better identify retailers who may be trafficking. Individual recipients can now be identified, for the first time, by suspect transactions.

More timely and precise data on draw downs of Federal funds to settle accounts are now available. This should permit the Food and Consumer Service to better manage funds and the redemption process.

If the Federal EBT task force goals are realized, one EBT card will permit access to multiple program benefits.

Recipients sometimes made small purchases with food coupons to receive cash change which was then used to purchase ineligible items. With EBT, this has been eliminated.

Cons

If only a single program uses EBT to deliver benefits, or if it is only used in smaller project areas, the presumed cost savings will not be realized. EBT will need to be implemented nationwide and involve multiple programs to be cost effective.

In the commercial world, if an error in the system causes an erroneous credit to a customer's account, the stores are able to have the error reversed. This same avenue does not appear to be available with Government programs short of providing the recipient notification and due process. This came to light in Alabama during implementation where food stamp recipients purchased food and their EBT accounts were properly debited for the amount of the purchase. However, due to a system error, hundreds of accounts received credits in the amount of the purchases, meaning the stores would not receive payment for goods they had sold. The stores did not have an avenue available to have the mistakes corrected without first involving the recipients.

Some thought EBT would eliminate trafficking in the Food Stamp program since there would be no food coupons. This has not happened since some stores are willing to traffick using the EBT card.

EBT systems have information which can be manipulated to identify stores and recipients suspected of trafficking. However, Federal and State agencies are faced with limited resources to address the large numbers of suspect stores and recipients.

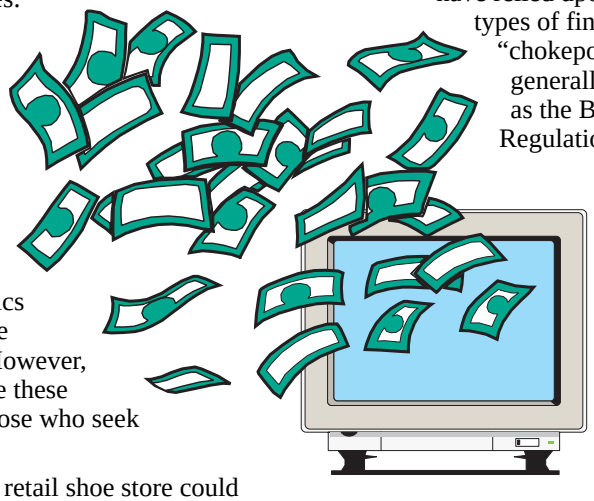
Following the Money in Cyberspace: A Challenge for Investigators in the 21st Century

by Stanley E. Morris

Stanley E. Morris, Director, Financial Crimes Enforcement Network, Department of the Treasury

New technologies have emerged which have the potential to change many of the fundamental principles associated with a "cash" oriented society. In fact, these developments may alter the means by which all types of financial transactions are conducted and financial payments systems are operated.

Law enforcement around the world has come to recognize over the years that "following the money" leads to the top of a criminal organization. Criminals need to move their funds through the financial system to hide and use the proceeds of their crimes. Currency is anonymous, but it is difficult to hide and transport in large amounts. The new electronic payment systems have the potential to change all this.



The speed which makes these systems efficient and the anonymity which makes them secure are positive characteristics from the perspective of both the public and law enforcement. However, these same characteristics make these systems equally attractive to those who seek to use them for illicit purposes.

For example, an American retail shoe store could accept smart cards for purchases. As the store's revenues increase, it could transfer the value of its revenues to another smart card or download the value to a computer. This value could, in turn, be transferred through the Internet to financial institutions, businesses or individuals around the world to pay invoices, order materials, or pay suppliers--in all cases, stimulating commerce, making trade less expensive and providing benefits to consumers.

Now, suppose the retailer is a narcotics trafficker. Consider the invoices the trafficker might pay, the supplies he might order and the transactions he might accomplish if, for instance, he could download an unlimited amount of value from a smart card to a computer, and then transmit those funds to other smart cards or computers in locations around the world--again, all anonymously, all without an audit trail, and all without the need to resort to a traditional financial institution.

It is because of these potential vulnerabilities that the Financial Crimes Enforcement Network (FinCEN), an organization within the Department of the Treasury that has the primary responsibility for setting, overseeing, and implementing policies to prevent and detect money laundering, has been meeting with the developers of advanced electronic payment systems and our law enforcement and regulatory partners to examine how criminals might use these new systems to move and launder the proceeds of their illegal activities.

Historically, law enforcement and regulatory officials have relied upon the intermediation of banks and other types of financial institutions to provide "chokepoints" through which funds must generally pass. In fact, many regulations, such as the Bank Secrecy Act (31 Code of Federal Regulations, Part 103), are designed specifically to require financial institutions to file reports and keep certain records to ensure that such a paper trail exists for law enforcement investigations. In an open environment like the Internet, exchanges of financial value could occur without the participation of a financial intermediary, and thus, the existing chokepoint could be eliminated. The advent of these new systems will also impact the effectiveness of traditional investigative techniques, which have typically relied on financial document analysis. How financial institutions will effectively "know their customers" in a potentially anonymous, paperless payment system is also a concern.

Another challenge facing law enforcement is that these payment systems are being designed to operate internationally in multiple currencies; therefore, it will be more difficult to determine the applicability of

(continued on page 20)

jurisdictional authority. For these and other reasons, it is critical that discussions continue with the developers of these systems, representatives from the financial services industry, as well as the domestic and international law enforcement, regulatory and privacy communities. Our colleagues in all of these areas have valuable insight into the implications of these new technologies.

Too often, Government regulators have attempted to thwart a potential threat by imposing burdensome regulations that reflect little appreciation of the nature of the threat, or business practices of the affected industries. We cannot make the same mistakes with cyberpayment systems. The technology is developing too rapidly, and the gains and efficiencies potentially created by the new systems are too important. At the same time, without thoughtful and balanced consideration of law enforcement concerns now, the prospects for abuse by organized crime, money launderers, and other financial criminals could be great. We need to look beyond our borders, both in terms of ensuring that the integrity of these systems is protected, and from a larger perspective that the United States continues to be able to compete fairly in a global market.

Earlier this year, FinCEN chaired a study by the Financial Action Task Force (FATF), the 26-nation organization created by the G-7 to address the global problem of money laundering. For the first time, FATF released a public report on existing money-laundering trends around the globe. This report contained an appendix discussing the money-laundering implications of emerging payment systems, such as electronic money and Internet transactions. Participants agreed that the technology is still in its infancy and to date, has been designed for low value consumer/retail transactions. However, FATF has positioned itself in a pivotal role to work in partnership with international developers, the law enforcement community, and the financial services sector to ensure these systems are developed in ways that minimize their potential abuse by criminals.

In May of this year, FinCEN issued proposed regulations designed to prevent and detect money laundering through money services businesses, a term used to describe money transmitters, issuers, redeemers and sellers of money orders and traveler's checks, check cashers, and currency retail exchangers. The regulations would register all qualified money services' businesses in a centralized data base, which will then be made available to law enforcement and appropriate Federal and State regulatory agencies. The proposed registration rule includes within the definition of money services businesses issuers, sellers, and redeemers (for funds) of stored value.

Even more recently, FinCEN concluded money-laundering simulation exercises, focusing on the implications of electronic money, with the Rand Corporation. These exercises brought together representatives from the industry developing these advanced technologies, as well as law enforcement, Government regulators and the banking community, to discuss hypothetical scenarios and develop solutions.

The Secretary of the Treasury has designated Eugene Ludwig, Comptroller of the Currency, as the coordinator of Treasury's efforts in this area. FinCEN, in concert with the Office of the Comptroller of the Currency, will continue to work with our law enforcement and regulatory counterparts throughout the Government. We do not want to impede the development of technologies that will benefit us all. Our goal is to inoculate, to the greatest extent possible, these new systems against crime and misuse and permit their healthy growth into the next century.❑

Don't Start the Revolution Without Me: Auditing Computer Investments

by Joseph A. Lawson

Joseph A. Lawson,
Director of Information Technology,
Office of Inspector General,
Department of the Treasury

A revolutionary concept is changing information technology (IT) management. IT is now viewed as a strategic asset and an investment, not just an expense. IT investment management is the process of turning innovative ideas into practical realities in which the agency earns a return on its investment. The investment is financial, but the return is measurable improvement in mission or program performance. The improvement can take many different forms, including reduced program costs, increased quality or speed, higher levels of customer satisfaction, etc.

For the Office of Inspectors General (OIG), IT investment management has huge economy and efficiency implications. Successful IT investment management can generate enormous productivity gains. Unsuccessful efforts incur enormous opportunity costs for what might have been, waste funds, and often lead to damaging headlines and negative publicity. Agency executives are designing the structures and procedures for IT investment management now. Auditors, because of their professional expertise, can provide feedback to the executives, but the OIGs must act quickly and decisively to become involved before the planning and building of IT structures are finished.

The Elements of IT Investment Management

IT investment management is a collection of ideas, attitudes and techniques that includes the following elements:

- Strategic planning and performance measurement focus us on the results we really want to achieve.
- Capital asset planning focuses us on where we should invest our resources, ensuring that we avoid investing to support lesser priorities or in functions that others can provide more efficiently.
- Business process reengineering makes use of IT to eliminate unnecessary work and significantly improve efficiency, speed, quality and customer satisfaction. The enabling technologies, such as relational data bases and networks, cannot improve anything unless the agency first redesigns its business processes.
- Return on investment reminds us that the benefits of development projects should exceed the costs. Instead of vague promises, we now need to commit to measurable improvements in mission or program performance, so we can verify the success of the project after implementation.
- Information architecture is the IT vision of the future. It describes the agency's requirements, information flows, systems components, standards and rules. The architecture has an enormous effect on the agency's infrastructure and application decisions, so it requires a strong, thoughtful design.
- Portfolio management draws the analogy between the management of financial instruments and the collection of production systems, systems under development and current proposals for new systems. In both cases, the portfolio manager replaces poor performers with more promising prospects as circumstances permit.
- Modular construction, breaking large projects into manageable chunks, combined with rapid application development techniques, enables us to solve specific problems quickly, typically no more than 18 months from start to finish. This is useful for reducing the risk of project failure or technological obsolescence.
- Risk management encourages us to use procurement and development techniques, such as performance-based contracting, to further reduce the risk of loss from IT initiatives. It also encourages us to avoid custom systems when off-the-shelf software will do, or attempting projects where the size, complexity or unfamiliarity would overwhelm our capacity to manage them.
- Agencies are appointing Chief Information Officers, and developing investment review boards and procedures to inaugurate IT investment management programs. These boards will make IT investment decisions, control development projects, and evaluate

(continued on page 22)

project results. OIGs can participate in a wide variety of ways in IT investment management program developments. What follows are some suggestions, although there are many other possibilities.

The Challenge for the Inspector General Community

OIGs have many options for traditional audits of various aspects of IT investment management. The General Accounting Office publication, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies': IT Investment Decision-making,* contains valuable information about the processes involved, the data required and the decisions made in IT investment management. The guide is invaluable for creating audit programs to examine project selection, control and evaluation.

The traditional audit process looks at historical events, and reports findings and recommendations long after the events. This works well during periods of relative stability. During periods of change, however, immediate feedback can affect matters before they freeze in place. Feedback that comes after the change is much less effective because structures and procedures harden during the delay, making further progress more difficult and costly. These structures and procedures will have significant consequences for years, thus agencies need help setting up these things now.

While an agency attempts to establish its program, the OIG can play a role as an independent advisor engaged in activities as they occur. The OIG can provide timely, practical, constructive recommendations to spur progress, solve problems, eliminate obstacles, and maintain a professional, ethical climate. There are three major points where the auditors can provide great benefits to the agency:

1. *Designing the Investment Review Board.* Each agency should have an investment review board consisting of high level IT, finance and program executives. The board has responsibility for reviewing and approving IT investment proposals, monitoring and controlling funded projects, and evaluating project results in terms of project goals and mission performance improvements.

The board selects projects based on data that demonstrate that a proposed new system will produce a sufficient return on investment after adjusting for the inherent project risk. After selecting projects, the board exercises ongoing control of the projects, monitoring them for early indications of trouble in their budgets, schedules, functionality and deliverables. When the board detects indications of serious trouble, it should take action to continue the project, modify it in some way to improve its prospects, or terminate it outright. At the conclusion of each project the board should evaluate the project to identify lessons learned and determine whether the project achieved the planned performance improvements.

The board should include representatives from across the agency so that it will have an agency-wide perspective. These members should be high enough in the organization so that their decisions are subject to override only by the agency head. A board composed of members of low rank will hesitate to question the value of a proposal or an ongoing project championed by executives of higher rank. Since the board must be able to identify and terminate failing projects, only the most senior managers can take the heat for such decisions.

The investment review board should encourage and introduce innovations that change the way the agency does business in addition to its formal responsibility to review and approve proposed investments. The board should not limit itself to processing requests for funding against elaborate, detailed criteria. Certainly the Office of Management and Budget has provided very useful and valuable criteria about capital planning, information architecture and risk management that the board must consider. However, the greater value of the board will come from the positive changes it encourages and supports.

2. *Managing the Portfolio and Architecture.* The board should also manage the agency's portfolio of IT investments. The portfolio consists of the current production systems, systems under development and proposals for new systems. Before the board can make any decisions about new initiatives, the agency must have an information architecture, an IT vision of the future that clearly describes where the agency wants to go functionally and technically.

The information architecture will have a serious effect in terms of future investments. The architecture may require significant investment in infrastructure (computers, networks, software, etc.). The board will make sure that proposed IT investments conform with the architecture, rejecting those that do not. If the architecture lacks good design, the agency may spend more than necessary to implement it. Before evaluating proposals, the board should validate the information architecture, making sure it fits the agency's business plans. The board should also validate the architecture for technical soundness, considering the probabilities that particular technologies and vendors will be viable several years from now.

Further, when making portfolio decisions, the board should take action based on the total life cycle costs of each system in the portfolio. This means that the board may need to decide when to replace older "legacy" systems. After a time, maintenance and opportunity costs may get so large that replacement is the smart choice.

3. *Monitoring, Controlling and Evaluating Projects.* When systems are under development, the board has the responsibility for ensuring that each project proceeds as planned. When there are warnings of unexpected costs, delays, inadequate deliverables or missing functionality, the board should take corrective action. When warning signs are apparent, the board could decide to continue the project as is, modify the project or the plan, or, in the most serious cases, terminate the project.

This requires honest reports from project managers, so the board needs to set the right tone. If it becomes apparent that the board only wants to hear good news, or that it overreacts to minor problems, project managers will most likely not be as candid as needed. Also, the board must

resist the temptation to micromanage projects. That is what the agency pays the project manager to do.

When projects end, either successfully or after termination by the board, the board should evaluate the project to identify lessons learned and verify achievement of the performance improvements. The board should avoid doing the sort of post-mortem that only identifies the project's problems, as this does great harm to the workers who probably did their best.

If an ongoing project has serious, insoluble problems, the board should decide to terminate the project. When the board admits mistakes and stops spending money on a useless project, it means the IT investment management process is working correctly. Instead of hammering the agency for its failure, we should salute the board for taking such difficult action.

Adaptive Challenges for OIGs

Effective involvement in the IT investment management program depends upon timely audit reports. Timely recommendations cost less to implement because they require less project backtracking. This is consistent with the proverb about designing in quality instead of inspecting out defects. To make recommendations in real time, so to speak, means that field work must be concurrent with the audited activities, and report writing, editing, publication and distribution need radical improvement. This invariably leads to consideration of two concepts that differ substantially from the traditional audit methodology, partnering and new audit products.

Partnering between auditors and management means sharing the day-to-day information about IT investment management activities. It does not necessarily mean sacrificing auditor independence. Traditional auditing relies heavily on reviewing documentation. We know from experience that documentation is often incomplete and usually produced long after the developers finish the underlying work. We cannot be effective unless management trusts us enough to allow us open access to inside information in real time so we know what is really happening, good and bad.

Partnerships require trust. Auditors need to trust management to freely share information, and management needs to trust auditors to act responsibly with it. Audit reports should attempt to influence change, not to confront or belittle managers as incompetent, foolish or morally bankrupt. (Of course, there are times when management is unable or unwilling to change, but here we are talking about managers who are trying to manage IT investments to improve performance.) Audit reports that misuse inside information quickly lead to closed doors, ending access to real time information about real problems. When this happens, the auditor must wait for the documentation and find something reportable. In a developmental environment, such reports will rarely be useful.

Partners bring value to the relationship. Auditors add value by acting independently, identifying problems, making practical and perhaps difficult recommendations, and preserving a professional and ethical atmosphere. When done constructively, auditors add great value to the relationship. Management also needs to understand that auditors must observe the requirements of independence. This means that auditors will not make managerial decisions, nor will they restrict distribution of their reports to just a few insiders. Our reports typically reach a broad audience, except when they discuss security or proprietary details. As long as the reports are constructive, the partnership should continue.

New audit products might enable us to deliver thoughtful recommendations in a more timely manner. We traditionally convey our audit results in formal audit reports that contain explanatory material, disclaimers, boilerplate, descriptions of the work performed, findings, recommendations, management's official response, etc. We spend a lot of time writing, editing, publishing and distributing our reports, leading to a lengthy delay between the end of field work and the distribution of the report.

We could reengineer the reporting process, eliminating sequential reviews and empowering a few to do the work of many. This could speed up the process, but not necessarily make the product suitable for use in a developmental environment. We really need to consider entirely new audit products.

We need new audit products that deliver our message more quickly and frequently than traditional audit reports allow. In meetings, a well-prepared, experienced auditor could provide immediate, verbal feedback that influences management. This could have the same effect as an audit report, but tailored to fit the situation. Letters to management could convey more serious or difficult matters relatively quickly. If the verbal comments or letters are insufficient or inappropriate, we have the option of escalating to a formal audit report.

Of course, in the era of strategic planning and performance measurement, auditors need to demonstrate the value of these kinds of activities. We need to measure how our participation affects the outcome of the development process. Partner satisfaction surveys are one method of measuring performance, and there may be others.

Conclusion: Don't Start the Revolution without Us!

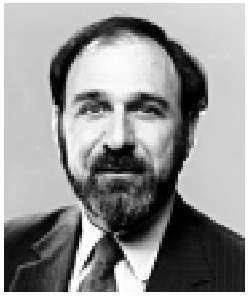
OIGs can provide a valuable service to their agencies. We can help them design and establish their investment review boards and procedures so that the boards have the best chance of making wise and effective decisions. Auditors can make sure that selected projects address business process reengineering opportunities, project realistic improvements in mission performance, and use modular construction that conforms with a well-designed information architecture. Additionally, auditors can help make sure that controls over selected investments ensure real investment returns in terms of measurable improvements in mission performance.❑

In Memory of…

Joseph A. Lawson, who authored this article, passed away on September 26, 1997, from a stroke suffered two days earlier. In a short time, Mr. Lawson had established a well-earned reputation as a leader in Federal information technology auditing. Mr. Lawson joined Treasury OIG after a distinguished career with the State of Virginia. He was a Certified Public Accountant and Certified Information Systems Auditor with a Master of Business Administration degree. Mr. Lawson is survived by his wife, Susan, three daughters and four grandchildren. Mr. Lawson was 49.

Policing the Global Village: Report on the Anti-Corruption Conference

by Stuart C. Gilman, Ph.D.



Stuart C. Gilman, Ph.D.,
Special Assistant to the Director,
U.S. Office of Government Ethics

Introduction

In March 1996, an epochal event occurred, hardly creating a ripple in the world press. In its third plenary session, the members of the Organization of American States (OAS) adopted the Inter-American Convention Against Corruption.[1] What is momentous about this treaty, and more importantly why it should be of interest to the Inspector General (IG) community, is the purpose of the rest of this essay.

Corruption of government, attended by waste, fraud and abuse, is not new. Corruption seems to be associated with government as far back as the Pharaohs, if not into pre-history. Interestingly, the attempts to fight corruption date just as far back, with mention being made of audits and punishment of civil servants by Joseph in Egypt in the Old Testament. Many Americans wrongly believe this battle is only being taken seriously in the United States. Some might grant that, in some rare cases, developed European countries such as England, France or Germany might take the fight against corruption seriously. However, this attitude seriously ignores the broad and growing consensus in other parts of the world that corruption is the greatest threat to democracy, stability and economic well-being.

The history of the Convention Against Corruption supports this idea and gives a sense of how universally important these concerns are becoming.[2] The commitment by western hemisphere nations to attack corruption effectively was made at the Summit of the Americas in Miami in December 1994. President Clinton made this a United States' priority coming out of the meeting.

Although the convention is often referred to as the Caldera Convention, after the President of Venezuela who was one of the driving forces behind it, the United States played a major part in developing the document. Ambassador Harriet Babbitt, her staff, and many American experts had a major role in the consultations and the writing of the final document.

The major leadership, however, was provided by the Latin American countries who contributed direction and energy in ensuring the document would be written and approved. President Caldera used his personal influence to get broad agreement throughout the Americas. As important, high-level and well-qualified individuals were sent to the drafting sessions by the majority of the countries. Dividing into groups, experts tackled each section of the document with a commitment to develop an instrument that "works." And, in the end the document represented a broad-based consensus among all of the OAS members.

The country that had the most difficulty with the details of the Convention was the United States. The United States had three general concerns: 1) Federalism (we cannot mandate anti-corruption laws to the States), 2) the separation of powers (the Executive Branch cannot mandate to the Legislative and Judicial Branches), and 3) illicit enrichment (the inability to explain the source of an accumulation of wealth). Through some artful rewriting, the convention was able to accommodate the United States' concerns. It is worth noting that our Latin American colleagues were willing to go much further than the United States and Canada and favored an absolute mandate of the preventive measures as well as provisions that would have made the document far more sweeping in its scope. In fact, many of us on the "American" negotiating team were fascinated by the irony of our opposing a significant strengthening of standards.

(continued on page 26)

[1] The United States signed the convention in June of that year and it will be up for ratification in the Senate within the next 12 months.

[2] For a discussion of this development see Stuart C. Gilman and Carol Lewis, "Public Service Ethics: A Global Dialogue," *Public Administration Review*, Nov/Dec, 1996, vol.56, no.6, p.517.

What Does the Convention Propose to Do?

The Convention is a bilateral treaty. That is, it comes into effect as soon as it is signed by two nations, for those countries. The Convention's major purpose is to ensure transparency of integrity and anti-corruption rules and laws across countries. The Convention also creates a common vocabulary to discuss anti-corruption initiatives, ensuring that no country can get away with euphemisms about fighting corruption while fully engaging in corrupt activities.

The Convention should begin to dampen corruption and ensure that those who violate the public trust can be more easily caught and punished. The impetus behind this apparent change in attitude (at least for the typical American citizen) is not merely altruistic or moral. Over the past several years, organizations, such as Transparency International and the World Bank, have documented the effect of corruption on investment. Private sector investment is discouraged in environments where corruption is rampant. And, many studies show a direct correlation between investment and low levels of public corruption.

Although the Convention has a number of goals[3], there are three primary areas that are of interest to the IG community: preventive measures, anti-bribery statutes such as the Foreign Corrupt Practices Act (FCPA)[4], and extradition agreements.

Preventive Measures

Perhaps the most sweeping area of the entire Convention is the preventive measures section. For IGs there is always a sense that no matter how many victorious battles are fought against specific acts of corruption, the war against corruption continues. In the past, there have been few international standards by which to judge a State's efforts to instill probity. The preventive measures section sets up 12 milestones by which both the United States and other countries can measure the effectiveness of their systems to battle corruption.

Within the first three elements the requirements for each nation to have Standards of Conduct, appropriate measures of their effectiveness, systems of reporting violations to appropriate authorities, mechanisms of enforcement and education of employees are established. In a critically important way it emphasizes the need for systems like the IGs and ethics systems currently in the Executive Branch of the Federal Government.

The next four elements highlight the importance of transparency in government. These include some type of public financial disclosure, an open and efficient procurement system, and control systems designed to deter corruption (e.g. openness of contracting). Additionally, there is a standard to deny favorable tax benefits to individuals who bribe or influence officials of other countries. (See the Anti-Bribery Agreement and Extradition section below for fuller discussion.)

Other standards include laws that would protect whistle-blowers and oversight bodies for "preventing, detecting, punishing and eradicating corrupt acts." The latter represents an international recognition of the role that IGs play in the fight for integrity in government.

Finally, there are standards that include deterrence of bribery by ensuring effective record keeping and transparency of publicly-held companies, to ensure effective accounting controls. The Convention also encourages participation by civil society, i.e., the public, interest groups and the press, in the oversight of government and, last, ensures that each country reviews the relationship between equitable compensation of their civil servants and problems of probity.

This latter issue is often ignored, and when not ignored misunderstood, because of the highly political nature of pay and salaries in the United States and elsewhere. The focus of this provision is on governments that do not pay a wage that an employee could possibly live on. Some countries pay their employees less than 10 percent of what is considered the "minimum living wage." And, other countries actually require a "payment" for such positions, often five or six times the annual salaries. This low wage is often rationalized as being supplemented by "gratuities." In the United States these would be viewed as bribes or illegal gifts. And, now the countries of the Americas have joined us in stating that such a compensation system is a form of corruption.

Anti-Bribery Agreement and Extradition

Using the recommended preventive measures as a platform, the Convention builds in enforcement, by recommending Foreign Corrupt Practices Act-type legislation for all of the countries of the Western Hemisphere. This section emphasizes a number of key legal elements to accomplish these goals. The most important is the elimination of tax advantages for bribing or influencing government officials in other countries. It will surprise even the most cynical that, until this year, one major European power actually had an entry on its corporate tax forms for deducting bribes paid in other countries.

The last major element provides for extradition in cases of corruption when the perpetrator has fled to another country. Very few countries in the Americas had extradition agreements in this area, and the Convention allows for the potential recovery of both the person and illicit gains through the mechanisms of the treaty.

Conclusion

The Convention reflects both the purpose of the IGs as well as the mission of the President's Council on Integrity and Efficiency (PCIE). It signifies that we are not only on

[3] See IGnet Website, http://www.ignet.gov/internal/train/educ.html, under the General subheading, for a complete text of the Convention.

[4] Foreign Corrupt Practices Act, 15 U.S.C. ''78dd, 78ff [EGR 1-025]

the right track, but in a number of ways we are a model to the rest of the world. The laws, structures and experiences of members of the PCIE are invaluable to these countries. Many members can provide guidance as to our successes and our failures in these efforts. And for that reason Article XIV emphasizes that countries will give the "widest measure of mutual technical cooperation on the most effective ways and means of preventing, detecting, investigating and punishing acts of corruption." Over the next several years, I believe the PCIE community will be asked for technical assistance by our sister countries in the Americas. My hope is that we greet this not as a burden, but as a responsibility.

This Convention is also a sign that the greatest contemporary danger to democracy--corruption--has been broadly recognized for the cancer that it is; and that the movement to attack corruption throughout the world cannot be resisted. As the great French novelist, Victor Hugo wrote, "greater than the tread of mighty armies is an idea whose time has come."❑

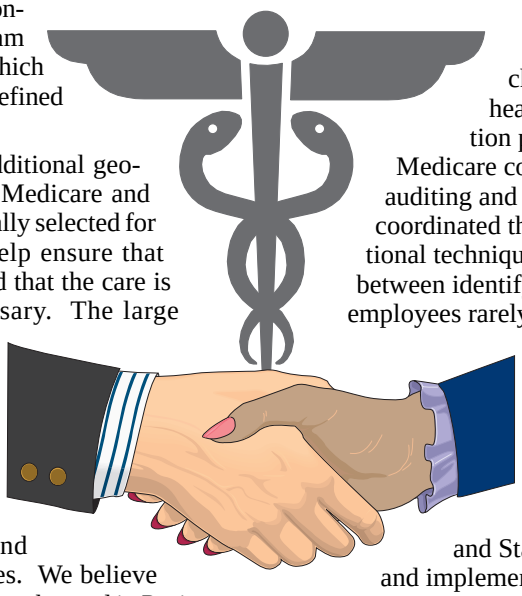
2001: An Investment Odyssey--Operation Restore Trust

by John M. Hapchuk

John M. Hapchuk,
Director, Programs and Operations Health Care Financing Audits Division, Office of Inspector General, Department of Health and Human Services

Initiative Objective

For 30 years, health care expenditures in the United States have risen faster than inflation and population. One factor is the unnecessary cost of fraud and abuse. Operation Restore Trust (Project ORT) is a long-term initiative, sponsored by the U.S. Department of Health and Human Services (HHS), to fight fraud and abuse in Medicare and Medicaid. It has two distinct phases: 1) a 2-year demonstration confined to five States and specific program areas; and 2) a multi-year continuation which will institutionalize the "best practices" refined in the demonstration.



The second phase will focus on additional geographical areas, and it will include all Medicare and Medicaid program areas with a few initially selected for special attention. This project will help ensure that the cost of health care is reasonable and that the care is provided only when medically necessary. The large increases in health expenditures (both appropriate and inappropriate) have caused significant financial stress on the Federal budget, State budgets, and on the beneficiaries who pay "out-of-pocket" coinsurance. Project ORT is designed to protect beneficiaries from health care providers who unfairly, and often illegally, seek to enrich themselves. We believe that many of the techniques developed or enhanced in Project ORT could be transfered and used to fight fraud and abuse in nonhealth areas.

The First 2 Years

Project ORT started as a 2-year demonstration project that developed innovative ways to fight fraud, waste and abuse in the five States with the largest Medicare and Medicaid expenditures. The demonstration was financed by $7.9 million from the Medicare Trust Funds. This funding was designed to supplement existing HHS funds for anti-fraud and abuse activities. An interdisciplinary team of Federal, State and local government representatives targeted Medicare and Medicaid abuses in California, Florida, New York, Texas and Illinois. About 12.4 million Medicare and almost 13.6 million Medicaid beneficiaries live in these States. The project focused on the areas of home health care, nursing homes (including hospices), and medical equipment and supplies. These are three of the fastest growing sectors of Medicare and Medicaid and accounted for about $63 billion in expenditures in 1996. Their rapid growth as well as our evaluation of the inherent risks in the determination of eligibility and provision of services showed that these three areas were ideally suited for the 2-year demonstration.

The 2-year demonstration project changed the way Government fought health care fraud. Prior to the demonstration project, program representatives, Medicare contractors, Medicaid State agencies, and auditing and law enforcement agencies rarely coordinated their attacks on problem areas. Traditional techniques were sequential, lengthening the time between identifying and solving problems. Front-line employees rarely participated in selecting targets and developing strategies to combat fraud. Project ORT broke with tradition by encouraging participants to coordinate their efforts earlier and focus on specific issues in defined locations. Front-line employees were now actively involved early, and national and State-specific plans were developed and implemented.

The Project ORT demonstration cultivated teamwork among various governmental groups, including three agencies within HHS--the Office of Inspector General (OIG), the Health Care Financing Administration (HCFA), and the Administration on Aging (AoA). Other participants included the Department of Justice (DOJ), representatives of State agencies, long-term care ombudsmen, and fraud

(continued on page 30)

specialists. Where before Federal, State and local governments rarely worked closely together, Project ORT used teams made up of these different groups to maximize their talents in an effective combination of auditors, evaluators, quality assurance specialists, program officials, ombudsmen, payment safeguard staff, attorneys, and prosecutors. The teams' use of joint planning, sharing of data bases to target problems, and blending diverse skills has made and will continue to make a major contribution toward restoring financial integrity to Medicare and Medicaid and set an example for others to follow.

One might question what was accomplished by the expenditure of $7.9 million of demonstration funds over the 2 years ended March 1997. Two types of products have emerged so far: 1) "end" products which can be quantified to some degree; and 2) new or enhanced techniques to reduce the incidence of fraud and abuse in health care.

End Products

Through its March 1997 termination, the demonstration phase of Project ORT had produced an impressive number of "end" products, such as:

- identifying $187.5 million owed to the Federal Government;
- resolving approximately 3,600 complaints (out of the 13,000 received) from the project's hotline (1-800-HHS-TIPS);
- obtaining 74 criminal convictions;
- settling 58 civil cases;
- excluding 218 providers from participating in the Medicare and Medicaid programs;
- completing 231 audits, inspections and other reviews with another 98 in process;
- working on 210 investigations and providing litigation support on another 69 indictments;
- training of 2,765 persons at 65 sessions on how to assist senior citizens to identify and report potential health care fraud and abuse; and
- developing evidence to support changes to legislation or regulations on home health agency payments, provider enrollment, billing for nursing services, hospice payments, and Medicare drug payments. Depending on the wording of the laws and regulations, these changes will result in millions of dollars in future Medicare and Medicaid savings.

Strategies For Future Years

The Project ORT demonstration also developed or "fine-tuned" six techniques (strategies) for use in reducing fraud and abuse in health care. We will use these strategies in all of our future Medicare and Medicaid anti-fraud and abuse activities. These strategies will be integrated into our daily activities so that they become our "way of doing business" in HHS.

1. Targeting, Execution and Resolution

Project ORT will continue to develop new ways of working with program managers, using payment data, and profiling possible abusers to help target audits, investigations, and other program reviews on the most abusive providers in certain program areas. Together, reviewers, investigators, auditors and appropriate program managers will employ more sophisticated methods of analyzing claims data to make these assessments. Where appropriate, they will be joined by medical personnel to identify and quantify payments for unnecessary care. These teams will also make referrals to criminal investigators when warranted. In addition, we will coordinate with DOJ and other entities to ensure that monies owed to the Government are collected and accounted for properly.

2. Coordination of Law Enforcement Actions

Project ORT will continue to emphasize increased coordination between program representatives, auditors, evaluators and criminal investigators. We will improve our coordination with other law enforcement agencies, such as the Federal Bureau of Investigation, to further reduce duplication, and work with DOJ so that our final products contain the information essential for criminal and/or civil litigation. As a result, we anticipate a large number of criminal convictions and civil recoveries. We will also ensure that former "problem" providers remaining in the program have stringent corporate integrity plans in place to ensure better compliance with existing health laws and regulations.

3. National Policies and Procedures

Project ORT will continue to identify needed improvements in national policies and procedures to eliminate fraud and abuse. Program evaluations and audits will expand on provider-specific audits and investigations. Both multi-state and multiple provider reviews will focus on individual aberrant providers and the systemic weaknesses allowing for such behavior. This work will measure the extent of problems nationwide and analyze the underlying incentives and weaknesses in the Medicare and Medicaid programs. Project ORT will recommend national policy or system changes to improve these programs. We will continue to monitor the status of policy changes identified in the demonstration.

4. Quality and Program Integrity

Project ORT will facilitate the integration of quality processes with program integrity. State and Federal survey and certification officials visit nursing homes, hospice providers and home health agencies on a regular basis, which places them in an excellent position to spot possible instances of fraud and abuse. Traditionally, their orientation has been on program compliance and certification issues. As part of Project ORT, however, they are trained to identify and report (to Medicare contractors) instances of medically unnecessary or noncovered services. They are provided

billing information from the Medicare contractors before they go onsite. The information that is collected is provided to Medicare contractors for decisions about payment and possible integrity violations. Project ORT will also explore whether this approach can be used in other types of services where quality is reviewed onsite. Prior to ORT, State long-term care ombudsmen have viewed their roles as resolving problems between patients and nursing home/home health agency providers. During the demonstration phase of ORT, they were provided training to expand their roles to identify cases of fraud and abuse.

5. Public Education and Involvement

Project ORT outreach activities will include educating and training aging network personnel, such as local and State ombudsmen and senior volunteers, to better identify and report potential fraud and abuse. We also will continue to operate a "user-friendly" fraud hotline and to develop additional strategies to involve the public. We have begun to establish a working relationship with the American Association of Retired Persons (AARP) and have helped them develop a nationwide survey on health care fraud and abuse. The results of the survey have provided us with information for our own outreach activities. We plan to continue to work with AARP staff as they conduct follow-up work on seniors' knowledge of and attitudes toward health care fraud and abuse. Also, we will contribute a monthly column on Medicare fraud and abuse for publication in the AARP newsletter. We have worked with AARP on their reprinting of the "Medicare Beneficiary HMO Advisory Bulletin" which was originally issued jointly by the OIG and HCFA.

6. Industry Partnerships

Project ORT will proactively involve health care providers. We will provide industry guidance through safe harbors, fraud alerts and other means. Further, we have developed a strategy for establishing partnerships with a small but crucial group of industry and professional groups to publish articles in their newsletters or journals, attend and speak at their meetings and conferences, and work with them to identify areas where we can most effectively focus their work. Also, we are working on a series of information kits for the general public and for industry groups that will educate and encourage individuals to report fraud and abuse. We will work with industry groups to develop voluntary compliance models through which health care providers can operate their own program integrity initiatives. In addition, we will continue to explore the use of a program to enable providers to voluntarily disclose overpayments. Finally, we will establish a fraud and abuse data collection program which can be easily accessed by law enforcement and other legitimate entities.

Summary

Project ORT is an initiative involving Government and nongovernment sectors to reduce the incidence of fraud and abuse in the Medicare and Medicaid programs. It has developed or enhanced six strategies which, so far, have produced impressive financial and program results. We believe that these strategies, appropriately modified, could be applied to other nonhealth programs to assist in preventing or reducing fraud and abuse.❑

Buckless Rogers in the 21st Century

by Robert Rothenberg

Robert Rothenberg, Associate Commissioner for Budget, Social Security Administration

"Buckless" is, perhaps, an exaggeration, but Federal agencies will face the 21st century expected to do more with less in an era of increasing accountability. The balanced budget agreement, however the details play out over the next several years, establishes a fixed "pie" of discretionary spending within which agencies will compete for limited resources. This competition will be framed by the concepts of the Government Performance and Results Act (GPRA) and the ongoing political process.

Currently, we view the budget process as a series of three intertwined steps: formulation, presentation, and execution. These major steps in the budget process are outlined in "A Citizen's Guide to the Federal Budget" which is part of the Budget of the United States for Fiscal Year (FY) 1998. Although this summary relates specifically to the FY 1998 budget, it provides a general timeline for the overall process.

For agencies such as the Social Security Administration (SSA), the focus is on the portion of our total budget that represents our administrative costs and is part of what is called discretionary costs. SSA's discretionary costs are driven by measurable workloads (e.g. claims to process) and the workyears and dollars needed to process these workloads. The administrative budget is formulated based on actuarial projections of national workloads and a productivity analysis which takes into account the policy and procedural changes necessary to achieve SSA plans. These plans are driven by our strategic plan and Presidential and Congressional priorities, including funding constraints, legal decisions, etc. Issues are "staffed-out" and discussed to decide on options to fund competing priorities and maximize the use of taxpayer dollars.

A critical part of this process is the technical calculations involved in translating workloads and policies into workyears and dollars. Workyears translate into dollars required to fund both the personnel costs and "other objects" costs, such as postage and supplies, of processing the work. In justifying your budget to the Office of Management and Budget (OMB) it is important to show the process you went through to get your numbers and the impact of incremental changes to those numbers. To do this

(continued on page 34)

Major Steps in the Fiscal Year Budget Process

Formulation of the President's budget for the fiscal year.	Executive Branch agencies develop requests for funds and submit them to the Office of Management and Budget. The President reviews the requests and makes the final decisions on what goes on in his budget.	February - December
Budget preparation and transmittal.	The budget documents are prepared and transmitted to the Congress.	December - February
Congressional action on the budget.	The Congress reviews the President's proposed budget, develops its own budget, and approves spending and revenue bills.	March - September
The fiscal year begins.		October 1
Agency program managers execute the budget provided by law.		October 1- September 30
Data on actual spending and receipts for the completed fiscal year become available.		October - November

the budget must be justified on strong policy and technical grounds. This is particularly critical in the passback and appeal process, where critical decisions need to be made by OMB and the White House on competing priorities.

Once formulation is complete, the President's budget must be presented to the Congress. Each agency provides budget schedules and related technical material to OMB as well as supporting material on policy decisions. The President then gives his State of the Union message followed by the presentation of the Administration's unified budget. SSA, along with other agencies, prepares supporting materials for its piece of the total including a press release on the budget request, a detailed justification for the Appropriations Committees, appropriations hearings testimony, and material used for briefing congressional staff on the budget request.

In recent years, the budget has become more integrated as a larger number of committees have been required to agree on budget issues before the House and Senate Appropriations Committees can begin work. First, the Budget Committees in both Houses must work out the details of the Budget Resolution followed by allocations to the Appropriations Committees and distributions to the subcommittees. In addition, the authorizing legislation may be required before funds can be appropriated. If we are lucky we actually get all of this worked out and get an appropriation by the beginning of the fiscal year. Let's hope this or some other process gets us our funding on time as we move toward the 21st century.

Well, we formulated the budget, presented it to Congress, and have an appropriation. The focus now shifts to executing the budget for that fiscal year--getting done what we planned for and told Congress we could do if it provided the authority and the funding. The technical process right now includes OMB apportionment, allocating resources provided in the apportionment to components within the agency consistent with workload and operating plans based on executing the agency plans. Execution of the budget is an ongoing process; adjustments are made throughout the fiscal year to ensure available resources are maximized to meet both anticipated and unanticipated workload demands and agency priorities.

Although I think that the core process will stay the same for some time--particularly the need for sound budget development, well organized presentations, solid execution and accountability--it is becoming apparent that the current, 105th Congress intends to place emphasis on the implementation of GPRA, enacted by the 103rd Congress.

With its combination of strategic plans, performance plans, and consultation among agencies and congressional oversight staff, GPRA is designed to provide a concrete, understandable link between the funds invested in and the gains received from Federal programs. As OMB Director Franklin Raines noted recently:

> "One reason for the deep disaffection with government in this country at all levels -- state, local, and national -- is that we poorly explain to the American public why the government does what it does....Being able to answer the public's questions about what they get for the money we spend should go a long way toward restoring their faith in the ability and interest of the government to do the right thing. This is an era of fiscal limits. Resources are scarce. Not every priority can be met, nor all needs satisfied. Every program must count. So we must ask: which programs are effective, and which are not? GPRA is intended to help all of us obtain better answers to those questions." (Testimony before the Senate Appropriations and Governmental Affairs Committees, June 24, 1997.)

As GPRA is implemented, we will need to relate resource requests to "outcomes" as well as "outputs." It will no longer be enough for an agency like SSA to say: If you give us X dollars we will process Y claims. Under GPRA, if SSA receives X dollars, it still will be expected to process Y claims but it will also be expected to commit to specific outcomes, such as a given customer satisfaction or payment accuracy rate.

The GPRA parallel for an IG may be that you will be expected to continue to process X number of successful prosecutions or collect X number of dollars; but, in addition, you may be expected to demonstrate how those "outputs" translate into an "outcome" such as a percent reduction in program fraud. The House and Senate Appropriations Subcommittees which oversee the agencies funded through the appropriations for the Departments of Labor, Health and Human Services, Education, and Related Agencies, have already exhibited an interest in monitoring IG performance and included the following language for each OIG in the conference report accompanying the FY 1997 appropriations:

> "The conferees believe that all of the Inspectors General need to do a better job of accounting for and tracking the savings that they claim to generate by their efforts. More attention must be paid to how much money is actually collected each year and paid back to the Federal government. The conferees direct the Inspector General to report to the Committees each quarter on:
>
> 1. The actual payments, as a result of fines, restitutions, or forfeitures, made to the United States Government as a result of his activities; and
> 2. How "funds put to better use" were used; this report must identify funds made available for use by management and the programs, projects, and activities that were increased as a result of these funds."

The difficulty in implementing GPRA arises in developing and measuring the performance goals. It is easy for an agency to measure objective workload outputs such as claims processed or passports issued; accounting systems are, generally, designed to measure quantities. It is, however, more difficult to measure outcomes such as improved customer satisfaction or deterred program fraud and abuse, which tend to be subjective.

For example, imagine operating a national chain of restaurants like the Interstate Baker of Bagels (IBOB). As the executive in charge of evaluating customer satisfaction

and developing a strategy to improve satisfaction, you decide to have each restaurant put customer satisfaction surveys on each table. As the surveys begin rolling into your office, you realize that there are several factors influencing customer satisfaction which you need to consider as you develop your remedial strategy:

- A large majority of returned surveys are critical of service. Does this mean that service is generally poor? Or are satisfied customers not filling out the survey cards? You may be more likely to hear from the customer whose order was incorrectly served than the customer whose meal was fine.
- When and where are complaints being generated? Are people complaining about waiting times during the Sunday brunch "rush" or during the graveyard shift when the restaurants are not busy? Service that is considered too slow by busy executives in the Northeast may be too brusque for the retirees in the South.
- Are any of the complaints related to matters which are out of the company's control due to Federal, State or local regulations?
- The surveys suggest a strong customer demand to add a carry-out/delivery service option. Should this be implemented regionally, to reflect customer demand, or nationally? Should carry-out/delivery be a workload added to existing restaurants or should they be stand-alone installations? Should the carry-out/delivery menu be an abbreviated version of the full-service restaurant menu? Would centralized carry-out/delivery services permit you to consolidate restaurants? What impact, if any, would these changes have on customers who preferred to eat-in (e.g. longer wait for food, sense of restaurant being too busy)?

Similarly, any evaluation of customer satisfaction with Federal agencies needs to consider these sorts of subjective influences. Despite the most efficient, courteous service possible, the citizen whose disability claim, mortgage application, or disaster relief claim was denied is not likely to rate the agency's customer service highly. Clearly, the performance measure decided upon and the target established are critical. If you have not been involved in deciding the targets and measures for your agency's FY 1999 budget, I would strongly encourage you to participate in this process in the future.

So what does all this mean to you? How will the results-oriented management requirements of GPRA impact budget formulation, presentation and execution for an IG organization? I see several possibilities:

- An IG could receive an appropriation that is simply a "pot of money" without traditional budget controls. Under this scenario, in theory, you would be free to make whatever efficiencies you see fit to meet performance goals including outsourcing work and upgrading equipment.
- You could become self-supporting; that is, your operating expenses would come from monies recovered from successful prosecutions. While this would tend to encourage further diligence in investigation and prosecution of fraudulent activities, such a funding mechanism would be hard to implement. Would IG budgets be based only on monies recovered, or would they include some amount representative of the scope of fraudulent activities discovered and terminated? Would IGs receive any funding based on the "value" of deterrence and how would that value be measured?
- IGs could "compete" for funds. This could be competition for resources within your agency. Or, it could be IGs competing against each other based on answers to questions such as: Where is the biggest bang for the buck: investigating and prosecuting Social Security fraud? Medicare fraud? or a nuclear threat to our environment? Who decides?

What is certain about budgeting in the future is the continual competition for scarce resources, the necessity to clearly define what you will deliver for those resources and increased accountability for how those resources are used including the actual outcome produced. To win a larger piece of the budget pie, an agency will need to display superior performance, whether under GPRA or in an alternate measurement system. In addition to developing and working toward GPRA measures, agencies will need to maintain technical proficiency in budgeting to assist in linking resource requirements to outcomes.

So given all this, what is the best course of action for you to take to make sure that the critical responsibilities you have to the American people continue to be met? I'll leave that up to you!❑

Byting Crime: Cybertrapping the Predators

by Thomas G. Staples

Thomas G. Staples,
Associate Commissioner for
Financial Policy and Operations,
Social Security Administration

Introduction

At some point in their lives, nearly all Americans receive benefits from the Social Security Administration (SSA). The sheer magnitude of SSA's programs is enormous. In FY 1996, SSA's programs accounted for nearly 25 percent ($386 billion) of the $1.6 trillion in Federal expenditures. More than 50 million Americans currently rely upon SSA programs. In 1996, SSA issued 15.9 million new and replacement Social Security numbers (SSN), processed 239 million earnings records, paid $367 billion in benefits, and issued 9 million Personal Earnings and Benefit Estimate Statements.

This article provides a brief summary of SSA's business process and the role the computer plays in record keeping and control of the business process. It also briefly describes the role SSA employees play and the nexus between employees and the automated systems controls. It closes with a short description of the next steps in capturing computer anomalies that may point to fraud and/or abuse. Because of the sensitive nature of this material it has been kept at a general level. Those auditors and investigators who have business reasons to further pursue this material should contact the author.

Number/Wages/Claims

The SSA business process consists of several well-defined sets of transactions.

The initial transaction is the one that causes a SSN to be issued in the name of a given individual. This transaction usually occurs during the first 12 months of life or upon arrival in the country from abroad. Currently, the parents of over 70 percent of all newborns request the SSN to be issued at the time of birth.

Subsequent to initial issuance there are sometimes changes to these basic records. Name changes as women marry are the most frequent record changes. Throughout the lifetimes of the number holders there are occasions when employers, and various State and Federal agencies, will verify the correctness of the name and number with SSA for use in their record systems.

Another well-defined transaction is the recording of earnings to the name and number issued. These transactions occur annually through reports from employers and from reports filed by self-employed individuals. They may also occur from time to time when the number holders review the earnings posted to their earnings records and identify additions or deletions that need to be made. In addition to issuing the original SSN and posting earnings to the SSN, other defined SSA transactions relate to claims the number holder may file for benefits and subsequent events related to the payment of these benefits, e.g. address changes, death reports, etc.

Establish/Update/Query/Delete

In order to administer SSA's programs, these basic transactions, and others, have been incorporated into a series of well-defined business processes. Each process has a clear point where records are established, and a clear sets of rules about whom may make changes or updates to these established records. In addition, the information collected in each business process can be accessed or queried as necessary by SSA employees and others who are authorized to have access to the information. Finally, if a record is to be deleted as part of the business process, there are clear and tightly controlled rules on the circumstances of each deletion.

These controls for establishing records, updating records and querying records are enforced by SSA's automated system through "access control" software that must be complied with or the work will not be processed by the system. While the foregoing information provides some insight to the basic business functions of SSA, it is incomplete without an understanding of the role human beings play in operating the SSA business processes.

The Audit Trail

When an authorized SSA employee establishes a record, whether it is a new SSN, a wage report, a claim filed, or an address changed, a permanent annotation is

(continued on page 38)

made in SSA's automated systems that record identifying information about the individual who established the record. Similarly any additions or deletions to the record are permanently recorded to SSA systems along with information about the individual who made the revision or deletion. In addition to information about the employee, other basic data are also automatically recorded by the system--time of day, office, computer terminal, etc. The automated system accomplishes these tasks in part by automatically and routinely recording the personal identification number (PIN) of the person entering the transaction. The PIN was assigned when the person first obtained access to the automated system. Through computer software controls, the PIN authorizes the SSA employee to access those parts of the system he/she needs to do his/her job but prevents the employee from all other parts of the system. For most purposes SSA uses the employee's position description as the control for what he/she can do in the system.

The PIN is permanent and is not changed throughout the career of the employee at SSA. The employee is protected from abuse of his/her PIN because the employee must also use a password known only to the employee to gain access to the system. The employee may change the password at any time and must change it on an established schedule. All systems records are stored indefinitely and can be readily accessed as needed by management or other authorized personnel e.g. security officers, investigators, etc. A portion, or extract, of these records exists in the form of a security audit trail (SAT).

While there are many day-to-day uses that SSA makes of the PIN file and the related SAT, the following is a short summary of some of those uses:

- Each departing SSA employee personnel action is checked against the PIN file to ensure systems access is correctly maintained, e.g. the employee's systems privileges are canceled if that action had not already occurred.
- Each reassignment from one job to another triggers a review, and change if needed, of the employee's systems capabilities.
- Highly sensitive SSA transactions are listed on the system for the information and use of the supervisor of the employee. Some of these transactions are selected for the supervisor to review and can only be cleared from the system log by the supervisor's PIN.
- For transactions where fraud and/or abuse may have been found in the past, two PIN's are required for the transaction to proceed through systems processing.

Also, the PIN and SAT files have been significant tools for the Office of the Inspector General's investigations' staff in determining the circumstances and facts in cases under review. Similarly, these automated records have played prominent roles in judicial proceedings against both employees and program clients charged with fraud and/or abuse. For example, the investigation and prosecution of a recent and complicated case involving credit cards and bank fraud relied extensively on SSA's record systems. The system identified instances where employees accessed the SSA record of the bank clients in order to obtain personal information that nongovernment individuals used to validate the credit cards. The records served as the key investigative documents and led to successful prosecutions.

These automated tools have been especially valuable in speeding up the rate at which investigations can be conducted. Many key events can be determined in a matter of minutes. More "global" searches of "traffic" for an entire office or for an employee's work over a period of months can often be accomplished in hours or at most a day or two. A few short years ago such requests would have taken weeks, if possible at all.

Next Generation Systems

With the automated record keeping capabilities described here, there are many valuable computer software programs that can be used to manipulate the data. Some of these tools also allow the user to search for anomalies in the data and to highlight certain patterns for further scrutiny. SSA uses many such tools today. With the increased computing speed and data compression that have occurred over the past decade and which are likely to continue, much more sophisticated tools can be developed. SSA is engaged in a multi-year effort in this regard.

One of the historical limitations to data sets for SSA and others has been that each major business process usually is separate from other business processes. In SSA for example, claims for benefits are in a system distinct from the wage system and both of these are distinct from the SSN system, and so on. Sometimes the possibility for investigating or auditing a particular event requires gathering and associating data from two or more of these systems. For example, a newly issued number and a claim for benefits within a short period of time could point to program fraud. Other examples include a claim for benefits shortly after a record of death is deleted from SSA's record systems, and sensitive systems queries that cannot be related to agency workloads.

With the automated systems capabilities under development these cross program "searches" for anomalies will be much quicker and much richer in terms of likely outcomes.

To meet this type of future scenario, SSA has to face challenges not previously attempted by others in the public or commercial sector. Because of the physical size of the systems (there are roughly 20 million "transactions" per day), the mere search or scanning function is a challenge. Also, the necessary communications across multiple systems poses additional challenges. While the tasks associated with developing such systems sometimes seem daunting, at the end knowing something has been accomplished that has not been done before is satisfying. The next generation for SSA's information systems security, in particular the anomaly detection software, clearly falls into this category.❑


UNITED STATES of AMERICA
PCIE
PRESIDENT'S COUNCIL on INTEGRITY & EFFICIENCY


UNITED STATES of AMERICA
EXECUTIVE COUNCIL on INTEGRITY & EFFICIENCY