

The JOURNAL OF PUBLIC INQUIRY

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES



SUMMER 1995

The JOURNAL OF PUBLIC INQUIRY

Editorial Board

Raymond J. DeCarli, Department of Transportation,
Office of Inspector General (OIG)

Stuart C. Gilman, Office of Government Ethics

Maryann Grodin, Council of Counsels to the Inspectors General

Donald Mancuso, Department of Defense OIG

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

Robert S. Terjesen, Department of State OIG

Wendy Zenker, Office of Management and Budget

David C. Williams, Nuclear Regulatory Commission OIG, Editor

Staff

Editorial Services

Karen M. Shaffer, General Services Administration OIG

Printing

Nicholas T. Lutsch and Jeff Rosen, Department of Defense OIG

Public Affairs

Robert S. Terjesen, Department of State OIG

Distribution

Martie Lopez-Nagle, 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 the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. Articles should be approximately 6 to 12 pages, doublespaced and should be submitted to Ms. Martie Lopez-Nagle, Assistant to the Editor, Office of Inspector General, Nuclear Regulatory Commission, Washington, D.C. 20555.

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

Profiles of the New Inspectors General <i>Author: Marian C. Bennett</i>	1
Adventures in Cyberspace: An Inspector General's Guide to the Internet <i>Author: Jerry Lawson</i>	7
Fully and Currently Informed: How Assistant Inspectors General Keep Their Bosses Aware Without Drowning Them in the Age of Information <i>Authors: AIGA viewpoint- James Ebbitt and Pete McClintock</i> 15 <i>AIGI viewpoint - Donald Mancuso and Patrick Neri</i> 15	
Dogs That Hunt: The Auditors and Investigators <i>Author: Stephen A. Trodden</i>	21
Fear of Flying: Acceptable Levels of Risk are Necessary to a Successful OIG Investigative Program <i>Author: Phillip A. Rodokanakis</i>	25
Partners Against Crime: Using a Culture of Collaboration to Win in the Fight Against Health Care Fraud <i>Author: June Gibbs Brown</i>	29
Case Notes: Recent Court Decisions on OIG Powers and Authority <i>Authors: Alexandra B. Keith and Maryann L. Grodin</i>	33
Things Your Mother Never Taught You: The OIGs' Auditor Training Institute and Criminal Investigator Academy <i>Authors: Andrew J. Pasden, Jr. and Kenneth R. Loudermilk</i>	37
Practical Evaluation for Public Managers: Getting the Information You Need <i>Authors: Michael Mangano, Penny Thompson, Jack Molnar, and Brenda Stup</i>	41
PCIE/ECIE Calendar	46



Profiles of the New Inspectors General

by Marian C. Bennett, Inspector General, United States Information Agency

The following profiles introduce the new Inspectors General (IGs) appointed by President Bill Clinton. Appointment dates are in parentheses after each name.



Marian C. Bennett

Marian C. Bennett - United States Information Agency (November 1993)

A New York City native who grew up in Minneapolis, Ms. Bennett graduated with honors in American history from Harvard and received her law degree from the University of Pennsylvania. Her Federal career spans 20 years, and includes experience at the Department of Energy Office of Inspector General (OIG) as a senior attorney, at the National Labor Relations Board as an attorney, and at the Department of Housing and Urban Development (HUD) as an executive assistant to the General Manager of the New Community Development Corporation. Ms. Bennett has two children, enjoys photography and swimming, and is active in several social organizations.



Jacquelyn L. Williams-Bridgers

Jacquelyn L. Williams-Bridgers - Department of State (April 1995)

Ms. Williams-Bridgers brings more than 16 years of experience in Federal auditing and evaluation to her position. In 1994, she was one of only 10 Federal employees to receive the distinguished Arthur S. Flemming Award. Other honors include the General Accounting Office's (GAO's) Meritorious Service Award. She began her Federal career with GAO, where she rose to the position of Associate Director for Housing and Community Development Issues. During a 1-year break in her GAO service, she joined the HUD OIG's Fraud Control Division. A native Washingtonian, she received her undergraduate degree from Syracuse University and a year later earned her master's degree in public administration from Syracuse's Maxwell School of Public Affairs and Citizenship. She and her husband have a son and a daughter.



Michael R. Bromwich

Michael R. Bromwich - Department of Justice (June 1994)

Mr. Bromwich brings extensive legal experience to his position. As a partner in the law firm of Mayer, Brown & Platt, he specialized in white collar criminal defense work. He established a pro bono program in his firm to enable young lawyers to handle criminal cases in D.C. Superior Court. Mr. Bromwich served as an Assistant U.S. Attorney for the Southern District of New York. Earlier, as the Associate Counsel in the Office of Independent Counsel: Iran-Contra, he coordinated the grand jury investigation and was one of the government's three trial attorneys in the case of the United States v. Oliver L. North. Mr. Bromwich received his bachelor's degree summa cum laude, his master's degree in public policy, and his law degree from Harvard. He and his wife, who is also an attorney by profession, have three children.

(continued on page 2)



June Gibbs Brown

June Gibbs Brown - Department of Health and Human Services (November 1993)
Ms. Brown has been the IG of the Navy's Pacific Fleet at Pearl Harbor, Hawaii, the Department of Defense (DOD), the National Aeronautics and Space Administration, and the Department of the Interior, in addition to holding a variety of positions in private industry. She has received numerous honors and awards, including DOD's Distinguished Service Medal, the Joint Financial Management Improvement Program's Financial Management Improvement Award, and the Association of Government Accountants' (AGA) Robert W. King Award. A fellow of the National Academy of Public Administration, Ms. Brown has also served as national president of AGA, served on the Boards of Directors of the Federal Law Enforcement Training Center, the Interagency Auditor Training Program at the Department of Agriculture (USDA) Graduate School, the National Contract Management Association, and the Hawaii Society of Certified Public Accountants (CPAs). She was also the national chairperson of the Interagency Committee on Information Resources Management. Ms. Brown received her bachelor's and master's of business administration degrees from Cleveland State University and her law degree from the University of Denver.



Martin J. Dickman

Martin J. Dickman - Railroad Retirement Board (October 1994)
A Chicago native, Mr. Dickman was a prosecutor for the Cook County, Illinois State Attorney's Financial and Governmental Crimes Task Force before his appointment as IG. Prior to that, he spent nearly 20 years as a member of the Board of Trade of the City of Chicago, where he served as presiding judicial officer at Exchange judicial hearings, and as a director and member of the Executive Committee. In this role, he established policy, long range strategic plans, and international development for the multimillion dollar Board. Mr. Dickman practiced law with a private firm, presided over tax-related disputes as a hearings referee for the Illinois Department of Revenue, interpreted and drafted legislation as Legislative Counsel in the Illinois House of Representatives, and served as an Assistant Corporation Counsel for the City of Chicago. Mr. Dickman received his bachelor's degree from the University of Illinois and his law degree from DePaul University.



Susan Gaffney

Susan Gaffney - Department of Housing and Urban Development (August 1993)
Ms. Gaffney joined the IG community in 1979 as Director of Policy, Plans, and Programs for the Agency for International Development. She moved to the General Services Administration (GSA) as the Assistant Inspector General for Policy, Plans, and Management, and was promoted to Deputy IG. From GSA, she moved to the Office of Management and Budget (OMB) as Acting Assistant Director of the Financial Policy and Systems, Management Integrity, and the Cash and Credit Branches. She developed OMB's financial management strategy, and developed policy for implementation of the Chief Financial Officers Act. In 1991, Ms. Gaffney was appointed Chief, Management Integrity Branch, where she developed governmentwide policy relating to the Federal Manager's Financial Integrity Act, OMB's High Risk List, and the IG Act. Ms. Gaffney received a master's degree from the Johns Hopkins School of Advanced International Studies. She is a recipient of the Presidential Rank Award for Meritorious Executive and the Joint Financial Management Program Improvement Award for Distinguished Leadership.



Eleanor Hill

Eleanor Hill - Department of Defense (February 1995)

Prior to her appointment as IG, Ms. Hill spent 15 years with the United States Senate's Permanent Subcommittee on Investigations, where she managed a wide variety of complex domestic and international investigations. As a result of those investigations, she was directly involved in the legislative process in a number of areas, including substantial work on comprehensive anti-crime and anti-drug legislation, student loan reform proposals, and drug enforcement related amendments. Prior to her Senate employment, Ms. Hill was an Assistant United States Attorney, and a special attorney with the Department of Justice's Organized Crime Strike Force in Tampa, Florida. Ms. Hill received her bachelor's degree magna cum laude and her law degree with high honors from Florida State University. She and her husband, who is also an attorney, have one son.



Luise S. Jordan

Luise S. Jordan - Corporation for National and Community Service (October 1994)

Ms. Jordan brings more than 17 years of financial management experience to her position. She was a senior manager with Price Waterhouse LLP's Office of Government Services, where she directed the audits and other projects for Federal agencies, government corporations, and government-sponsored enterprises. She also served as a technical expert on Federal auditing and accounting issues. At the GAO, she directed the first consolidated audits of the USDA and Department of Veterans Affairs (VA) life insurance and compensation, pension and education programs. As a project manager in GAO's accounting group, she provided technical assistance and guidance to resolve complex financial reporting, budget and cost, and pension accounting issues. Prior to joining GAO, she was the general accountant for CSX Chessie Systems. Ms. Jordan is a graduate of the University of Maryland and a CPA. She and her husband, an environmental engineer, have four children and two grandchildren.



Valerie Lau

Valerie Lau - Department of the Treasury (October 1994)

Ms. Lau's background includes 13 years of Federal service and 4 years as a career consultant specializing in audit training with an international career management firm. She also served as an adjunct faculty member of the USDA Graduate School. An Oakland, California, native, Ms. Lau joined the Department of the Treasury as a taxpayer service representative for the Internal Revenue Service. She served as executive director of the Western Intergovernmental Audit Forum, which honored her with its 1990 Leadership Award, and worked as a senior evaluator for GAO and as an auditor with the Defense Contract Audit Agency. Prior to her appointment as IG, Ms. Lau was Director of Policy for the Office of Personnel Management and liaison with the National Performance Review. She received her bachelor's degree from the University of California at Berkeley and a master's degree in career development from John F. Kennedy University in Orinda, California. She is the author of a training manual for the Institute of Internal Auditors and an article for the [GAO Review](#).

(continued on page 4)



Wilma A. Lewis

Wilma A. Lewis - Department of the Interior (April 1995)

Ms. Lewis, a native of St. Thomas, U.S. Virgin Islands, brings an extensive legal background to her position. She most recently served as the Associate Solicitor, Division of General Law, Department of the Interior. Ms. Lewis began her legal career as a lawyer with the firm of Steptoe and Johnson in Washington, DC. She then joined the Civil Division of the U.S. Attorney's Office in Washington, DC, as an Assistant United States Attorney. Ms. Lewis has served on the Civil Justice Reform Act Advisory Group for the U.S. District Court for the District of Columbia, and is currently a member of the Advisory Committee on Local Rules for the District Court. She has served as a lecturer and instructor on issues of employment discrimination law, and as a Professorial Lecturer in law in trial advocacy at The George Washington University National Law Center. Ms. Lewis received her bachelor's degree with distinction from Swarthmore College, where she was elected to Phi Beta Kappa. An active alumna of Swarthmore, she serves on the Board of Managers and as an admissions representative. She was also a member of the Washington Area Tennis Patrons Foundation, Inc. Ms. Lewis received her law degree from Harvard.



Charles C. Masten

Charles C. Masten - Department of Labor (December 1993)

Mr. Masten began his law enforcement career with the Federal Bureau of Investigation (FBI) as a special agent in Memphis in 1973. Four years later, he was transferred to the Little Rock office where he served as supervisory special agent for several program areas. In 1985, he came to Washington, DC, where he handled special inquiries relating to Presidential appointees. Two years later, he was promoted to program manager of three of the six FBI security programs. He also served as an Inspector's Aide in Place where he conducted inspections of FBI field offices throughout the United States. Prior to becoming IG he was the Department of Labor's Deputy IG. Prior to his tenure at the FBI, Mr. Masten served as a U.S. Navy officer in Vietnam. He also served as an assistant national bank examiner and as a chief operations officer for a Georgia bank. Mr. Masten received his bachelor's degree from Albany State College and his MBA from the University of Arkansas.



George J. Opfer

George J. Opfer - Federal Emergency Management Agency (November 1994)

A 25-year veteran of the U.S. Secret Service (USSS), Mr. Opfer was the Assistant Director of the Office of Investigations before his appointment as IG. In that capacity, he was responsible for the overall planning and direction of criminal investigations and detection for the USSS. Prior to that position, he served as Assistant Director for the Office of Inspection. As a special agent, he conducted counterfeit investigations and coordinated emergency preparedness for the Presidential Protection Division. Mr. Opfer is a past recipient of the Presidential Rank Award for Meritorious Executive. Mr. Opfer received a bachelor's degree in management from St. John's University. He and his wife have three children.



Jeffrey Rush, Jr.

Jeffrey Rush, Jr. - Agency for International Development (September 1994)

Mr. Rush has been a member of the OIG community for 24 years. He began his career as a criminal investigator with the USDA OIG, rising through the ranks to the position of Deputy Assistant Inspector General for Investigations. During the year prior to his appointment as IG, he served as acting IG for the Peace Corps. Prior to joining the OIG community Mr. Rush served in the United States Army, where he was trained as a counterintelligence agent. Mr. Rush, a graduate of Baker University in Baldwin City, Kansas, received his law degree from George Mason University. He has been admitted to the Virginia and District of Columbia Bars, and is a member of the American Bar Association. As a volunteer, Mr. Rush has been active in his community in a pro bono housing law project and as an attorney for a homeless shelter. He and his wife have a son and a daughter.



Roger C. Viadero

Roger C. Viadero - Department of Agriculture (October 1994)

A New York City native, Mr. Viadero brings more than 25 years of law enforcement experience to his position. During his 15 years with the FBI, he served as chief internal auditor for the New York Division, management consultant on internal audit and audit control procedures for police departments across the country, professor at the FBI National Academy at Quantico, Virginia, and most recently as chief of the audit unit in Washington, DC. Before joining the FBI he served with the New York City Police Department as an officer and homicide investigator. Mr. Viadero received his bachelor's degree in public accounting and his master's degree in business administration from Pace University in Pleasantville, New York. He is the author of numerous articles on law enforcement and management. □



Adventures in Cyberspace: An Inspector General's Guide to the Internet

by Jerry Lawson



*Jerry Lawson, Counsel to the
Inspector General, National
Archives and Records
Administration*

What is the Internet, and why should I use it?

The Internet is a global linkage of large computers, mostly owned by businesses, universities, and governments. Most of these larger machines have smaller computers attached. The key connections are special high capacity leased telephone lines capable of carrying large amounts of data. The fascination of the entertainment and news media communities with the sensational and trivial aspects of computer telecommunications has created some widespread misperceptions. The truth is that the most significant part of the online world, the Internet, was originally designed by the Department of Defense as a means of enhancing the productivity of government officials (originally mostly military, with a sprinkling of users from the academic community and high tech businesses).

The Internet is no longer managed by the Federal Government, and literally millions of other people have found that it can be used for other purposes, ranging from political organizing to disseminating rock videos. The same power that makes the Internet well suited to accomplish these diverse tasks makes it also eminently well suited to accomplish its original purpose: helping government employees communicate and perform their work more efficiently.

Exactly how would it benefit me if I could go online with Internet?

By learning at least the bare minimum necessary to let you use electronic mail (e-mail), and/or the Internet, you can work more productively. For most Federal employees, e-mail is by far the most valuable online function. For little or no charge, you easily can send and receive messages almost instantly from people across town—or on another continent. If your organization has widely dispersed geographical components or your employees travel frequently, obtaining Internet accounts from a service provider with many local access telephone numbers can result in major savings on telephone, fax and postage bills. Aside from often being cheaper than the alternatives, e-mail is qualitatively superior in some ways, and more and more

people are deciding that they prefer e-mail to paper or telephone communications for most purposes. No postal delays. No illegible faxes. No voice mail. No telephone tag.

Recently the National Archives and Records Administration (NARA) Inspector General (IG) decided that he should coordinate with the Office of Management and Budget (OMB) before implementing a particularly innovative approach in his agency. Using e-mail, the IG in

question had his idea completely reviewed and approved by senior OMB management in 12 hours. As we all know, in the Federal Government, paper does not flow at that speed. E-mail can.

There are several reasons to prefer e-mail rather than telephone communications in most situations. E-mail is less intrusive for the recipient. I know my message won't interrupt the recipient at an inconvenient time, as a telephone call might. People read their e-mail only when they want. Another advantage of e-mail is that being brusque and



(continued on page 8)

An Inspector General’s Thumbnail Guide to Key Internet Features

Feature	Purpose	Drawbacks	Comments
E-mail	Easily send and receive electronic messages.	Not everyone has an e-mail address (yet).	Most valuable Internet feature for most business users. Can send and receive e-mail to and from other networks (CompuServe, etc.).
Mailing Lists	System under which e-mail sent to a central location is “echoed” to “subscribers.”	Can be difficult to learn about relevant ones. Some have low “signal to noise” ratio (i.e., there’s a lot of chaff).	Extremely useful for keeping in touch with others who are interested in the same topics. May be public or private, moderated or unmoderated. “IGNet” runs many lists dedicated solely to IG topics.
Newsgroups	Collections of e-mail messages on special topics (over 12,000 at last count).	Most have low “signal to noise” ratio. So many interesting topics, it’s easy to get distracted.	Excellent way to get free technical support, do research or get in contact with experts on specialized subjects.
FTP (File Transfer Protocol)	Transfer files to and from distant computers.	Can be difficult to use unless you have good interface software. Often hard to learn about good files.	Can download wide variety of free files, including: software updates and bug fixes, copies of Supreme Court decisions on day of issue, etc. Related search tool known as Archie will rapidly search for a particular file world wide.
Gopher	Finding aid that adds user-friendly menus to help find Internet resources.	Can only use data that someone has linked to a gopher site.	Fast operation. Related search tool known as Veronica will search gopher menus world wide easily.
WWW (World Wide Web)	A “turbo-charged gopher” system: very easy to use “point and click.” “Hypertext” adds graphics, sound and even video to the gopher text interface.	Operates slowly if graphics feature is used. Difficult to find WWW sites with much useful legal information.	Sometimes called the “Swiss Army Knife of the Internet” because it can be used to access ftp, Telnet, mail, etc. Easiest to use, most spectacular and fastest growing Internet feature. You can speed up operations by turning off the graphics feature. Can be used to inexpensively present information to the public through “posting” of a WWW page.
Telnet	Can log into a remote computer and operate it as if you were at a terminal directly connected to that computer.	Most of the destination computers that allow telnet access require the use of the difficult UNIX operating system.	Can be difficult to navigate after logged into the remote computer.

to the point is not considered rude. When calling someone on the telephone, most people feel at least some slight sense of social obligation to chitchat for at least a while before getting down to business, and socialize a little more after conducting business. With e-mail, by contrast, if someone asks you a question, all you have to do is hit the "Reply" button to quote the question, and enter "Yes" or "No," as appropriate. You can be more expansive if you wish, but in this environment no idle chitchat is necessary. People won't think you are rude, just efficient. Finally, I like to make notes of what was said in important communications. With telephone conversations, this means hasty, illegible scribbling and hoping I can remember all the key points. With e-mail, all I do is select the "Print" command. It's even more efficient if you have a good e-mail program that lets you organize and store old messages on disk with a "drag and drop" filing system. Instead of rummaging through a file cabinet, you can use powerful automated sorting and searching tools to find the data you need.

Another benefit from having an e-mail connection is the ability to subscribe to free Internet mailing lists that relate directly to your work. An Internet mailing list allows a message sent to a central address to be automatically forwarded to all subscribers. There are literally thousands of such Internet mailing lists for various special interest groups.

IGNet, an interagency working group, operates 12 mailing lists, some general and others for specialized groups within the Office of Inspector General (OIG) community. There is a list for investigators, one for auditors, one for Executive Council on Integrity and Efficiency discussions, one for President's Council on Integrity and Efficiency discussions, and so on. These lists provide an easy way of keeping up with new developments in your field, sharing with others innovative approaches that you have discovered, and obtaining ready guidance from subject matter experts.

Newcomers to the online world are most likely to find e-mail the online feature that immediately becomes indispensable for them, but depending on the nature of your work, you may eventually find even more useful one or more of the Internet's other features, such as:

- Usenet Newsgroups, collections of e-mail messages on over 12,000 different topics,
- File Transfer Protocol (ftp), which allows easy transfer of large amounts of data,
- Telnet, which provides the ability to log in as a user of a remote computer,
- Gophers, programs that use a text-based menu structure to make it easy to find information on remote computers,
- Internet Relay Chat (IRC), real time online conversations, which can be used as an easier, cheaper alternative to face-to-face meetings or conference calls, and

- The World Wide Web (WWW), which enables you to navigate through distant computers and find data by using hypertext and easy to use "point and click" software.

Due to its ease of use and power, the World Wide Web is by far the fastest growing part of the Internet, and this is where American businesses are beginning to set up shop in great numbers. World Wide Web access programs (browsers), like Mosaic and Netscape have been called the "Swiss Army knives" of the Internet because they can perform most of the other Internet functions, using one common user interface. Training time can be reduced even further through the use of customized "home pages," which can contain hotlinks for instant access to Internet features of interest to people working in a particular field, such as auditing, investigations, or law.

If we get an Internet connection, won't people in my office waste time "surfing the Net" instead of working?

This year we discovered that an employee of our agency had made nearly \$2,000 worth of calls to several 900 number voice sex lines. No one would seriously suggest that, because telephones could be abused, our agency should try to operate without telephones.

Poor employees will find a way to waste time whether or not you are on the Internet. The solution is good supervision, not depriving your organization of a tool of great potential power. At NARA, we have found that one key to avoiding problems is a written policy that spells out clearly what, if any, forms of personal use are appropriate.

This sounds good, but it doesn't apply to me, because no one in my office knows much about computers and I can't get any help from my agency's computer support staff.

Five years ago, even a year ago, you might not have had any satisfactory options for taking your office online. The major commercial online services offered only limited Internet access, if any. Setting up a full service Internet account was primarily the realm of technical gurus. Things have changed.

The recent development of new, easy to use software and an improved communications infrastructure (including the growth of commercial services like America Online, Prodigy, etc.) have radically changed the situation. It is now possible for even people who know next-to-nothing about computers to quickly and easily join their colleagues online, including the Internet, at minimal cost. Millions are doing so.

(continued on page 10)

Ways to go Online Compared

Type of System	Examples	Structure	Owner/Manager	Fees	Advantages	Disadvantages
BBS (Bulletin Board System)	OPM Mainstreet. World Data Network in Reston.	Typically a PC with one or more attached modems and telephone lines allowing outsiders to call in.	Mostly individuals, including many hobbyists. Called "Sysops" (System Operators).	Some charge fees, usually low, but most are free.	Low cost. Easy to contact. Some have gateways for Internet e-mail.	Typically not as many resources or as well organized as the major commercial on-line services.
Commercial OnLine Service	CompuServe, America Online, Prodigy, GEnie, Delphi.	One or more large computers linked to telephone network with many POPS (local "Points of Presence") so users avoid long distance charges.	Corporations. For example, GEnie by General Electric, Prodigy by Sears & IBM, CompuServe by H&R Block.	Monthly fee in \$8 to \$15 range that includes some "free" hours. Fee for extra hours and "premium" features.	Easy to log on. Management usually provides easy to use software and user support. Most now offer a few Internet features.	High cost. Fewer available resources than on the Internet. None offers full Internet access.
Internet	There is no "example," because there is only one Internet.	"Network of networks." Key machines are large computers owned by universities and large businesses that are linked by leased high-capacity telephone lines.	The individual computers on the Internet all have owners, but there is no real owner or manager of the Internet as a whole.	There is no fee for Internet use itself. If you have to get access through a commercial service provider, you pay a fee of \$15—\$35 month. for assistance in getting connected.	Lower cost than the commercial services. Extraordinarily rich in resources. Some accounts include privilege of posting material on World Wide Web.	System appears chaotic to new users (no owner/manager). Limited user support. Sometimes difficult to connect to popular sites.

Individuals typically get Internet access by going through a "service provider." These are mostly local businesses you can reach with a local telephone call who already have a large computer and high capacity telephone line. They will let you piggyback on their connection, usually for a fee.

Within a couple of years, maybe less, not having an e-mail address will cause people to react the same way they do today if you tell them you don't have a fax number.

I can already send and get e-mail from Prodigy (or America Online, or CompuServe, etc.). Why do I need to worry about the Internet?

You may not. Nearly all government officials can benefit by having an e-mail account, but that does not mean they need to be "on the Internet." Just as an MCI telephone customer can call someone on the Sprint system, or AT&T, today all the major commercial online services can send and receive e-mail to and from the Internet, and vice versa. If your message needs to go over the Internet to reach its destination, your system should route it for you automatically, without any further involvement on your part, aside from possibly addressing it a little differently.

If you find that Prodigy or one of its competitors meets all your needs, and you are comfortable with it, there is probably no compelling reason for you to switch. On the other hand, many people find that they like the extra flexibility and power that they get from accessing the Internet more directly, instead of going through a commercial online service. For example, you are more likely to find sophisticated e-mail handling features like threading, "kill files" and "bozo filters" in software designed specifically for Internet usage. These features can save you time by automatically grouping your message by topic or sender, and screening out messages on topics that don't interest you or from senders who don't interest you.

Above and beyond better e-mail handling, the Internet offers other powerful features and a depth of resources that no commercial online service can match. Finally, for all except extremely low volume users, an Internet account will probably be cheaper than going through one of the commercial online services.

What kind of equipment is needed?

No state-of-the-art, expensive hardware is necessary to set up individual Internet accounts through an Internet service provider. All you need is a computer, an ordinary telephone line and a modem. Essentially all modern government offices already have personal computers and telephone lines. A modem is a device that lets your personal computer send and receive data over a telephone line. Modem prices range from \$80 to \$120 for a 14,400 bps model, today's most common for business use (bps = bits per second, a measure of data transmission speed), to \$150 and up for a high speed 28,800 bps type. (These prices are for ordinary voice grade telephone line modems. If you have only one of the newer digital telephone systems, you will need a more elaborate interface.) Your modem can share a voice line, and callers to the number will get a busy signal

only when you are actually using it, normally only a short time each a day.

If your organization is large enough, you may want to establish a direct connection to the Internet, and route it through your office Local Area Network (LAN). This approach could be cheaper in the long run, depending on the size of your organization, but it introduces some security risk, and requires technical knowledge and an initial investment in routers, firewalls, etc.

How can I use the Internet if I don't know Unix and I don't have 4 years to spend learning about it?

Most of the large computers on the Internet use the operating system known as Unix. While it's quite difficult to become a Unix expert, it's fairly simple to learn the minimum number of Unix commands needed to operate a Unix shell Internet account. Furthermore, if you don't want to face this simple challenge, there are even easier alternatives. With the right interface software, the average government employee computer user can accomplish anything he or she might need or want to accomplish without ever looking at a Unix command line. Unix is still there, underneath the simple menus, but modern software shields users from its apparent difficulty. You can now navigate the Internet using simple menus and point and click software.

How much would the service cost?

You can get an individual Internet account for from \$15 to \$30 per month in the Washington area, which has a high level of competition among service providers. This price would typically include anywhere from 2 to 6 hours of service a day, far more than most government employees are likely to need. Commercial online services like Prodigy, etc., tend to be more expensive overall, because they charge hourly fees, plus have the disadvantage of offering only limited Internet access.

Who is the best service provider and what is the best software?

There is no single best service provider or software package for everybody. The optimum solution in a particular situation will depend on a variety of factors, including geographic location, the hardware and operating system available, expertise of the prospective users, cost, and most important, what the users need or want to get from the connection.

One fact makes the process of selecting a service provider a little easier: with Internet e-mail, all roads lead to Rome. After e-mail gets onto the Internet, it all travels the same way, and is substantively the same on receipt, though it may look slightly different to recipients using different types of software.

An Inspector General's Thumbnail Guide to Types of Internet Accounts

Account Type	Examples	How Does It Work?	Advantages	Disadvantages
Specialized Mail-Only Account	WinNet. Some local BBS's, including OPM Mainstreet.	Users send and pick up mail by calling a computer that is connected to the Internet.	Can be cheapest, depending on usage pattern. Can use mail to access ftp, some other Internet resources.	Limited access to some of the Internet's other useful tools.
“Dial Up” Shell Account. Could be on a BBS, a commercial service, or with a commercial Internet service provider.	Some local BBS's. Delphi (more extensive shell access than any of the other major services). Netcom shell account.	User dials into an Internet-connected computer that treats user as if he or she had a terminal on that computer. User not directly connected to the Internet.	Connection sometimes cheaper and easier than other alternatives, depending on usage pattern.	Limited choice of interface software. Often must use difficult UNIX commands. Usually, no graphical access to WWW feature.
Specialized “Dial In” SLIP/PPP type account (Serial Line Internet Protocol/Point to Point Protocol) on commercial Internet service provider	Netcom's “Netcruiser” account. The Pipeline.	A service provider gives users free interface software that is pre-configured for easy set-up and use.	Extremely easy to use. Price is competitive.	Must use provider's software, which has some limitations.
Regular “Dial In” SLIP/PPP account on commercial Internet service provider	Netcom regular PPP account.	User goes through service provider's equipment, and once on Internet, is treated as an Internet “host” machine.	Full Internet service. Wide choice of available software, much of it free.	Depending on the software and service provider selected, can be difficult to set up. Often more expensive than shell account.
Dedicated high capacity SLIP/PPP account	Large businesses, universities, and government agencies.	An organization that has linked its internal network to the Internet through a large high capacity leased telephone line.	All the advantages of a dial up SLIP/PPP account, plus extremely fast data transmission.	Only a few organizations have such connections.

As Federal Government officials, we have some options not available to private business. The Office of Personnel Management (OPM) operates "OPM Mainstreet," a Bulletin Board Service (BBS) for use by Federal employees conducting official business. It is a large computer that allows "dial up" accounts by modem and has a gateway to send and receive Internet e-mail. You may not find it as flexible or as easy to use as some other alternatives, but it is a tool that many in the government have found invaluable.

If your organization has very little computer expertise, another option is a commercial online service like America

Online, Prodigy, CompuServe, Delphi, GENie, etc., which are usually relatively easy to set up and use. For more power and flexibility it is best to go to a commercial Internet service provider.

The pros and cons of these approaches are discussed in more detail in a set of white papers prepared by the NARA OIG specifically for IGs. Your office can get a copy by sending an e-mail message to jerry.lawson@arch2.nara.gov with the phrase Get Internet Docs as the only text in the message block. If you don't have access to e-mail yet, call (301) 713-6666 and we will send you a copy by postal mail. □



Fully and Currently Informed: How Assistant Inspectors General Keep Their Bosses Aware Without Drowning Them in the Age of Information

by James Ebbitt and Pete McClintock; Donald Mancuso and Patrick Neri

Keeping the boss informed is a priority with all Assistant Inspectors General (AIGs). Nobody wants to be on the receiving end of the question: "Why wasn't I told?" But the fact is you can't tell the boss everything. There are limits to what anyone can absorb. Selecting what the boss really needs to know and gauging when he or she needs to know it becomes the fine art of managing. Both audit and investigative senior managers face the challenge of keeping their bosses informed. Each profession has unique characteristics that pose special balancing questions, yet both face many of the same concerns. This article examines the art of juggling information from both perspectives.

The Assistant Inspectors General for Audits' (AIGA) Viewpoint



*James Ebbitt, AIGA,
Department of Agriculture*

*Pete McClintock, AIGA,
Small Business Administration*



We compared the audit processes at our two agencies, the OIGs at the Department of Agriculture (USDA) and the Small Business Administration (SBA). USDA's OIG is one of the largest in the Federal Government, and SBA's is one of the smaller. It may seem that AIGs of small OIGs have an advantage over their large-agency counterparts: the amount of information small agencies have to select from should be easier to handle. Yet our experience shows this isn't true. Small agencies are faced with the same needs as large, and they create similar methods of coping with the same obstacles. We found that the similarities between our channels of information outweighed any differences in our size.

AIGA (continued on page 16)

The Assistant Inspectors General for Investigations' (AIGI) Viewpoint



*Donald Mancuso, AIGI,
Department of Defense*

*Patrick Neri, AIGI, Department of
Housing and Urban Development*



Headlines: "Senior Officials Under Investigation;" "IG Agents Raid Contractor Facilities;" "Federal Agents Arrest Local Businessmen".

Major investigations are frequently headline-grabbing events. How much attention these investigations should command at the top level of an OIG is, however, dependent upon several factors. Relatedly, inasmuch as OIG investigators are generally located in the "field" as opposed to being concentrated within the "Beltway," there are administrative and management challenges inherent in this structure that sometimes differ from the challenges faced in other OIG components. In this article, we will examine these factors and challenges

AIGI (continued on page 17)

Interestingly, USDA's OIG was created after a massive agricultural fraud scheme showed that better communication was needed between audit and investigative organizations. Communication has thus been a concern for us at USDA since our beginning. With over 300 diverse programs to keep up with and a large Department of approximately 110,000 employees to monitor, we are often challenged by our goal to keep managers informed of the financial and operational problems we find. We are no less challenged by our need to keep our IG informed.

USDA's mission is a broad one. It serves the Nation's farming community by stabilizing commodity prices, conserving farmland, opening foreign markets, and aiding agricultural research. It serves the Nation's consumers by guaranteeing wholesome foods in the marketplace and providing a nutritious diet for those in need. It protects the Nation's forests, and it stimulates the economies of small-town areas. Its FY 1995 budget is about \$65 billion.

Within this busy environment, the OIG identifies program problems across the board and recommends solutions. The OIG employs about 350 auditors, 225 criminal investigators, and 200 statisticians, computer specialists, lawyers, analysts, and administrative and support staff. It operates out of 43 offices across the country with a FY 1995 budget of \$63 million.

Keeping up with such a broad network of USDA functions and OIG offices requires a healthy flow of information and more than a little mental agility. Programs can easily be confused, and agency acronyms can start to sound like alphabet soup. Keeping up has in fact been

made more difficult by the changes brought on by reinvention plans. Under the Secretary of Agriculture's 1994 Executive Order, USDA is reorganizing from a Department with 43 agencies to one with 29. This shift is something of a culture shock for this long-established family of USDA employees. It's also tough on OIG staff, who now have to learn a new set of agency names and acronyms. The old, familiar Farmers Home Administration isn't there anymore. Now we must master the distinctions between such organizations as the Consolidated Farm Service Agency and the Rural Business and Cooperative Development Service.

But communicating with the IG is, after all, our job. Information must be available when we need it, and it must be easily understandable when we deliver it. This requires attention and focus. It also requires involving the IG in the three critical stages of our audit process: audit planning, audit execution, and audit reporting.

During the audit planning stage, we develop profiles and strategies to understand each of the Department's 300 programs and to assess the internal control risks associated with them. A profile details everything about the program it describes: how it is delivered and what management controls are in place to ensure its integrity. Strategies, both short-term and long-term, are then developed to address real or perceived control risks. This planning process includes all of the OIG staff as well as the pertinent USDA program officials and managers. We meet with program officials to discuss our risk assessments and to find out where they think we need to perform audits.

AIGA (continued on page 18)



and provide perspectives from two differently sized OIG investigative offices. One has a staff of nearly 500 personnel while the other employs about 130. While different in size, the Departments of Defense (DOD) and Housing and Urban Development (HUD) OIGs have similar missions and authorities with respect to the criminal investigations each conducts.

Inspectors General (IGs) are Presidential appointees who play a critical role in their Departments. They must determine the scope and level of detail needed to fulfill their responsibilities as senior executives. Regardless of the size of the OIG, certain events demand senior level attention. Defining which events will command immediate attention and the manner by which they should be identified and communicated is one of the more important challenges facing an IG and his or her AIGI.

The sheer volume of available information frequently dictates that reporting priorities must be agreed to and an effective level of trust be established early in the relationship between the AIGI and his or her IG. This "partnership of trust" is perhaps the single most important aspect in the IG/AIGI relationship and must be based on a common understanding of exactly what is expected and how those expectations will be realized. Indeed, the importance of this aspect of the relationship is not unique to the investigative AIG but is a critical ingredient with all other AIGs as well. It is in this area that good managers excel and less successful ones fail.

As chief executives of large agencies, IGs cannot afford to be perceived as being ill-informed regarding matters of importance involving their organization. They rightfully rely on their AIGs to keep them current. Here again, trust and clear communication are imperative. Whether through daily contact, personal briefings, e-mail, or more formalized written communications, an IG must feel confident that he or she can depend on the AIGI for prompt and accurate information.

As with all levels of communication, this is a two-way street and requires both flexibility and a willingness to state with clarity exactly what needs to be said. Especially at the start of a relationship, the IG must clearly communicate his or her expectations and sensitivities. Some IGs may want to be called at home at midnight on matters of importance while others may settle for discussion as the first order of business the next morning. The AIGI also should determine what the IG "needs" in level of detail. This is usually affected by the background and experience each IG brings to the job. A former prosecutor, for example, requires far less detail than someone who may not have had the benefit of that background in evaluating the need for a broad based search warrant. Once an understanding is reached as to what is needed, the AIGI must then determine what is "wanted." Often this requires a level of diplomacy as well as a period of trial and error. Finally, the AIGI must take the time to explain the strong and weak points inherent in the organization's information systems, seek clarification where needed and, finally, communicate the IG's requirements to subordinate staff to ensure that all players in the process understand what will be required of them. Once

begun, the process of communication must be allowed to evolve in a positive fashion.

Only after this process of communication reaches a level that is understood and accepted by both parties can a true partnership of trust be established. This partnership is then based not only on open communication but also upon a recognition of, and sensitivity to, each partner's unique management styles and concerns.

The primary discriminating factor in a large organization frequently becomes one of quantity rather than just priorities. As many of us can attest, information overload can be as much a problem as insufficient information. The AIGI must therefore develop an information system that incorporates the Department's unique requirements, keeps the IG apprised of critical data yet, at the same time, insulates the IG from extraneous, less important facts and information.

In considering the large volume of available data, we must assume that there is a dependable automated information retrieval system in place. Computers have proven invaluable in the investigative community as a method of tracking case information and providing a system of quick and accurate retrieval. Matters of possible interest such as arrests, search warrants, subpoenas, consensual monitorings, undercover operations, and various other investigative techniques need to be carefully tracked along with the administrative and statistical data typical of other case data systems. Regardless of what type of system is put in place, it must be flexible enough to produce the kind of information needed in a timely manner. While it is virtually impossible for an AIGI to have a working knowledge of all ongoing cases, it is possible to build into the case data system appropriate "flags" so that certain cases or events trigger special consideration and review. In both HUD and DOD, flags are used for such matters as Hotline cases and Congressional inquiries. In DOD, other flags include areas of special interest such as the issuance of safety alerts in cases where product quality may affect the health and safety of military forces. Whatever system of checks and balances is used however, it should never be so rigid as to preclude adjustment for unusual events that may be of broader interest to the IG or other OIG or Department manager.

While arrests and search warrants are tracked both at HUD and DOD, only those of particular significance are "briefed up" to the respective IG. The search of a major contractor in which a large number of agents—or agencies—participate would, for example precipitate IG notification, whereas a search or arrest that is effected without incident and is not expected to draw widespread attention would not normally be briefed. Similarly, in a large OIG, it is unreasonable to expect an IG to be kept abreast of every consensual monitoring use or Hotline allegation when those may well number in the hundreds or even thousands each year.

Regardless the size of the OIG, the level of detail that could be communicated to the IG far exceeds the time available by the IG to consider all of that information. For this reason, it is critical that an AIGI recognize that

The IG is very much a part of this process. He sits in with us during the audit planning sessions, and he joins us in our meetings with program officials. He also gets helpful reminders from us throughout the program year as we revisit the strategic audit plan to ensure we are committing our resources in the most efficient way. Most importantly, he talks to our Congressional oversight committees to get their views on where we need to spend our resources.

During the audit execution stage, the flow of information is apt to become rapid and inundating. At any given time during the year, we have approximately 200 audits underway. Our regional offices are in charge of managing these audits and of keeping OIG management informed of their progress. Our headquarters audit divisions act as liaisons between the field staff and agency program managers in Washington DC. The divisions stay informed of the various audits underway in each region in their respective areas, and they keep abreast of major issues that are developing in the field. Division staff are sometimes sent to the field to observe program and audit operations first-hand; otherwise they may be seen huddled around the fax machine in headquarters or hurriedly taking notes over the telephone.

Our management information system charts the progress of each audit on a monthly basis. Information is input into the system in our field offices and we access the data in Washington, DC monthly. We then have a conference call with each region to discuss the progress on each audit and any major trends that are developing. We send the IG summary data from our management information system, and we inform him immediately of significant issues needing urgent attention by agency managers.

Communication during the audit execution phase requires the most focus. The wealth of information must be distilled to crystalize the critical issues. We inform the IG of our progress through twice-a-week staff meetings, frequent one-on-one dialogues to discuss issues as they arise, and monthly audit briefings that serve as a general roundup of progress on our strategic audit plans. We also meet biweekly with the Deputy Secretary to inform him of significant audit and investigative concerns. These meetings serve as another forum to keep the IG keyed to the "hot" issues.

Our audit reporting process is a standard one for reporting audit results: our reports explain what problems we found, and an executive summary section allows us to provide a "brief" of the significant results and a synopsis of the key recommendations. When written well, these sections are fast to read and easy to understand.

What has been very effective for us, however, has been our Management Alert system. We have created a document, called a Management Alert, which we use during an audit to quickly notify agency managers that we identified an issue that requires their immediate attention. Brevity and timeliness are the ingredients of the Management Alert, and they have worked well in getting management's attention. Because Alerts often deal with sensitive issues and are distributed to the highest levels of management in the

Department, we involve the IG as soon as we are ready to issue one. The IG also participates in our discussion with agency officials responding to an Alert. We use Alerts judiciously because we don't want them to become just another type of report that does not have an urgent message.

The size of our agency and the number of programs we audit at USDA make a difference in what information we focus on at any given time, but not in how we view our work. We firmly believe, and we tell our staff at USDA, that every audit we conduct is of critical importance to the Department. Some will generate considerably more controversy or require more immediate corrective action than others, and we make sure the IG and Department managers are fully aware of these. But we believe all our audit work, controversial or not, is important to improving the operations of USDA.

Communicating with the IG at a small agency is certainly a less complex process than at a large agency because there are fewer auditors and a lighter workload about which to keep the IG informed. Nevertheless, the process we have in place at SBA's OIG mirrors much of the process at USDA.

SBA's mission is to aid, counsel, assist, and protect the interests of small businesses to preserve free competitive enterprise and to maintain and strengthen the overall economy of our Nation. SBA has about 3,700 employees located in almost 100 cities throughout the country. SBA's major programs include business loans, disaster loans, venture capital financing, surety bond guarantees, government contracting, minority enterprise development, and business counseling. As of March 31, 1995, SBA had over \$30 billion in loans, guarantees and liquidation assets outstanding.

In FY 1995, the SBA OIG has an appropriation of \$8.5 million which funds 104 positions. In FY 1994, the OIG also received \$3 million in supplemental disaster funds to be used until expended for disaster-related work, including the employment of 14 temporary auditors and investigators.

The Auditing Division is comprised of 35 full-time permanent employees and 7 temporary employees. In the last year, the Auditing Division issued 18 audit reports and had about 20 audits in various stages of process at any given point in time. Obviously, this is not a large workload in terms of keeping the IG apprised of the status, problems and key findings. Yet, communication can be a problem if it is haphazard and unclear.

To preclude haphazard communication, SBA OIG has several structures to facilitate routine communication, a system that tracks planned versus actual performance, and scheduled meetings with specific communication purposes. Our planning system begins each summer when the AIGs provide plans for anticipated work over the next 3 years. The AIG for Management and Legal Counsel combines these plans with the priorities of the IG into the OIG "Planning Guidance." This document becomes the basis for

AIGA (continued on page 20)

investigations are but a part of the overall mission of an OIG and that the IG properly depends upon each AIG to optimize available time. It is here that the AIGI must weigh factors such as the potential for adverse publicity, the surfacing of the foibles of their Department and its key people, and the impact that exposure of criminal conduct may have on critical business dealings or even on national security. This is by no means to imply that the OIG can be anything but aggressive in addressing these issues. Still, in the course of pursuing sensitive matters, the AIGI must decide when and to what level of detail the IG needs to be apprised of certain investigations.

In considering management and administrative issues, just as with operational ones, the AIGI must have an understanding as to what the IG requires in the way of information. In a small OIG, an IG may want to be a party in such decisions as the hiring and promotion of all employees or in decisions relating to travel, training, purchase of investigative equipment, etc., whereas in a large OIG those decisions are delegated to the AIGI. As with operational matters, it is imperative that the AIGI recognize the IG's personal desires and design a management system that is sensitive and responsive to those needs.

Once an understanding is reached as to what and how much information is to be communicated, an AIGI must determine the means through which this will occur. Nothing will ever replace face-to-face meetings and discussions but this is not always feasible in a large organization. In cases where a meeting is impractical or otherwise unnecessary, telephone contacts as well as the use of electronic mail (e-mail) and other written communications can serve to provide needed information with a minimum of disruption. In DOD, the AIGI uses several forms of correspondence to keep the IG currently informed. Quarterly Executive

Summaries detail a sampling of current cases while Bi-Weekly Activity Reports provide an overview of all sorts of operational and administrative activities such as the filing of indictments, sentencing, civil recoveries, significant contacts with parties both within and outside the Department as well as matters impacting training, budget, and "local news" from the OIG's more than 40 field locations. The HUD OIG utilizes a Weekly Report to the Secretary which reports on significant prosecutive actions as well as on activities involving high profile initiatives such as Operation Home Safe, an initiative targeted at violent crime and fraud in public housing and multi-family equity skimming.

The use of e-mail is perhaps one of the most useful innovations available within virtually every OIG. Prudent use of e-mail can greatly facilitate communication between an AIGI and an IG. E-mail provides a system that reduces the need for scheduled meetings, allows for quick review and comment, and is easily transportable when one or both executives are traveling. In this way an AIGI can frequently err on the side of more information rather than less in deciding what is, or might be, of interest to his or her boss. E-mail allows an AIGI to easily adjust the flow of information in line with current priorities and in a manner that is least intrusive to the IG's schedule. Of course, e-mail is never a substitute for the personal contact that is necessary in dealing with high priority matters.

In summary, effective communication is an art and recognizing what topics need to be shared with your supervisor is at best a continuing process. In many ways it can be compared to learning the writing style preferred by a supervisor which frequently requires some trial and error. It should be noted, however, that in the field of investigations, errors can be both costly and embarrassing and are best not repeated. □

developing our annual activity plans where specific audits and projects are identified and serves as a communication tool with the Agency's policy makers and program managers.

The Auditing Division maintains an automated, monthly management information system which describes each project's planned and actual milestones, tracks the amount of time expended and provides a short description of the status of the audit. The monthly project status report is provided to the Deputy IG. On a quarterly basis, we develop a report for the IG which reflects the progress of projects contained in the original activity plan. For each project, we include a brief description of the objective, background and justification for the project, the proposed work plan, the anticipated product or results, and the status for the quarter. Once completed, the findings or accomplishments are briefly summarized for the IG for his use with the AIGA in formal quarterly reviews of the division's performance against the IG approved plan. This document is a ready reference for the IG on the history, status, and results of the Auditing Division's work.

Additional communication structure is added through routine meetings. Weekly, the OIG executive team meets to discuss items of general importance; this meeting lasts about an hour and each participant usually has the floor for no more than 10 minutes. Biweekly, each AIG meets individually with the IG to discuss activities within his or her area of responsibility and to obtain policy guidance from the IG. These meetings can last up to 2 hours and therefore are much more detailed. Most of the time, key staff attend so that the IG can be provided a first-hand account of the issue rather than receiving second-hand information. Monthly, the OIG executive team briefs the SBA Administrator on OIG activities. If more than a brief summary of a particularly significant audit is necessary, the IG and the AIGA will brief the Administrator on audit results separately. Of course, the AIGA has access to the IG

on any matter at any time. Moreover, the IG meets with the Administrator every other week on matters of concern to each operating division.

The trick in keeping someone informed is to avoid inundating him or her with a plethora of information. This is true for either a large or small organization. We have, on occasion, provided our IG at SBA with too much detail, on too many matters, for too long a time. Therefore, we cull out the insignificant and concentrate on matters of substance.

Clarity and brevity must be the foremost consideration for successful communication. Because auditors tend to be detail-oriented, this can be difficult for many of us. In most instances, both the written and verbal communication structures we use at SBA to keep the IG and others informed about our work require us to boil an audit report into three or four paragraphs or a 3 or 4 minutes oral summary.

The audit finding reporting structure is very useful in summarizing most messages. Several sentences, conveying the condition, criteria, cause and effect, provide a useful and complete synopsis of any finding. Add a few illustrations of actual problems, and chances are the message will be remembered. If more detail is required, it can be given. If that formula does not fit a situation, then the journalist's formula of who, what, when, where, and why may be of use. Years ago, a former IG used that format for summarizing items of significance for top agency management and insisted the rest of the staff do likewise. It was very successful.

In summary, the methods of keeping the boss informed don't seem to change significantly with the body of information in the pipeline. Careful selection and timeliness are the keys. Routine communications and concise messages ease the process. These principles should help communication between the busy AIG and the busy IG, regardless of the size of the organization.□

Dogs That Hunt: The Auditors and Investigators

by Stephen A. Trodden

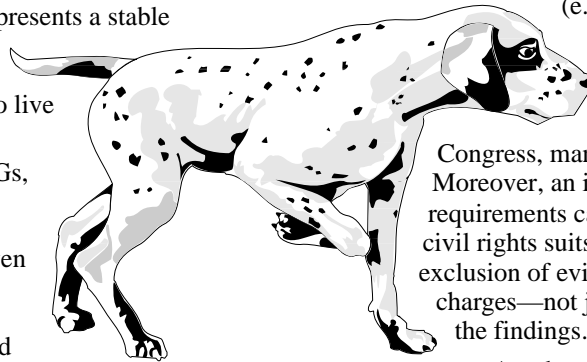


*Stephen A. Trodden,
Inspector General,
Department of Veterans Affairs*

By the mid-1970's, the concept of an Office of Inspector General (OIG) was an idea whose time had come. With passage of the Inspector General (IG) Act of 1978, the process of establishing

and activating IG offices was firmly in place. The mission of these new and unique organizations was to improve the economy, efficiency, and effectiveness of government programs and to detect and prevent fraud, waste, and abuse. To fulfill this mission, audit and investigative functions were unified under one roof. That Congress chose to include these two disciplines within the framework of the OIG demonstrates a similarity in the overall purpose of these two disciplines. However, Congress also chose to recognize their differences by providing for two statutory positions beyond that of IG: an Assistant IG for Auditing (AIGA) and an Assistant IG for Investigations (AIGI). Now, after almost 17 years, there remains the question in some minds concerning whether this unification represents a stable marriage or a relationship that was doomed from the start, separated by irreconcilable differences, yet forced to live together in the same house.

Since the establishment of the OIGs, there has been much discussion about, and some attempt at, combining these disciplines. They have, however, proven too diverse to do so. While it may be possible in the short term to train an individual in the worlds of auditing and investigating, that individual, as do the majority of human beings, will exhibit an affinity with one profession over the other. This is not a bad thing; few sports figures easily adapt to multiple roles. While there are exceptions, the Deion Sanders are few and far between. Put another way, for those looking for the ideal fraud-stopping animal, it is not the "audigator." Nor is it the mating of a bloodhound with a basset hound; for if you try, all you'll get is a dog that won't hunt.



Any attempt to articulate the difference between these two disciplines is difficult because the educated reader will undoubtedly conjure a myriad of exceptions to any general traits or rules that are stated or portrayed by examples. Nevertheless, some generalizations can be hazarded.

The most obvious difference is the remedy contemplated as a result of conducting each activity. An audit makes recommendations to Departmental officials for program changes to promote efficiency and effectiveness. The auditors are trying to create a positive. An investigation gathers facts for presentation to an official (generally a judge) empowered to adjudicate and punish malfeasance. The investigators are attempting to eliminate a negative.

Investigations generally are reactive, whereas audits frequently are proactive. Audits are overt and conclude by seeking input (and, if possible, concurrence) from the managers being audited; investigations are often covert and result in the subject's answering charges before a court. Investigators routinely encounter a higher degree of hostility when their actions threaten a subject's reputation or liberty; auditors generally do not operate in as unfriendly an environment. The value of auditors' work is impaired if it fails to comply with standards established by their peers (e.g., the General Accounting Office or professional associations).

Investigators' work must comply with a diverse set of requirements imposed by the Constitution, Congress, many courts, and various agencies. Moreover, an investigator's failure to meet these requirements can itself give rise to tort claims, civil rights suits, criminal contempt citations, exclusion of evidence, and dismissal of the charges—not just a loss of confidence in the findings.

Another major difference is the amount of control each discipline can exercise over its activities. The auditors generally try to control events. The investigators are often controlled by events. Once actual audit work commences, the audit staff usually maintains control over the pace and direction of the various audit steps. Once an investigation is referred for prosecution, or when a prosecutor is consulted and, as is often the case, grand jury proceedings are initiated, the Department of Justice plays a major

(continued on page 22)

role. The OIG cannot dictate the scheduling of grand juries, nor can it dictate the order in which cases are handled by an Assistant United States Attorney.

Despite their dissimilarities, these two disciplines can, and do, join forces to produce significant results. The area of defective pricing is one where millions of dollars have been collected from contractors due to the joint efforts of auditors and investigators. Through the application of coordination of remedies, several approaches to the project can take place simultaneously in the pursuit of criminal, civil, and/or administrative sanctions.

Each discipline operates most effectively when it maintains its unique manner of operating while pursuing a joint strategy to achieve a common objective. When the two disciplines are working in tandem, the auditors' expertise in gathering and following the facts, developing audit trails, and analyzing of large volumes of data, used in concert with the investigators' interviewing techniques and knowledge of human behavior, create a team that is seldom defeated. The big questions are, when do you bring the two disciplines together to form a team, how do you determine their relative involvement, and who decides what needs to be done and when.

If investigators are pursuing a criminal case and there comes a time when audit assistance would be extremely helpful, then the investigators are in the best position to coordinate their respective efforts, at least initially. Conversely, if the auditors, during a planned audit, determine that answers provided to them by contractor personnel may not be completely truthful, and that a series of interviews of current and former employees, away from the audit site, would be helpful, they may ask for investigative assistance in conducting these interviews. Clearly, in this instance, the auditors are in charge. Care must be taken by auditors, who are assisting in a criminal investigation, to represent their efforts correctly so as not to open themselves and their organization to charges that they denied the subjects of an investigation due process. Both auditors and investigators should have access to counsel to ensure that the issues are identified and pursued in such a manner that the efforts of both disciplines will provide the evidence needed to support the charges. In some cases, OIG counsel may be the appropriate discipline to coordinate the work of the auditors and investigators.

Problems are more likely when the nature of the offense and probable outcome are unclear (fraud or administrative issues) and both disciplines must be involved in sorting out the details. For example, the issuance of an audit report may impede the investigation and the auditors may be requested to delay the report publication. Legitimate concerns are often raised, particularly when the subject of the audit is an entity within a department or agency. The obligation to bring to management's attention some serious problems, particularly when the status quo could cause, for example, additional dollar loss or liability, needs to be weighed against a future successful criminal prosecution. The same difficulties can apply in situations external to the agency. When confronted with cost mischarging or defective products, there may be divergent

views as to the best approach for resolution. The auditors may wish to settle with the contractor administratively. The investigators may push for criminal and/or civil prosecution. The latter, obviously, will take longer. The contractor is anxious to put the current problem behind and move on to other things. This is especially true when contractors face possible suspension or debarment. Notwithstanding the direction the case takes, without the concerted efforts of both groups, the result may not be maximized.

Working and playing well together is easier said than done. While disputes between audits and investigations can be turf-related, the issue often in dispute is credit for work. It is easy to say that there should be enough credit to go around on a successful project. However, auditors know they do not get full credit until the final report is issued. In joint projects, this means in many cases holding up the release of the audit report for months or years while the case goes through the slow legal system. Alternatively, the impact of hundreds of hours of investigative work may be less visible when joint effort results in an administrative settlement rather than in an indictment, conviction, or a judgment or settlement of a civil fraud case.

The impact of this credit issue should not be underestimated because people perceive that their next promotion, award, or training assignment, etc., rides on credit for their work.

While the interaction of auditors and investigators presents some challenges, meeting these challenges has resulted in some notable success stories. The Department of Defense (DOD) has the largest OIG in the community, the largest group of criminal investigators, and the largest group of auditors. The latter is concerned with major program audits, such as large dollar weapons systems. Contract audits are generally conducted by the Defense Contract Audit Agency (DCAA). Departments and agencies, other than DOD, also may utilize the services of DCAA to conduct contract audits. Most of the fraud referrals to the DOD criminal investigators are made by DCAA rather than in-house OIG audit staff.

One thing the DOD OIG has done, in the area of investigative support, is to assign an audit "advisor" to the AIGI. This advisor, a senior level auditor, reviews suspected contract irregularity reports furnished by DCAA to the criminal investigators and "quality controls" the referral, i.e., the advisor raises certain questions and issues that should be addressed from the outset so that the evaluation of the referral conducted by the investigators is most productive.

Once a referral is accepted for investigation, the investigators have the ability to request audit support from the DCAA Regional Manager. This manager may have cognizance over as many as 30 audit branch offices. Requests for audit assistance are routinely made and routinely granted. The auditors selected to assist the investigators most likely have specific audit expertise in the type of contract to be audited/investigated or, more routinely, the selectees are the auditors who detected the suspected irregularity. The auditors selected are assigned to the investigative office which requested the assistance. The DOD OIG has found this collaboration useful and

productive. Hundreds of millions of dollars have been recovered as a result of these efforts.

The Department of Veterans Affairs (VA) OIG is not only much smaller than its DOD counterpart but it also does much of its contract audit work in-house. We have had success in the area of defective pricing by establishing a contract referral panel consisting of senior representatives from audits and investigations, in coordination with our counselor's office. The panel provides a forum to work out differences between audits and investigations on the sensitive issues relating to direction, timing, and division of responsibilities in the area of defective pricing cases. Since establishment of this panel, there has been a substantial increase in recoveries from contractors who do business with VA.

While I have drawn on examples of success from the two OIGs with which I am most familiar, there are undoubtedly others. The important elements of successful collaboration are clearly defined objectives for the role of each of the OIG's components on a particular initiative, meaningful work assigned, respect for the contributions of each discipline, and shared credit for results achieved.

Auditors and investigators have worked together, and will continue to do so when the opportunity arises, with each contributing a unique set of talents. The current system of operation is not broken; let's not try to fix it. Rather, let us, as agents of change, look for ways to increase the instances where these two dynamic professions can be used to accomplish the OIG mission: to promote economy and efficiency in government.□



Fear of Flying: Acceptable Levels of Risk are Necessary to a Successful OIG Investigative Program

by Phillip A. Rodokanakis



*Phillip A. Rodokanakis,
Special Agent-in-Charge,
Singapore Field Office,
Office of Inspector General,
Agency for International
Development*

In the aftermath of the Watergate scandal, the rapid increase in Federal spending, exposure of fraud and other abuses in a variety of Federally funded programs, the Congress saw the need for a drastically different oversight function. Prior to the establishment of independent Offices of Inspector General (OIGs), audit functions had long been part of the operating component of each agency. Investigative units were often highly independent offices that reported directly to top agency management. The OIGs were based on the concept that the two professions would reinforce each other and that they would derive benefits from pooled resources and organizational independence.

Over the past 17 years, Congress has established OIGs in more than 60 Federal agencies, of which nearly 30 presently require Presidential nomination and Senate confirmation. The vast majority of these offices were established by the Inspector General (IG) Act of 1978 and the IG Amendments of 1988. OIGs are required to report regularly both to their respective agency heads and to Congress. The IG Act intended that this dual reporting relationship ensure public disclosure of OIG findings and OIG independence from agency pressures.

What are investigative risks?

All investigations are subject to risk of failure. An investigation might fail by not uncovering the culprits after expending significant investigative resources or by not developing a strong enough case to result in appropriate charges against the culprits. There is risk in declining to investigate a matter, either because the initial complaint was not succinctly defined or because operational priorities dictated that the matter should not be investigated. Investigations that achieve some prosecutive or administrative

results may fail to fully expose the scheme or the underlying causes which allowed the situation to take form in the first place. As a result, the risk exists that the criminal activity will continue long after the investigative file is closed.

What are unique risks faced by OIG investigators?

One risk stems from the fact that the overall objectives of the OIG investigative mission are mixed and not clearly defined. In traditional law enforcement organizations, the investigative mission is clear and usually centers along violations of criminal statutes, and investigative results are referred to prosecutors for resolution through the criminal justice system. OIGs, however, are subject to varying directives and operational priorities. The dual reporting provision of the IG Act can create conflict for the investigative program. External elements sometimes want scandals brought to light by OIG investigations fully exposed. On the other hand, most agency executives would much rather have investigations carried out discreetly with no outside fanfare. Some would even argue that agency management may wish to have adverse findings forgotten rather than risk the negative publicity resulting from prolonged investigations and trials. An investigation may uncover a scandal that may adversely reflect on the agency and result in a serious rift between the OIG and agency management. Any effort by OIG management to try to prevent negative investigative findings from surfacing could lead to failed investigations and allegations of loss of OIG independence.

Another area of possible risk for OIGs is the fact that OIG senior managers may come from disparate disciplines and may not have strong investigative backgrounds. In traditional law enforcement organizations, senior managers usually have risen through the ranks and have a clear understanding of the objectives and risks associated with investigative operations. This may not be the case in an OIG, and this lack of familiarity with investigations may be the source of difficulties in communication.

(continued on page 26)

Another fact to consider is that OIG investigations often involve more than suspected violations of criminal law. OIGs investigate civil or administrative matters and respond to political considerations or agency priorities. In addition, OIG investigators might conduct internal affairs investigations focusing on agency employees. Investigators may also be called upon to review agency programs and operations. This lack of a clear and consistent role definition in OIG investigative programs adds considerably to the risks associated with managing investigations.

Finally, the role of the OIGs has been complicated further by recent National Performance Review (NPR) initiatives. The 1993 report issued by Vice President Al Gore recommended that the OIGs change their method of operation to be more collaborative and less adversarial. Although this recommendation can be readily applied by changing audit approaches, when it comes to investigations, no change in methodology can alter the adversarial nature of an investigation—it's hard to take a collaborative approach when your ultimate goal is to put someone in jail!

How can an OIG minimize investigative risks?

While risk is inherent in any investigative effort, minimizing that risk is an important element of successful management. The OIG organizational structure creates unique challenges for investigative offices.

Utilize Management by Objectives (MBO) approach

Adopting the MBO philosophy can greatly assist OIGs in managing investigative risks. Simply stated, MBO is a management approach that focuses on goals rather than tasks. What is accomplished is more important than how it is accomplished, with the obvious proviso that the ends are achieved through appropriate means. MBO emphasizes teamwork and team results, which are essential to any successful investigation. Effective managers must direct the vision and efforts of all in the organization toward a common goal. Objectives on all levels and in all areas should also be keyed to both short-range and long-range considerations. Each member of the team contributes something different, but they must all be pulling in the same direction. Individual performance therefore requires that each investigation be directed toward the objectives of the whole organization.

Initiate and agree on a strategic management process

These principles are particularly important to OIG investigations because of the nature of white collar crime investigations. Due to their complexity, fraud investigations often succeed in spite of the criminal justice system or the procedures employed by the parent agency. Investigative work can be frustrating and tedious. Cases take a long time

to develop. New difficulties arise as culprits invent new schemes. There must be painstaking attention to detail. In short, cases take persistence and imagination. Such imaginative persistence is difficult to sustain if an investigator is simply told to be imaginative and persistent. These qualities are so difficult to define concretely in any specific case that a supervisor simply cannot order a person to give that extra measure of imagination that can make the case. Successful investigators must display considerable initiative and self-motivation. OIGs need to provide individual investigators with strong motivation to attain the organizational goals.

Effective managers empower employees because they believe in the innate potential of people to innovate and add value. On the other hand, the fundamental problem facing OIG managers is how to exercise adequate control and simultaneously provide for flexibility, innovation, and creativity. Applying MBO principles along with risk containment steps will not only reduce the risks associated with OIG investigative programs, but also go a long way toward establishing more productive and cohesive investigative units.

To establish a successful OIG investigative program, key internal agency officials and external elements such as oversight committees must agree about the overall OIG planning effort and the investigative process. Involving agency officials is usually crucial to the success of OIG programs, since OIG actions involve and/or affect multiple parties and operational divisions within the agency. An effective investigative program requires clear support from top management, personal links with the rest of the agency, and the time to explain the usefulness of investigations to agency managers, who may pay lip service to the need for an effective investigative element, but would secretly prefer that it would simply go away. If these elements are lacking, the investigative program will run into internal problems.

The OIG must come to grips with how much information can be shared with agency officials without compromising the investigation. The agency managers must understand that the investigative objectives will usually differ from those of the agency and that the need to protect the confidentiality of the investigative process may require the OIG to proceed without sharing any investigative findings with the agency management, even though they may have a crucial effect on agency operations. On the other hand, the OIG must attempt to share as much information as possible with the agency managers. This delicate balancing act will require developing a new mind set as investigators are usually taught to only share investigative details with those having a clear need to know.

Clarify organizational mandates

The formal and informal mandates placed on the OIG must be clearly understood. It is surprising how few organizations know precisely what they are mandated to do and not to do. How many OIG employees have completely read the relevant internal policy directives or manuals that

outline the office's formal mandates? It may not be surprising, then, that many employees make one or both of two fundamental mistakes—either they believe they are more tightly constrained in their actions than they are or they assume that if they are not explicitly told to do something, they are not allowed to do it.

In addition to understanding the strategic and operational mandates of the OIG, the investigators must also understand the agency's vision, mandates, and processes. To develop a successful investigative program, the OIG investigators must become thoroughly familiar with the programs, systems, and procedures that are unique in each agency.

Define an investigative strategy

OIGs must develop an overall strategy concerning the investigative program. The goals and objectives of the investigative office must be clearly articulated and understood by management and staff alike. This is an area that should call for very little individual interpretation. All investigators should clearly understand the type of allegations that they will readily investigate versus those that they would routinely decline. Although this is a basic operational requirement, it is amazing how different individuals perceive or fail to see the need for initiating an investigation.

Once the goals and objectives of the OIG investigative program are outlined, they must be communicated to the agency. This is essential to ensure that employees understand the function of the OIG investigators and are readily willing to participate and assist in ongoing investigations. In the Federal Government's "doing more with less" environment, it is particularly important for investigators to gain the cooperation of agency employees who are dealing with their own priorities.

Furthermore, the OIG must continue to express the goals and objectives of its investigative program to maintain the cooperation of agency employees, long before or after the conclusion of a particular investigation. As agency employees are the first line of defense in detecting and preventing fraud, waste, and abuse, their willingness to report their suspicions to the OIG is vital. Maintaining open channels of communication with all agency employees is imperative. Employees should not view OIG investigators as internal police who only spell problems for anyone with whom they come into contact.

A working risk model must also balance line and staff management. Most organizations allow either the line managers or the headquarters staff to dominate the investigative process. Striking a balance between the extremes is difficult, but OIG managers can begin by considering how they will use the results derived from successfully completed investigations. Will the results be used to set preventive controls or to weed out other similar abuses that did not result in criminal behavior? By asking these questions, the tendency to control investigations from headquarters to reduce potential damage can be balanced against the tendency of line elements to run with the investigation with a complete disregard for the consequences.

Assess the risks of a particular investigation

Risk assessment for investigations is difficult. No two investigations and no two investigative teams are ever exactly the same. Usually, the crucial consideration is the complexity of the underlying case.

If the target of the investigation is the head of an agency, the risk of a major schism between the OIG and the rest of the agency is significant. The OIG needs to preserve its independence and refer the investigative findings as early as possible to the Department of Justice. Fortunately, for most of the cases initiated by the OIGs, this example is not the rule. In routine cases however, it is hard to assess the associated risks since the extent of the potential damage resulting from the criminal activity under investigation is not known in the early stages of the inquiry.

In evaluating risk, questions should be asked as the case is developing and the facts become known. For example, what is the damage caused by the criminal activity? What is the potential outcome of the investigation? What is the likelihood of agency action to prevent a similar scheme from occurring in the future? In terms of damage to the reputation of the agency, what is the agency's exposure? Would the criminal activity have had the chance to occur if the program officials had been alert and doing their jobs? Had systemic weaknesses been identified in the past and had the program management failed to take corrective action?

Match risks with in-house capabilities

Successful OIG investigators must develop skills unique to their agency. In addition to the basic skills required of investigators who specialize in white collar crimes, they must become proficient in specific agency programs, processes and procedures.

Also, management must assess the particular skills and strengths of each investigator before determining the ideal team to undertake a particular investigation. For example, it would make no sense to assign an investigator with no understanding of computers to a computer fraud case—doing so would in all likelihood lead to a failed investigation.

However, matching investigative skills to the case under investigation is difficult. Cases are usually developed by the special agent first assigned the investigation. If at a later time it becomes apparent that the investigator lacks certain necessary skills, there is reluctance to reassign the case either because of the limited available investigative resources or a general resistance to reassign a case once the investigator has devoted much time and has become the de facto case expert.

Complex cases call for diverse investigative talents, a strong investigative team, and a tough leader to coordinate everyone's efforts. Under no circumstances should coordination of a team effort be delegated casually. Complex white collar crime investigations follow Murphy's Law; if something can go wrong, it usually will. In addition to

(continued on page 28)

developing the case, the team leader should be sensitive to and readily recognize potential areas of risk. Once the team identifies potential risks, it should immediately report them to the OIG management so that it can assess them and act accordingly.

Choose the right investigative methods

Just as matching the skills of the investigators with the underlying case is crucial, it is just as important to ensure that the proper investigative methods are employed throughout the life of the investigation. For example, it makes no sense to fingerprint a potential subject if there are no latent fingerprints developed in the first place or if fingerprints have nothing to do with the commission of the crime.

A poorly executed investigation can result in negative publicity and/or civil claims against the OIG and the assigned investigators. In this age of the lawsuit, this consideration seems even more applicable. On the other hand, the fear of a potential lawsuit should not be allowed to paralyze the investigation or the OIG investigative program.

Monitor the investigation

Despite the need to empower investigators to do their jobs properly, OIG managers should monitor the progress of investigations, particularly those having a high-profile or the potential for adverse publicity. Nevertheless, monitoring is not synonymous to micro-managing! Good operating

procedures should be in place so that at key points the case agents will automatically report events to management without the need for the headquarters' staff to take over the investigation.

Operating directives should spell out concise examples of when line investigators must report findings to higher management. For example, the directives may list time limits within which the field elements must notify headquarters when sensitive cases are initiated. The same should hold true during the course of the investigation.

Everyone in the OIG management structure likes to become involved in a flashy or high profile case. This type of investigation usually involves tedious and prolonged routine, and senior managers can become disinterested or overwhelmed by other priorities. It is, therefore, particularly important to have in place the appropriate directives that would alert OIG managers when investigative activities may be going awry or reaching a threshold that may result in an adverse impact for the OIG organization and/or the agency.

Conclusion

Risk can never be eliminated entirely. OIG managers, however, can take steps to minimize risks by establishing a clear investigative strategy, by selecting the right investigators and techniques, and by properly monitoring the situation. The end result will be an effective OIG investigative program. □

Partners Against Crime: Using a Culture of Collaboration to Win in the Fight Against Health Care Fraud

by June Gibbs Brown



June Gibbs Brown, Inspector General, Department of Health and Human Services

The escalating cost of this Nation's health care should be of concern to all of us. In 1967, the United States expended \$51 billion on health care; this year those costs will reach

\$1 trillion. The government's budget figures for Medicare and Medicaid, the two Federally-funded health care programs overseen by the Department of Health and Human Services (HHS), are similarly daunting. Medicare expenditures for FY 1995 are estimated at \$177 billion, a 9 percent increase over the previous year; Medicaid expenditures are expected to reach \$88 billion in FY 1995, a 7.8 percent increase over FY 1994. At the current rates, Medicare's board of trustees reports the Medicare Part A program may be bankrupt by 2002.

As the Administration and the Congress consider ways to reduce or control these expenditures, one issue that must be confronted is the percentage of health care dollars lost to fraud and abuse. The General Accounting Office estimates the Federal health care programs lose as much as 10 percent of their funding to the inappropriate, and at times criminal, practices of health care providers. These lost dollars not only deprive program beneficiaries of needed medical services, but the waste fuels public cynicism about the effectiveness of these programs and the government in general.

The challenge of investigating health care fraud

Oversight of the Medicare and Medicaid programs is provided by the HHS OIG. As the IG, I have challenged my staff to join me in developing innovative and result-oriented approaches to fighting health care fraud in the Medicare and Medicaid programs. The task has not been an easy one. The health care industry provides an environment

which is ripe for scam artists. The coverage and reimbursement of medical services are governed by a complex and often inconsistent set of rules, which provide countless "loopholes" to be abused. The ambiguous nature of medical treatment, combined with patients who are often weak and vulnerable, make it possible to bill unnecessary tests and useless equipment to the programs. Additionally, defrauders will exploit the relationship of trust between physician and patient by rewarding the doctor for referring patients inappropriately. Whether a cash bribe or an

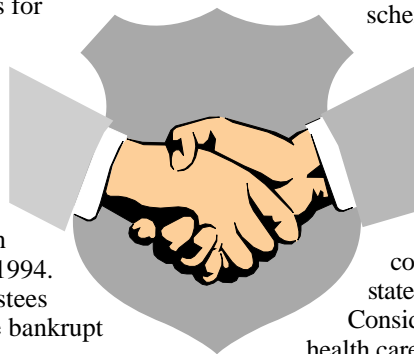
inflated return on the doctor's investment in the scheme's joint venture, the objective is to override the physician's ethical and fiduciary duties, at the expense of the patient and the health care programs.

While these characteristics of the health care industry have always made it vulnerable to fraudulent schemes and abuses, recent years have seen a surge in complex schemes which often span several states and implicate millions of health care dollars. Considering the phenomenal amount of money in health care, perhaps it is not surprising that a better organized and more ambitious breed of scam artists is targeting the Medicare program. After all, the notorious Willie Sutton once observed that he robbed banks because that was where the money was! To respond to this increased sophistication in health care fraud schemes, I believe we must shift our organizational culture away from intra- and interagency competition and toward an emphasis on interdisciplinary collaboration and teamwork.

Fostering collaboration within the HHS OIG

The following are several examples of how we are fostering this culture of collaboration in my office. Traditionally, the Office of Audit Services had played only a supporting role in the conduct of health care criminal investigations. Now that office is training its staff of auditors to work more closely with the Office of Investigations when audit findings suggest criminal fraud. We have been sending groups of auditors for intensive training in criminal investigative techniques at the Federal Law

(continued on page 30)



Enforcement Training Center. These “audigators” are proving to be invaluable in unraveling the most elaborate health care fraud schemes.

The OIG’s Office of Evaluation and Inspections (OEI) also is being better integrated into the fight against health care fraud. OEI uses its evaluations and analyses based on payment data and survey work to identify system vulnerabilities in the Medicare and other Departmental programs. In addition to guidance for policymakers, the resulting analyses now give our auditors and criminal investigators targets for further development, as well as case specific data for existing investigations. For example, when OEI interviewed beneficiaries during an evaluation of Medicare’s durable medical equipment (DME) benefit, it uncovered a significant number of people who said they had never received the equipment billed to Medicare. The resulting nationwide investigation of DME suppliers produced numerous criminal convictions, substantial restitution to the health care system, as well as much needed changes to Medicare’s coverage and reimbursement rules.

To ensure that this philosophy of interdisciplinary teamwork is recognized and flourishes, we have made other changes in the HHS/OIG culture. The OIG work planning process is now a collaborative effort in which the different component managers share their work planning documents with each other before they are finalized. This ensures that these strategic documents reflect the contributions of each component and its expertise. To emphasize the importance of this change in thinking to each individual on my staff, we also have rewritten personnel performance plans to recognize and reward cross-component efforts. In addition, I have established an annual award to be given to the OIG group and outside agencies that best epitomizes this collaborative spirit.

Interagency teamwork: the National Medical Enterprises investigation

The benefits of greater collaboration and sharing of resources also have been realized in our relationship with other Federal and State law enforcement and regulatory agencies. On behalf of HHS, I now meet on a monthly basis with high level officials of the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Health Care Financing Administration (HCFA) to coordinate our strategy against health care fraud. The FBI and my office also have placed our special agents in each others’ headquarters in order to improve our health care databases and case targeting. We disseminate to other Federal and State agencies our list of individuals and companies that have been sanctioned because of abuses against the Medicare program in order that the sanction may be given a more widespread effect.

The collaborative approach also means avoiding needless “turf battles” with our allies in this fight. OIG auditors have been successfully working significant Medicaid audits with their State audit agency counterparts; the decision concerning which office will be designated to

lead the audit is reached collaboratively and based upon the expertise required by the task. Further, I have authorized the Medicaid Fraud Control Units to work Medicare cases where a Unit’s investigation of a Medicaid scheme implicates the Medicare program, thus expanding these groups ability to fight health care fraud at all levels.

These and other agencies’ efforts to fight health care fraud using a team approach are producing favorable results. The recently concluded case against National Medical Enterprises (NME) is instructive. NME’s Psychiatric Hospitals subsidiary managed more than 60 psychiatric hospitals and substance abuse centers nationwide. Through an elaborately structured scheme affecting more than 30 states, NME kept patients hospitalized longer than necessary in order to use up the available insurance coverage, and billed insurance programs multiple times for the same service and when no services were actually provided. What is more, NME paid kickbacks to doctors and referral services so that they would refer patients to NME’s hospitals, and then billed Medicare for these illegal payments.

The 3-year investigation of this fraud required extraordinary coordination of Federal and State law enforcement agencies, including the Criminal and Civil Divisions of DOJ; the FBI; the Defense Criminal Investigative Service, the investigative arm of the Department of Defense OIG; the United States Postal Inspection Service; the Internal Revenue Service; the Office of Personnel Management OIG; the Securities and Exchange Commission; the Medicaid Fraud Control Units; and the U.S. Attorneys in 23 Federal districts. One example of the coordination required of this massive health care investigation was the August 1993 operation in which more than 20 search warrants were executed simultaneously at NME hospitals, corporate offices and other sites across the country. This enormous effort produced over 100,000 boxes of documents, which were inventoried, analyzed, and incorporated into the government’s case.

The teamwork and extraordinary coordination paid off for the government. On June 29, 1994, NME Psychiatric Hospitals agreed to plead guilty to six counts of making kickbacks to doctors to refer Medicare and Medicaid patients, and one count of conspiracy to defraud the United States. In addition, NME paid \$379 million in criminal fines, civil damages, and penalties, the largest amount ever obtained in a health care case. Criminal pleas also have been obtained from a significant number of the NME managers and physicians implicated in the kickback scheme and more are expected as the investigation continues.

Operation Restore Trust: taking teamwork the next step

As evidenced by the successful conclusion of the NME case, integration of the varied expertise and perspectives of the different Federal and State law enforcement agencies is essential to the successful conclusion of these complex investigations. However, I believe we can expand the interdisciplinary team concept even further. Working

jointly with HCFA, our offices have recently unveiled a demonstration project—Operation Restore Trust—which is using this innovative team approach to prevent and detect fraud and abuse in two rapidly growing sectors of the health care industry: home health agencies (HHAs) and nursing facilities (NFs) and related supplies and services. The Secretary of HHS has included this demonstration project as part of the Department’s Reinvention of Government Initiative.

Operation Restore Trust was initiated in early 1994 after a review of the findings contained in reports and investigations conducted by the components of OIG and HCFA identified HHAs and NFs as particularly susceptible to fraud and abuse. In the home health industry, for example, the OIG observed the prevalence of several types of fraud including cost report fraud, use of untrained staff, falsified plans of care and kickbacks. Between 1990 and 1994, OIG investigations led to 25 successful criminal prosecutions of HHAs or their employees. In 1993 and 1994 alone, 39 HHAs or their employees were excluded from participation in the Medicare and Medicaid programs.

Nursing homes also have become an increasing source of Medicare and Medicaid abuse. The vulnerability is a result, in part, of the Medicare reimbursement system which pays for nursing home services under two very different parts of the program. This dual payment system has resulted in inappropriate cost shifting and double payment schemes which result in both program loss and financial burdens on beneficiaries. Suppliers of medical equipment and supplies are often implicated in these schemes. For example, between 1990 and 1994, our investigations resulted in over 130 successful criminal prosecutions of medical equipment suppliers or their employees.

Based upon the results of our initial work, we concluded that a more concentrated effort was needed to address the burgeoning fraud in these two sectors of the health care industry. To that end, we have assembled project teams from three Departmental agencies: OIG, HCFA and the Administration on Aging (AoA). These three components bring very different perspectives and expertise to the problem at hand. The OIG will provide the teams with the range of professional skills of its auditors, criminal investigators and program evaluators.

HCFA, through its Benefits Integrity Office and its contractors, will develop data on targeted subjects concerning billing and payment patterns. It also will integrate into the project its surveyors who, in addition to their traditional role of reviewing quality of care, will be trained to look for signs for fraud and abuse. HCFA policy staff also will contribute by reviewing project findings that implicate HCFA reimbursement policies so that loopholes can be closed and abuses stopped on the front end.

The State Long-Term Care Ombudsman, through AoA, will coordinate with HCFA in identifying medical suppliers which provide unnecessary services and excessive supplies. The Ombudsmen are uniquely qualified for this task, since their role is to advocate to protect the health, safety, and welfare of the institutionalized elderly in nursing facilities

and board and care homes. These core Departmental teams will work in concert with other project team members, including DOJ, United States Attorneys, State Attorneys General and the Medicaid Fraud Control Units. These team members will actively participate in the targeting of investigations and prosecution of cases.

In considering the challenge of integrating such a diverse group of organizations and professionals toward common objectives, the Department concluded that the project initially should focus its resources in five states: New York, Florida, Illinois, Texas and California. These states were chosen because over one third of the Medicare and Medicaid beneficiaries reside in these five states. In addition, approximately 40 percent of all the money paid by these two health care programs to HHAs and nursing facilities went to companies in the same five states.

Operation Restore Trust: reaching out to the health care providers

Perhaps the most innovative aspect of Operation Restore Trust is that we are not restricting the teamwork concept to governmental entities. We also are enlisting the support and participation of the very industries that will be the target of the initiative. I believe that the majority of health care providers are concerned about the well-being of our beneficiaries and want to work within the legal confines of the Medicare and Medicaid programs. When billing irregularities occur, whether as a result of misunderstandings of the law or a lack of adequate oversight by the company’s management, these providers want to do the right thing by working with the government to resolve the problem.

To assist these health care providers, the OIG will continue the practice of issuing “Special Fraud Alerts” as a vehicle to identify fraudulent and abusive health care practices. Members of the health care industry have indicated that these fraud alerts have a powerful and positive impact on industry behavior. Accordingly, my office will be issuing a series of fraud alerts addressing abusive practices of home health agencies and nursing home facilities. Honest providers can and should use these fraud alerts as a tool to scrutinize their practices and make sure they are acting within the law.

When that process of self-examination uncovers a potential problem of program fraud, the home health and nursing home providers in the five states also will be given an opportunity to self-disclose the matter to the OIG under favorable terms. Voluntary disclosure offers self-disclosing companies the opportunity to minimize the potential cost and disruption of a full scale audit and investigation, to negotiate monetary settlements with the government based upon the matter disclosed, and to reduce or avoid an OIG permissive exclusion. The disclosure program also benefits the government by expediting the investigation and resolution of program abuses, as well as giving insight into schemes that might otherwise go undetected.

(continued on page 32)

Under procedures developed in conjunction with DOJ, a company (the pilot program is not available to individuals) may be admitted into the program provided that it is not under scrutiny by the government for the matter disclosed and agrees to fully cooperate with the verification of the disclosure. While the program cannot offer amnesty where the disclosure implicates the company criminally, successful completion of the disclosure process is given favorable consideration under DOJ's prosecutive guidelines.

Conclusion

In order for the Federal Government to continue the process of reinventing itself, we must examine the assumptions that underlie policies and practices of the organizations we serve. Actively promoting a culture of collaboration within agencies and among governmental departments is essential if we are to succeed in an era of diminishing resources and increasing challenges. I believe our experience at HHS shows that with teamwork, even the most formidable problems can be solved.□

Case Notes: Recent Court Decisions on OIG Powers and Authority

by Alexandra B. Keith and Maryann L. Grodin

The independence of the Office of Inspector General (OIG) investigative community was reaffirmed in two recent appellate court decisions. These decisions can be found at U.S. Nuclear Regulatory Commission v. Federal Labor Relations Authority, 25 F.3d 229 (4th Cir. 1994) and Department of Justice (INS) v. Federal Labor Relations Authority, 39 F.3d 361 (D.C. Circuit 1994). The Federal Labor Relations Authority (FLRA), in administrative proceedings, issued two decisions that attempted to subject OIG investigations to union labor negotiations and agreements. The Fourth and District of Columbia Circuit Courts of Appeals recognized the independence of the OIGs and overturned the FLRA decisions. The Fourth Circuit held that the Nuclear Regulatory Commission (NRC) could not be compelled to negotiate with its union about procedures governing OIG interviews. Shortly thereafter, the D.C. Circuit held that the Department of Justice (DOJ) OIG could prohibit an Immigration and Naturalization Service (INS) agent from consulting privately with his union representative during an OIG interview and could question the employee about his conversations with the union representative.



Alexandra B. Keith, Counsel to the Inspector General and Assistant Inspector General for Investigations, National Credit Union Administration



Maryann L. Grodin, Counsel to the Inspector General, Nuclear Regulatory Commission

OIGs historically have been recognized as independent and separate from the Federal labor relations process, both in the context of their own functions and authority and in their relationship to agency employees. The Federal Service Labor-Management Relations Statute (FSLMRS), 5 U.S.C. Section 7112 (b)(7), provides that a bargaining unit including, “any employee primarily engaged in investigation or audit functions relating to the work of individuals employed by an agency whose duties directly affect the internal security of the agency, but only if the functions are undertaken to ensure that the duties are discharged honestly and with integrity,” would not be an appropriate unit. Thus, OIG investigators and auditors have not been permitted to organize or join Federal sector employee unions.

As importantly, the OIG as an entity has enjoyed a unique status in labor relations case law. The landmark

decision on the issue of OIG exemption from the rules applicable to other agency components is National Federation of Federal Employees, Local 1300 and General Services Administration, 18 FLRA 789 (1985), (hereinafter “GSA”). In that case, the FLRA held that the agency had no duty to bargain over union proposals purporting to influence the conduct of OIG investigations. Here the FLRA stated:

“[I]nsofar as the proposal would seek to have the Agency head utilize his general supervisory authority over the IG [Inspector General] to influence the manner in which that official conducts investigations it impermissibly infringes upon the independence of the IG to undertake such investigations. The intent of Congress ... is that agency officials respect the freedom of the IG to determine what, when, and how to investigate agency operations and that the IG not be subjected to pressure by any part of the agency. Thus, the independence of the IG under law precludes negotiation on proposals purporting to influence the conduct of the IG investigations.” 18 FLRA at 794-795.

A significant incursion against this well-established independence occurred in 1988 with Defense Criminal Investigative Service (DCIS) v. FLRA, 855 F.2d 93 (3rd Cir. 1988), (hereinafter “DCIS”). In that case, OIGs had argued that they need not provide interviewees with union representation because OIGs were so independent that they could not be considered “representative(s) of the agency” for purposes of the statute. In DCIS, the judge sided with the FLRA, stating that DCIS investigators, Department of Defense (DOD) OIG agents, were employees of the DOD and thus were “representatives of the agency” for purposes of the FSLMRS. This was because the OIG

(continued on page 34)

agents' purpose when conducting interviews was to solicit information concerning misconduct that could be used to discipline employees.

Accordingly, since 1988 OIG investigators provide warnings known as "Weingarten rights," when they interview bargaining unit employees as suspects of criminal or other misconduct. The Weingarten case law, codified at Section 7114(a)(2)(B), provides an exclusive representative of an appropriate unit in an agency the opportunity to be represented at "any examination of an employee in the unit by a representative of the agency in connection with an investigation if— (i) the employee reasonably believes that the examination may result in disciplinary action against the employee."

NRC union tries to bargain about OIG investigations

With those somewhat contradictory cases as predicates, the National Treasury Employees Union (NTEU), the authorized bargaining representative for certain NRC employees, advanced four proposals to the NRC regarding procedures to be followed during investigative interviews of agency employees by the NRC OIG. While the proposals themselves are not relevant to the court's decision, but rather the requirement to bargain, we will briefly discuss them to give you a flavor of what was at stake for OIGs.

Proposal 1 would have given union representatives the right, during investigative interviews, to clarify questions posed to employees and answers given by them, to suggest names of other employees with knowledge of the issue, and generally to advise the employee. Proposal 2 would have required the investigator to apprise employees subject to disciplinary action of the general nature of the interview and the employee's right to have a union representative present. Proposal 3 would have required an investigator to provide Miranda warnings to employees being interviewed for possible criminal conduct. Proposal 4 would have required similar warnings when criminal prosecution had been declined but employees were subject to dismissal for failure to answer questions, i.e., "Kalkines" warnings provided in writing.

The agency refused to negotiate on these proposals, contending that to do so would infringe on OIG independence mandated by the Inspector General Act of 1978. Therefore, according to the NRC, the proposals were not negotiable because 5 U.S.C. Section 7117(a)(1) establishes NRC's duty to bargain only to the extent that proposals are not inconsistent with any Federal law. Because the proposals contravened the IG Act, they were inconsistent with a Federal law and

thus the NRC refused to bargain. The Union filed a petition with the FLRA, which ordered the agency back to the bargaining table.

FLRA changes its mind about OIG independence

The FLRA surprised many in the OIG community with this decision. Not only did it overextend the DCIS decision, but it overturned its own precedent established in the GSA case. What made the FLRA change its mind 10 years later? The FLRA said that it was convinced by the DCIS case mentioned above.

The FLRA stated:

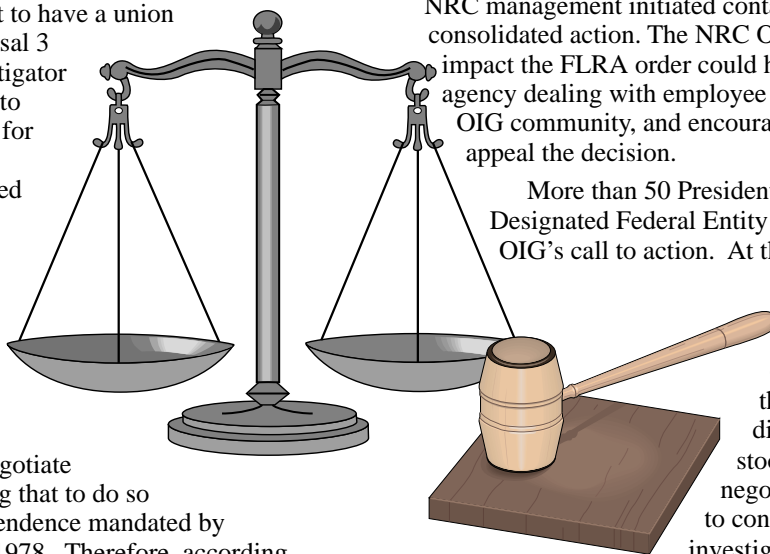
"[W]e find that because IG representatives are employees of the agency and, thus are subject to the agency's obligations, under the [Federal Labor Management Relations] Statute, an agency cannot declare proposals concerning IG investigations non-negotiable solely on the ground that, under section 3(a) of the IG Act, all proposals concerning IG investigations are outside the duty to bargain." 47 FLRA No. 29, at 9.

The OIG community rallies for independence

Because the NRC OIG was not a party to either the bargaining negotiations or the initial FLRA litigation, the OIG community was largely unaware of the case. Had the Union convinced NRC management to negotiate, the OIG may never have had the opportunity to protest until an agreement had been signed, and the Union attempted to have its terms enforced. After rejecting the FLRA decision, NRC management initiated contact with the OIG to take consolidated action. The NRC OIG, understanding the impact the FLRA order could have on any OIG in an agency dealing with employee unions, quickly alerted the OIG community, and encouraged NRC to ask DOJ to appeal the decision.

More than 50 Presidentially appointed and Designated Federal Entity IGs responded to the NRC OIG's call to action. At this time, OIG independence clearly became the major focus of what had been one agency's labor dispute. Other OIGs found themselves facing a major dilemma. If the FLRA order stood, their agencies could negotiate away the OIG's ability to conduct independent audits and investigations. On the other hand,

if IGs insisted on negotiating for themselves, they would become "management" and would face the inherent conflicts of interest in such a position. In addition, IGs noted that the diversity and complexity of employee unions could effectively stymie their investigative functions. When



asked to comment on the practical difficulties of the FLRA order, one IG responded that his agency negotiated with 80 bargaining units. If he had to negotiate a separate agreement with each one, much less administer 80 separate procedures for conducting OIG interviews, he might have no time left to accomplish his statutory mission! If OIGs were to be the subjects of agency/union negotiation about investigations, then why not everything else? IGs responded that the holding could have been precedent for unions to demand negotiation on a multitude of issues not required by law, an outcome contemplated neither by the DCIS case or the Congress when it enacted the IG Act.

The information obtained from the OIG community, along with strong support from the agency solicitor, aided greatly in acceptance of the appeal by the DOJ.

Fourth Circuit overrules FLRA

In their able representation, the DOJ appellate staff referenced the data obtained from the OIG community. As a result of their efforts and the convincing statistics from the OIGs, the FLRA decision was overruled. In overruling the FLRA decision, the Fourth Circuit concluded that it had improperly expanded the limited holding in DCIS. In fact, the DCIS case did not address bargaining over any terms and conditions of employment. Its sole purpose was to ensure that employees were provided their “Weingarten rights,” even in OIG interviews. In order to do this, the DCIS court had to view OIG agents as “representatives of the agency” for that narrow purpose. The DCIS court was careful to note that the term “representative of the agency” as used in 5 U.S.C. Sec. 7114(a)(2) may be defined differently depending on the specific rights and duties at issue. Thus, it could call OIG agents “representatives of the agency” for the purpose of Weingarten rights only, and for no other purpose.

The Court found that the FLRA misunderstood this holding to mean that, if OIG investigators were “representatives of the agency,” they were subject to all of an agency’s obligations under the FSLMRS. If this were so, the FLRA concluded, the agency head could negotiate and compromise an OIG’s investigative rights so long as the result was not inconsistent with Federal law. This interpretation would have expanded the union’s rights and would have directly interfered with the ability of OIGs to conduct investigations.

More support for OIG independence in INS case

The most interesting aspect of the United States Department of Justice (INS) v. FLRA, supra, is that its ruling directly contradicts the Third Circuit’s holding in the DCIS case, which, as mentioned above, found that a DCIS investigator was an agency representative for purposes of the FSLMRS.

The DOJ INS case addressed a narrower question than NRC’s in its battle with FLRA in the case just discussed.

The case arose when the DOJ OIG opened an investigation of a Border Patrol agent suspected of, *inter alia*, selling government ammunition, and falsifying his time and attendance records. The suspect’s union representative was allowed to be present during the interview with the OIG agent (really an INS employee serving as the OIG’s representative for this purpose). However, during the interview, the suspect asked to stop the proceeding twice so he could meet privately with his union representative. The OIG agent denied the request.

The OIG agent also interviewed the union representative to ask about information he had received from the suspect. The union representative refused at first, stating that the conversations with the employee were “privileged.” After the OIG agent told him there was no such privilege and that he was required to testify about what he knew of the employee’s misconduct, the representative answered all questions about the employee’s misconduct that he had learned from their talks.

The union then brought unfair labor practice charges against the OIG, asserting that the refusal to permit the employee to talk privately with his representative during the examination, questioning the representative and the employee about their “privileged” conversations, and generally restricting the representative’s conduct during the interview, violated the FSLMRS. The Administrative Law Judge and the FLRA upheld the unfair labor practice charges.

FLRA overruled again

On appeal to the U.S. Court of Appeals of the District of Columbia Circuit, the Court overturned the FLRA’s ruling. The fact that the OIG investigator and the suspect were employed by the same “parent agency,” the DOJ, did not convince the court that the OIG agent was acting as a “representative of the agency” under Section 5 U.S.C. 7114(a)(2)(B), permitting union representation. It would be just as incongruous, said the court, for an employee to be permitted a union representative when he is called before a grand jury or an FBI interview, because United States Attorneys and FBI agents are also Justice employees.

The Court also cited the NRC case with approval, and used strong language to support the OIG’s statutory independent authority to decide “when and how” to investigate. That authority would be impaired if another Federal agency, i.e., the FLRA, could influence the OIG’s performance by finding unfair labor practices against OIGs. “The IG does not stand in the shoes of management,” said the Court. To perform his duties independently and objectively, the IG cannot side with management or the union.

The Court did state in a footnote that any person would be prudent to secure legal representation if they are to be questioned under oath. It cited the Administrative Procedure Act provision, 5 U.S.C. Section 555(b), which provides that anyone, “compelled to appear before an agency or representative thereof is entitled to be accompanied, represented, and advised by counsel.” In our view,

(continued on page 36)

this statement breaks no new ground of concern to OIGs. OIG agents have no testimonial subpoena authority and thus cannot “compel” an appearance. Accordingly, agency employees who are required by regulation or instruction to cooperate with an OIG investigation, do not have the right to bring their attorneys along to the interview, although many OIGs will allow it. In sum, the OIG performed no unfair labor practices in refusing to permit the suspect Border Patrol employee from conversing privately with his union representative or in talking with the union representative about the suspect’s misconduct.

With respect to the argument that the conversations between the employee and his union representative were “privileged,” the Court said that the privilege derives from the employee’s right to union representation. Thus, it is good as used in cases against management; however, the OIG, an independent entity, is not management in this labor relations context.

Conclusion: OIGs stronger and more independent

These two cases should hearten the OIG community because they clearly evidence Federal courts’ recognition of the OIGs as independent, criminal investigators, in addition to being civil and administrative fact-finders. In order to carry out their criminal investigative mission, OIGs need the tools that the other traditional law enforcement agencies use, even if they use them infrequently or in different ways. One of these tools, the freedom from imposition of Federal employee labor laws, is intended to protect Federal workers in the labor-management, but not the criminal, context. The OIG community can also be proud that it rallied quickly and decisively to assert its statutory authority.□

Things Your Mother Never Taught You: The OIGs' Auditor Training Institute and Criminal Investigator Academy

By Andrew J. Pasden, Jr. and Kenneth R. Loudermilk

A significant achievement of the President's Council on Integrity and Efficiency (PCIE) is its success in establishing organizations to train auditors and investigators from every Federal OIG. For years, the PCIE has sought to provide consistent, professional and affordable training for auditors and investigators that emphasized the special and unique needs of the OIG community. In 1991, the PCIE launched its Auditor Training Institute at Fort Belvoir, Virginia. The Criminal Investigator Academy at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia opened its doors 2 years later. In a relatively short period of time, these organizations have become focal points for the continued professional development of OIG employees. In addition, students from outside the OIG community are welcome to attend sessions on a space available basis. The Directors and staff of both training facilities work closely together to coordinate and supplement course offerings for each discipline. They facilitate an exchange of speakers and instructors between the two sites to take advantage of the professional expertise available from each organization. The operations of the Auditor Training Institute and the Criminal Investigator Academy mirror the essence of the Inspector General concept of two distinct professions working together to achieve a common goal.

The Inspectors General Auditor Training Institute (IGATI)



By Andrew J. Pasden, Jr.,
Director, Inspectors General
Auditor Training Institute

IGATI is located at Fort Belvoir, Virginia, about 20 miles south of Washington, DC on the Potomac River. It operates as a joint PCIE effort, with the Department of the Treasury OIG serving as the lead

agency. The PCIE's Audit Committee members serve on IGATI's Board of Directors.

Affordable, quality training for auditors to meet "Yellow Book" standards had long been a concern of the OIG community and had been the subject of two PCIE studies. The IGs were not satisfied with the training available to their auditors because the courses available from the private sector, as well as colleges and universities, addressed broader topics and served a much larger audience of auditors than just those employed by Federal OIGs. Since it was almost impossible to obtain needed training from outside sources, OIGs often resorted to in-house training as an alternative. The problem, of course, was that besides being very costly to design, maintain, and deliver, in-house training took the most experienced auditors away from their normal audit activities and put them in the roles of course

IGATI (continued on page 38)

The Inspector General Criminal Investigator Academy (IGCIA)



Kenneth R. Loudermilk, Director,
Inspector General Criminal
Investigator Academy

The same training problems that plagued the audit side of the house were also experienced by the OIG investigative community prior to the establishment of IGCIA. The unique needs of OIG

criminal investigators could not be adequately addressed by outside sources, and in-house training proved expensive and difficult to schedule and deliver. In August 1993, the PCIE sought to remedy these difficulties by establishing the IGCIA at FLETC in Glynco, Georgia, midway between Savannah and Jacksonville, Florida. The PCIE's Investigations Committee members serve on the IGCIA's Board of Directors.

The IGCIA provides a cadre of experienced professional OIG instructors who are dedicated to improving course content and instruction and to developing and presenting additional advanced training specific to the needs of the OIG criminal investigator. The location was selected to take advantage of the FLETC's unique training facilities and excellent instructor staff. A few of the FLETC resources used by the Academy include firearms ranges, raid

IGCIA (continued on page 39)

IGATI (continued)

designers and classroom instructors. Also, in-house delivery of nearly identical basic auditing courses at several OIGs resulted in considerable duplication of effort and cost throughout the community.

As a solution to this dilemma, in December 1990 the PCIE members voted to establish IGATI. It is the only training organization that addresses the unique audit responsibilities of the Federal OIGs. The appointment of the Audit Committee members to the Board of Directors ensures that IGATI's courses are focused on current training needs within the community. All training programs must be approved by the Board before they can become a part of IGATI's curriculum. Senior OIG audit officials are active players in the selection and development of specific topics that are taught in the programs.

Currently the curriculum includes 13 programs that range in length from 2 days to 3 weeks. Three programs are designed to teach basic skills and abilities auditors need as they progress into positions of higher responsibility within the OIG audit organizations. The first is intended for entry level auditors, and focuses on the skills and abilities needed to perform tasks expected of them during their first 2 to 3 years in the profession. The second program is aimed at those auditors who have advanced to a level where they are expected to function with a greater degree of independence, usually after they have gained 2 or 3 years of experience. The third is designed for first line supervisors who have primary responsibility for planning, conducting, and reporting on the results of an audit.

Another group of three programs concentrates on the skills and abilities needed to conduct financial statement audits in the Federal environment. In these programs, special emphasis is given to teaching how to satisfy the requirements of the Chief Financial Officers Act. A third set of programs zeros in on the auditor's requirements to design and conduct steps intended to look for fraud. One of the programs covers the auditor's basic responsibilities as set forth in the Government Auditing Standards and discusses briefly many of the different types of fraud that can be perpetrated against the government. The other programs delve more deeply into specific types of fraud and the methods auditors can use to discover them.

The final group of programs for auditors deals with technical skills that are necessary to be successful in many different

types of audit settings. For instance, one teaches how to make effective audit-related presentations, such as entrance or exit conferences, briefings, or oral audit reports. Another program shows how to use the tools and techniques developed by Dr. Edward Deming to isolate abnormal variations in an ongoing process, and thereby direct audit efforts toward identifying the causes of those situations. IGATI also offers a program for OIG criminal investigators designed to provide a working understanding of the audit process and an appreciation of how the work of auditors can be very beneficial to the successful completion of an investigation.

IGATI's Deputy Director is responsible for the development and delivery of the training programs. This person supervises a small cadre of professional auditors who form the nucleus of the instructor corps. Currently, there are four instructors on board, three of whom are on detail from various OIGs. The salaries and related costs are paid by IGATI. This staff performs the majority of the program development work as well as serves as the thread of consistency in the curriculum.

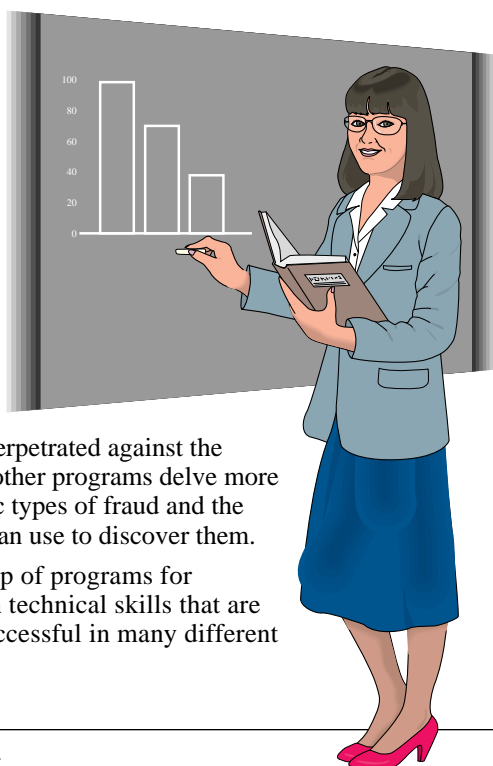
The total instructor corps is much larger, however, totaling nearly 200 itinerant volunteers from throughout the OIG community who teach sessions ranging in length from 1 to 8 hours. There is a wealth of talent in the various OIGs that the IGATI constantly taps in an effort to ensure that our auditors are given the very best opportunity to learn their profession. Active participation by frontline auditors brings many benefits to the training and education of OIG employees. To ensure quality instruction, IGATI maintains a program to train and accredit instructors.

In FY 1993, the Congress provided a special "no year" appropriation to cover IGATI's start-up costs. This interim financing was provided with the understanding that within 5 years, IGATI would become financially self-sufficient by charging tuition for its programs. The Board of Directors has taken this mandate very seriously, and anticipates that IGATI will reach the financial "break-even" point in FY 1997, 1 full year ahead of the schedule Congress outlined when it provided the start-up funds.

The Board of Directors has been very careful not to let the Institute grow at too fast a pace, although growth has been substantial. Quality training will continue to be IGATI's primary goal. The first training program began in July 1991, and the second was not added until April 1992. By September 30, 1994, the curriculum had grown to seven programs. Currently, 13 programs are up and running.

Graduation statistics reflect the steady growth pattern. In FY 1991, 97 students attended IGATI programs. The totals grew to about 400 in FY 1992, 675 in FY 1993, and 850 in FY 1994. In FY 1995, IGATI expects to graduate more than 1,300 students.

For more information about IGATI, please write or call: Inspectors General Auditor Training Institute, P.O. Box 518, Ft. Belvoir, VA 22060-0518, (703) 805-4501, fax (703) 805-4503. □



IGCIA (continued)

houses, interviewing complexes, role player services, and a 3-acre athletic complex. To date, the IG CIA has graduated over 200 students from its basic and advanced training programs.

Generally, the IG CIA adheres to the curriculum development and revision processes employed by the FLETC. Both involve direct input by the IG CIA's customers at curriculum development and revision conferences, which are held periodically at the FLETC. Students attending IG CIA training programs are requested to critique each course and the overall program. This feedback system also contributes to revision of the curriculum.

IG CIA currently offers the following training programs:

Inspector General Basic Training Program (IGBTP)—This program, developed in 1991, is managed by the FLETC's Financial Fraud Institute. In response to customer input, the IG CIA revised this program by changing the emphasis to written and oral communications and advanced law enforcement skills. The length of the program was also reduced to 2 weeks. Two courses in advanced interviewing and three advanced firearms courses have been added to the program along with a basic writing skills course and practical exercise. A "continuing thread" investigation takes the student from the initial complaint through case planning, conducting interviews, and writing memoranda of interview to a presentation before an Assistant U.S. Attorney.

Contract Fraud Agent Training Program (CFATP)—As a recognized expert in procurement fraud, the Department of Defense (DOD) OIG shared its contract fraud training program with IG CIA. Through additional course development, this intensive 5-day advanced program is appropriate for all agencies conducting procurement fraud investigations and includes the latest changes to the Federal Acquisition Regulation. This program is taught by DOD OIG employees.

Accounting Overview for Special Agents (AOSA)—DOD OIG also provided its 3-day Accounting Overview advanced program for special agents. Students are trained to understand general accounting terms, the auditing process, and how to work more effectively with the government auditor.

Employee Conduct Investigations Training Program-For Criminal Investigators (ECITP-CI)—The USDA OIG helped to adapt its Employee Conduct Investigations program. This advanced program is for the criminal investigator who will be working criminal and non-criminal misconduct investigations against agency officials. This program stresses communication skills, investigative skills, and legal considerations. USDA and IG CIA employees and other subject matter experts are utilized in this training. A "continuing thread" investigation has been developed for this program to enhance the learning experience. Students prepare a plan of investigation, conduct a subject interview, and prepare a written sworn statement.

Employee Conduct Investigations Training Program-For Non-Criminal Investigators (ECITP-NC)—This USDA program is targeted at persons who conduct non-criminal employee misconduct investigations. This program is designed for organizations that use non-GS 1811 personnel

in conducting employee investigations. It is similar to the ECITP-CI except it provides additional training in interviewing techniques.

Transitional Training Program (TTP)—This shortened version of the IG Basic Training Program was developed by the IG CIA staff for criminal investigators with 3 or more years of experience in a traditional law enforcement organization who have recently transferred to an OIG. These agents know how to interview and write reports, but they need to learn about the Inspector General Act, safeguarding employee complainants, and serving IG subpoenas. Emphasis in this program is on subjects relating directly to OIG special agent duties and responsibilities.

Hotline Operators In-Service Training (HOIST)—This training previously was provided by the PCIE in Washington, DC. IG CIA strongly believed that the unique training facilities at the FLETC, primarily the interview complexes and role players, could greatly enhance this training. This program was developed by IG CIA in consultation with the OIGs and will change each year as needed to provide basic and advanced training to hotline operators.

Bloodborne Pathogens Training Program (BPTP)—IG CIA developed this program to assist OIGs in meeting Occupational Safety and Health Administration (OSHA) and Presidential directives. This export program meets the requirements of the OSHA regulation and Presidential order concerning workplace training on bloodborne pathogens. The cost is minimal because the trainer travels to the OIG's location.

Undercover Agent Training Program (UATP)—IG CIA used the more traditional curriculum development conference process to develop this program. Several OIGs sent personnel experienced in conducting or managing undercover operations to participate in this conference. U.S. Customs Service, the Bureau of Alcohol, Tobacco and Firearms, Internal Revenue Service-Internal Security, and FLETC also provided experienced personnel to help develop this program.

While IG CIA's primary mission is to provide direct training to its customers, it also performs several other functions to assist OIGs with their training. IG CIA assists in locating sources of specialized training from both contract and government sources. In the past year, IG CIA assisted four OIGs in developing in-service training in conjunction with FLETC. IG CIA also co-hosts the annual Association of Directors of Investigation conference held at FLETC and has assisted several OIGs in developing their bloodborne pathogens exposure control plan and assisted an overseas OIG field office in developing an agency-wide physical fitness program.

Recently, FLETC asked the IG CIA to assist the United Nations in developing a training program for its newly formed investigations unit. This investigations unit, patterned after an OIG, would have worldwide jurisdiction and oversee multi-million dollar programs. IG CIA, working with FLETC, developed and conducted a 2-week training program specific to their needs.

IG CIA (continued on page 40)

IGCIA (continued)

IGCIA represents the PCIE at the FLETC. The Director of the Academy is on the FLETC Intra-Agency Council and the Participating Organizations' Partners in Training group. A member of the staff participates in all relevant conferences for revising or developing training programs at the FLETC.

The IGCIA's staff consists of a director, a training technician, and four course developer/instructor positions, one of which remains vacant. The bulk of the courses are taught by IGCIA and FLETC instructors. IGCIA also relies upon itinerant volunteers from various OIGs and other agencies to instruct in courses requiring specific technical expertise in some of the advanced training programs.

Four OIGs fund the director and each of the instructor positions and three OIGs jointly fund the training technician position. In FY 1996, OIGs will contribute pro rata shares of the costs for IGCIA staffing and operations. Currently, OIGs contribute only toward IGCIA operating costs. Additionally, a modest tuition is charged to cover program costs, such as textbooks, role players, and room and board.

IGCIA will continue to assess the training needs of its customers and respond with programs designed to meet the unique needs of the OIG investigative community. For additional information, please contact the IGCIA, Building 69, FLETC, Glynco, GA 31524, (912) 261-3768, fax (912) 267-3473. □

Practical Evaluation For Public Managers: Getting the Information You Need

by Michael Mangano, Penny Thompson, Jack Molnar, and Brenda Stup

The following article is adapted from the publication, Practical Evaluation for Public Managers. The book describes the authors' evaluation system and their experiences, makes a strong case for program managers themselves to go beyond routine data collection to analyze and evaluate their programs, and presents low-cost, accessible strategies for accomplishing this.



Michael Mangano,
*Principal Deputy Inspector General,
Department of Health and Human
Services (HHS) OIG*



Penny Thompson, Chief,
*Health Care Branch, Office of
Evaluation and Inspections,
HHS OIG*

Jack Molnar, Senior Analyst,
*Social Security Administration OIG
(former HHS OIG employee)*



Brenda Stup, Senior Analyst,
*Social Security Administration OIG
(former HHS OIG employee)*



How many times have you discovered you were missing a critical piece of information and...

Couldn't figure out why service-delivery was inefficient?

Couldn't understand why clients seemed dissatisfied?

Couldn't answer an inquiry about your program's accomplishments or weak spots?

Couldn't make a strong case for additional budget dollars?

Couldn't assess the extent of program fraud or abuse?

Couldn't be sure you made the right decision about which action would make the most significant program improvement?

You may have missed an opportunity because you lacked timely and reliable information. Armed with the right information, you could have made more informed decisions, eliminated a bottleneck, understood your clients' problems, documented your program's strengths and weaknesses, effectively argued for resources, protected the program from profiteers, or known which changes would produce the biggest payoff.

If you are a program manager or analyst, you are probably inundated with data and statistics. You may not even recognize an information deficit. Yet you may often find you don't have data-based answers to policy and operational questions when you need them, despite the huge investment being made in data collection and reporting in public programs.

This article is about getting the information you need in a timely manner and at a relatively modest cost. By "information," we mean something more than the data typically produced by management information systems. Rather, we use information to mean a collection of facts and logical conclusions about them which answers the types of questions we posed above. By learning and using a variety of strategies for obtaining information, you can better address specific problems, gain insight into what's happening in your program, and determine what directions you should be taking. These strategies can help you reduce complexity and uncertainty in your day-to-day decision-making and see beyond the many immediate problems you face.

(continued on page 42)

Sharing techniques and approaches

This article describes the methods used by a group of professional analysts dedicated to putting practical program information in the hands of the people who need it in time to make a difference. The strategies we present are drawn from our experience as analysts in the HHS OIG.

Our organization, the Office of Evaluation and Inspections, comprises about 100 analysts who come from a variety of educational and occupational backgrounds. Stationed across the country, we work in teams to conduct short turnaround evaluations of HHS programs.

We tend to be very pragmatic in our outlook and approach. We search out the methods and data sources that will produce the best information in time to be useful. In fact, we measure our success in terms of program improvements and dollars saved or put to better use. We strive to anticipate critical issues. We define our studies using a relatively sharp focus. Our techniques allow us to reach logical conclusions rather than definitive answers. We believe timing is the key to our success and that, no matter how accurate, information provided too late is of little value.

We are interested in making our commonsense approach to evaluation—providing outcome-oriented, practical information for immediate use—available to program managers and others who may not consider themselves evaluators.

Why evaluate?

The American public is demanding better government. As the private sector devotes more attention to meeting customers' needs, people want and expect the same responsiveness from government. We look to the Federal Government to provide for a common defense, to collect taxes, to assist the needy, to regulate health care, to monitor air quality, to operate parks, to keep defective products off the market...the list goes on and on. However, the staffing levels and budgets that previously sustained these programs and services are shrinking.

Is it really possible to “do more with less,” and “work smarter, not harder?” The evidence from the private sector seems to say it is. Over the last decade or more, innovative managers in a number of industries have shown us a virtual quality explosion coupled with significant cost reductions. They did it by investing in employee training and modern equipment, reducing the ranks of middle management and empowering all staff, redesigning products to stress quality and “delight” customers, rethinking basic processes, and focusing on the long term. This is how the U. S. automotive industry, particularly Ford and Chrysler, turned itself around and became competitive again.

People have begun to realize that if such dramatic improvement can be achieved in the private sector, it can be accomplished in the public sector as well. We are seeing the results of this awareness in several initiatives to improve accountability in the management of Federal programs.

Reporting out the results

In November 1990, the Congress passed and the President signed the Chief Financial Officers Act. One of the objectives of the Act is to “provide for the production of complete, reliable, timely and consistent financial information for use by the executive branch of the government and the Congress in the financing, management and evaluation of Federal programs.” The Act also requires agencies to collect information needed for “the systematic measurement of performance” and to report the information in their financial statements. Managers of Federal agencies covered by the Act are required to establish indicators for assessing their programs and to report the results of their assessments to Congress. The measurements can include inputs, outputs, outcomes, and impacts. Managers will now be held publicly accountable for program accomplishments.

The Government Performance and Results Act of 1993 further strengthens Federal government accountability by mandating quantifiable program results. In passing this law, Congress set out to “improve the confidence of the American people in the capability of the Federal government, by systematically holding Federal agencies accountable for achieving program results.” The law requires each agency to “establish performance indicators to be used in measuring or assessing the relevant outputs, service levels, and outcomes of each program activity.”

Managing for quality

These new requirements for accountability to Congress, and, more importantly, to the taxpayer, demand new information-gathering strategies for managing Federal programs. As we noted in the introduction, current management information systems often provide a profusion of data without answering basic questions about program effectiveness. A change in philosophy within government highlights this “information deficit” perhaps more than any new statute. Learning the lessons of the private sector, many public managers have adopted Total Quality Management (TQM) as a guide to improving performance. While there are differences among approaches to TQM, all have in common some basic tenets: continuous improvement, client focus, employee empowerment, investment in training, strategic planning, and quality measurement.

TQM requires good information. To continuously improve your program, you have to know which processes and systems need improving and where the biggest impact on your operations can be gained by new strategies and ways of doing business. You will need to evaluate the effects of the changes you make, to determine when new problems crop up, and to deal with unforeseen obstacles that prevent you from achieving the good results you intend. You will need to set performance standards appropriate to the fundamental purpose of your organization. By showing progress toward those standards, you can convince others of the value of your improvements. Documented progress will help garner support from your staff and, eventually, the public. It will enable you to build on your successful

initiatives. Further, it will assist the executive and legislative branches in resource allocation, to your benefit.

However, good measurement systems need “care and feeding”—ongoing analysis and refinement. This requires some investment in establishing and maintaining those systems. TQM teaches us to consult regularly with our customers, in our case, the public, Congress, and other organizations impacted by our products, in instituting performance standards and measurement systems.

Reinventing government

These new philosophies about government’s role and about how government should respond to changing expectations are described in Osborne and Gaebler’s book Reinventing Government. By challenging many of the traditional roles and methods of government, Osborne and Gaebler demand that public managers reassess what they do. One of the most notable responses to this challenge has been Vice President Gore’s 1993 National Performance Review (NPR). Modeled after the Texas Performance Review, the NPR entailed a major assessment of all Federal programs. On a smaller scale, such efforts now are taking place at all levels of government, and not as one-time reviews. We are entering a period where programs need to “reinvent” themselves as times and challenges change. You as a program manager will need to evaluate your agency’s performance and to assess the external environment on an ongoing basis to ensure your success.

The direction is clear. To be successful, government managers will have to develop the skills and tools to evaluate program performance. Your ability to respond to public pressure for effective and efficient service delivery will depend on your ability to get the information you need when you need it. You can plan an active evaluation program to meet your own information needs and set your own performance standards...or you can wait for others to tell you what to do.

Evaluation strategies

Evaluation, as we defined it earlier, means obtaining information for use in decision-making. So the first step in deciding what kinds of evaluations you should undertake is to decide what your questions are. Some examples of key questions that may not be easily answered from data you now collect are: What are the unintended harmful effects of your program or bottlenecks impeding efficient service? How do beneficiaries, interest groups, or your own workers view the program? How vulnerable is your program to criminal abuse?

A number of specific types of evaluation techniques can help answer your key questions.

Client satisfaction surveys use public opinion survey techniques to determine the nature and extent of clients’ experiences with a program and to assess their satisfaction with the services they received. These surveys can determine the extent to which the entire population of clients is

satisfied with service, the satisfaction levels of certain groups of clients, and what kinds of experiences or services are related to high or low rates of satisfaction.

Traditionally, government managers have relied on their own expertise and operating reports to make decisions on how to run their programs. Program assessments have centered around inputs and outputs, based on criteria internal to the organization’s operations. If you are a manager, more than likely you could tell us at the drop of a hat your processing time and accuracy for a particular workload, whether this is acceptable performance based on the size of your staff, and whether this meets regulatory standards. What you may not know is how important or acceptable this performance is to your clients. TQM quickly teaches us to look to the client to define quality. In this new operating environment, program quality is often measured in terms of success in meeting clients’ needs and expectations.

TQM also broadens our concept of “client.” In the conventional view, the clients of a program are the end-users of its products or services, such as Social Security or Medicare beneficiaries. However, when we define clients as the people or organizations who affect or are affected by the program, as prescribed under TQM, we begin to identify many other kinds of clients. These may include:

- program staff,
- service providers,
- other government agencies, or
- private sector groups that are subject to program regulation or that rely on program data.

As you and other government managers go about “reinventing” your programs to meet clients’ needs and expectations, you will have to develop client-based performance goals and indicators to assess your progress. The basic way to do this is to get input directly from your clients.

Performance indicator studies identify and test possible gauges of inputs, outputs, and outcomes that indicate how effective and efficient a program is at achieving its intended purpose. While performance measurement terminology is still somewhat variable, indicators can be described as representing “what,” or a quantity of inputs, outputs, or results. Measures, on the other hand, express “how well” as a ratio of input to output, of output to results, or of output or results over time. Thus, the relationships between and among indicators can give you useful information about the success of your program. Since indicators form the basis for performance measurement, they will be our focus in this chapter. (Although for simplicity we discuss the “program” as a whole, performance indicator studies also can be used in managing individual components of a program, such as customer service or quality assurance.)

As we discussed earlier, performance measurement is becoming very important to public managers, who are being held increasingly accountable for the success of government programs. Both the Chief Financial Officers Act and the

(continued on page 44)

Government Performance and Results Act require Federal managers to measure performance. The management concepts that form the basis of TQM and reinventing government also depend on the use of performance measurement.

We're all familiar with performance measures. Teachers grading students are measuring performance. Supervisors rating employees also are measuring performance. Other measures are far less systematic or formal, such as the number of requests for a recipe or the number of complaints about a barking dog. While the process is generally imperfect and often criticized, performance measurement, in one form or another, is a routine part of our lives.

Yet the science, or perhaps art, of developing and using performance indicators and measures is still somewhat in its infancy in government. In the past, public programs have captured a great deal of data on inputs (budgets, staff) and outputs (numbers of clients served, number of claims processed). For the most part, these things are easily measured. However, the public sector hasn't collected much information on outcomes or impact, the ways in which a program fulfills its fundamental purpose. Output measures provide feedback on your program's achievements but may show you very little about whether those achievements led to meaningful results. Outcome measures give you feedback on whether the results you were looking for actually occurred but less information about whether your program was responsible for them. In such an imperfect world, program managers need to develop and test a variety of measures and obtain advice from a wide range of stakeholders.

Compliance reviews involve assessing an activity or output and comparing it to a standard. As covered in the last chapter, performance measures assess how well the program is meeting its basic purpose. This purpose may or may not be stated explicitly in statute or other legally binding form. On the other hand, compliance reviews are designed to determine if specific activities are occurring in accordance with legal, regulatory, and administrative requirements.

As a public sector manager, more than likely nearly everything you do is governed by law and regulations. Your program—its purpose and authority, its funding, and possibly even your job—is established by law. Details about the processes you use to administer your program may be legislated. If your organization funds other public agencies or service providers, the nature of their involvement in your program may be mandated also. These laws, and the regulations that implement them, serve as standards against which your program's performance can be measured.

You probably already produce or receive information about program compliance—audits and legislatively-mandated reports. However, at any point in time, your chief executive may want to know if you, your contractors, or grantees are meeting legal standards that aren't routinely monitored. Legislative oversight bodies may, too.

Shouldn't you be the first to ask and answer these questions? Using evaluation techniques to investigate compliance issues can prepare you for such challenges as well as give you a deeper understanding of what's happening in your field operations.

Effective practice reviews are a way to learn from the successes of others—to discover methods, processes, projects, or practices that have the potential to work well for similar programs. Often, program managers rely on their own personal experience and judgment to assess and decide among alternatives. Those wanting definitive answers can invest in evaluations that assess impact over long time periods. While personal experience is often too limiting, such impact evaluations are often too costly and time-consuming. Effective practice reviews provide a middle-ground approach. They look for lessons learned by a number of professionals or at a number of service-delivery sites. They sacrifice some of the precision of full-scale impact evaluations in exchange for faster (and less costly) information.

Effective practice reviews draw on a number of analytical techniques including:

- reviewing prior studies to see if certain innovations have already been proven effective,
- collecting opinions from the people most familiar with the program or issue about whether or not a practice works well or holds promise,
- analyzing available data to determine if the implementation of a practice has resulted in improved program outcomes over time, and
- making on-site visits to directly observe the effectiveness of program activities.

The findings from effective practice reviews provide program managers with a basis for saying, "This idea might work for us."

Early implementation reviews are studies that assess the vulnerabilities, problems, and successes of a new initiative or program during the start-up period.

New mandates and requirements provide one of your best opportunities to test the usefulness of developing an evaluation capacity for your program. Any venture into uncharted territory comes with risks. Your role in implementing new responsibilities may involve taking on new and different functions, providing service to new clients with unfamiliar needs or characteristics, interacting with new provider groups or industries, or creating new policies, procedures, or data systems. Regardless of how well you've planned the implementation of these new requirements, some unanticipated problems will almost certainly arise, and they can have serious consequences.

Emerging issue reviews are evaluations that help you scan the environment to identify new trends that represent potential problems, challenges, or opportunities for your program. Think about how you would use evaluation if you

worked in the private sector. In addition to assessing your clients' satisfaction with your product or service, you would test the marketplace to see how you could make your clients even happier. You would explore ways to expand your client base, your services, or your product line. You would continuously monitor the environment and its effects on your clients' willingness to use your products or services.

A strong analogy can be drawn between market research in the private sector and environmental scanning in public programs. Program managers can pursue policy and issue development purposely and reflectively, in the same way as managers in private enterprise. While the bottom-line motivation for the private sector is beating out the competition, the objectives of environmental scanning for both private and public managers are surprisingly similar. For example, you might "test the marketplace" to determine:

- if your customers' needs are changing. You may be able to offer a new product or service to increase your clients' support for your program.
- if your customer profile is changing, e.g., if your customers are older or younger, or more urban, suburban, or rural than they used to be. You could use this information to determine the effect on demand for your product or service and to anticipate future changes.
- if your customers, despite liking your product or service, are having concerns about its effect on their health or the environment. You might use this information to change your product or service to address customers' concerns.
- if your advertisements communicate your message clearly to potential new customers. You should use this information to know if you are targeting your information to the right groups and communicating effectively with those audiences.

Conclusion

By now, we hope we've convinced you of the benefits of developing or improving the evaluation capacity of your program. We'd like to remind you of the forces leading you in this direction: the Chief Financial Officers Act, the Government Performance and Results Act, the NPR, and TQM, all of which are designed to make government programs more accountable to the public they serve. We also hope that our discussion of different evaluation strategies has given you some practical ideas (and enthusiasm!) for putting evaluation to good use in your program.

Once you've made program evaluation an integral part of your management system, we believe you'll quickly see significant uses for the results, whether you are testifying before a legislative committee, meeting with your Chief Financial Officer, vying for program resources, striving to meet clients' needs and expectations, or planning for the future. At times, the payoff from your evaluation activities may seem small and you'll be tempted to put your money or staff elsewhere. Yet the benefits of evaluation are more than the findings of a single study. Since program evaluation is basically a process of asking and answering the right questions and using the results to achieve improvements, it builds on itself. It can energize your approach to the problems and opportunities you encounter. Program evaluation ultimately can change the entire culture of your organization as it frees people from rigid, short-sighted patterns of thinking and as it focuses everyone's attention on the real purpose for the program's existence.

For more information

Copies of the full publication, Practical Evaluation for Public Managers, are available by request by writing the U.S. Department of Health and Human Services, Office of Inspector General, 330 Independence Avenue, S.W., Room 5660, Washington, DC, 20201. □

Calendar of Professional Meetings & Events for 1995

Date	Time	Event	Contact
Sept. 12	2-4 pm	President's Council on Integrity and Efficiency (PCIE) Meeting	Jenny Banner Wheeler (202) 619-3081
Sept. 13	2-4 pm	Executive Council on Integrity and Efficiency (ECIE) Meeting	Hubert Sparks (202) 884-7675
Sept. 14	2-4 pm	Joint Financial Management Improvement Program (JFMIP) Steering Committee Meeting	Donna Tebeau (202) 512-9201
Sept. 18	2-4 pm	Inspector General/ Chief Financial Officer (IG/CFO) Conference	Martie Lopez-Nagle (301) 415-5898
Sept. 20	10 am	Counsel of Counsels to the Inspectors General (CCIG) Meeting	Harry Jorgenson (202) 973-5019
Sept. 26	9 am - 12 noon	Fresh Page: Re-engineering the Office of Inspector General Model Forum	Martie Lopez-Nagle (301) 415-5898
Sept. 28-29		American Institute of Certified Public Accountants (AICPA) Update Conference	Mary Foelster (202) 434-9259
Oct. 10	2-4 pm	PCIE Meeting	Jenny Banner Wheeler (202) 619-3081
Oct. 11	2-4 pm	ECIE Meeting	Hubert Sparks (202) 884-7675
Oct. 12	2-4 pm	JFMIP Steering Committee Meeting	Donna Tebeau (202) 512-9201
Oct. 18	10 am	CCIG Meeting	Harry Jorgenson (202) 973-5019
Oct 95		The Wages of Sin: Emerging Issues in Law Enforcement Forum	Martie Lopez-Nagle (301) 415-5898
Oct. 24-25		PCIE/ECIE Retreat	Jenny Banner Wheeler or Martie Lopez-Nagle
Oct. 30 - Nov. 1		AICPA National Governmental Training Conference	Mary Foelster (202) 434-9259
Nov. 9	2-4 pm	JFMIP Steering Committee Meeting	Donna Tebeau (202) 512-9201
Nov. 14	2-4 pm	PCIE Meeting	Jenny Banner Wheeler (202) 619-3081
Nov. 15	2-4 pm	ECIE Meeting	Hubert Sparks (202) 884-7675
Nov. 15	10 am	CCIG Meeting	Harry Jorgenson (202) 973-5019
Nov. 95		Congress Watch Forum	Martie Lopez-Nagle (301) 415-5898
Dec. 12	2-4 pm	PCIE Meeting	Jenny Banner Wheeler (202) 619-3081
Dec. 13	2-4 pm	ECIE Meeting	Hubert Sparks (202) 884-7675
Dec. 20	10 am	CCIG Meeting	Harry Jorgenson (202) 973-5019
Dec. 21	2-4 pm	JFMIP Steering Committee Meeting	Donna Tebeau (202) 512-9201



