The JOURNAL OF PUBLIC INQUIRY

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

SPRING 1996

The JOURNAL OF PUBLIC INQUIRY

Editorial Board

Staff

Editorial Services

Karen M. Shaffer, Social Security Administration OIG

Printing

Frederick Watson, 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

Business Process Reengineering: Choosing The OIG's Role

by Thomas Barchi and Scott Buchan

Thomas Barchi,
Assistant Inspector General for Audits,
Office of Inspector General,
Nuclear Regulatory Commission

Scott Buchan,
Senior Management Analyst,
Office of Inspector General,
Nuclear Regulatory Commission

Business Process Reengineering (BPR) projects are beginning to roll through Government agencies. Supporters talk of BPR efforts sweeping away outdated and time-consuming operations, and replacing them with more efficient and better performing processes. Hopefully. Federal managers performing BPRs on their operations are investing significant time and money, so success is critically important given current budgets. Because of the crucial factors of money, staff, and efficiency, an OIG needs to be aware of BPRs and must determine what role it desires to take as they progress. OIGs will choose different levels of involvement depending on the BPR target, the relationship between the OIG and the Federal agency, and an OIG's resources and philosophy. There are valuable gains to an OIG and the agency to be achieved with OIG involvement; however there are some cautionary limitations to consider as well. On the whole though, if done well, OIG interaction with an agency will give BPRs a greater chance for success, yielding a positive result for the Government and the public.

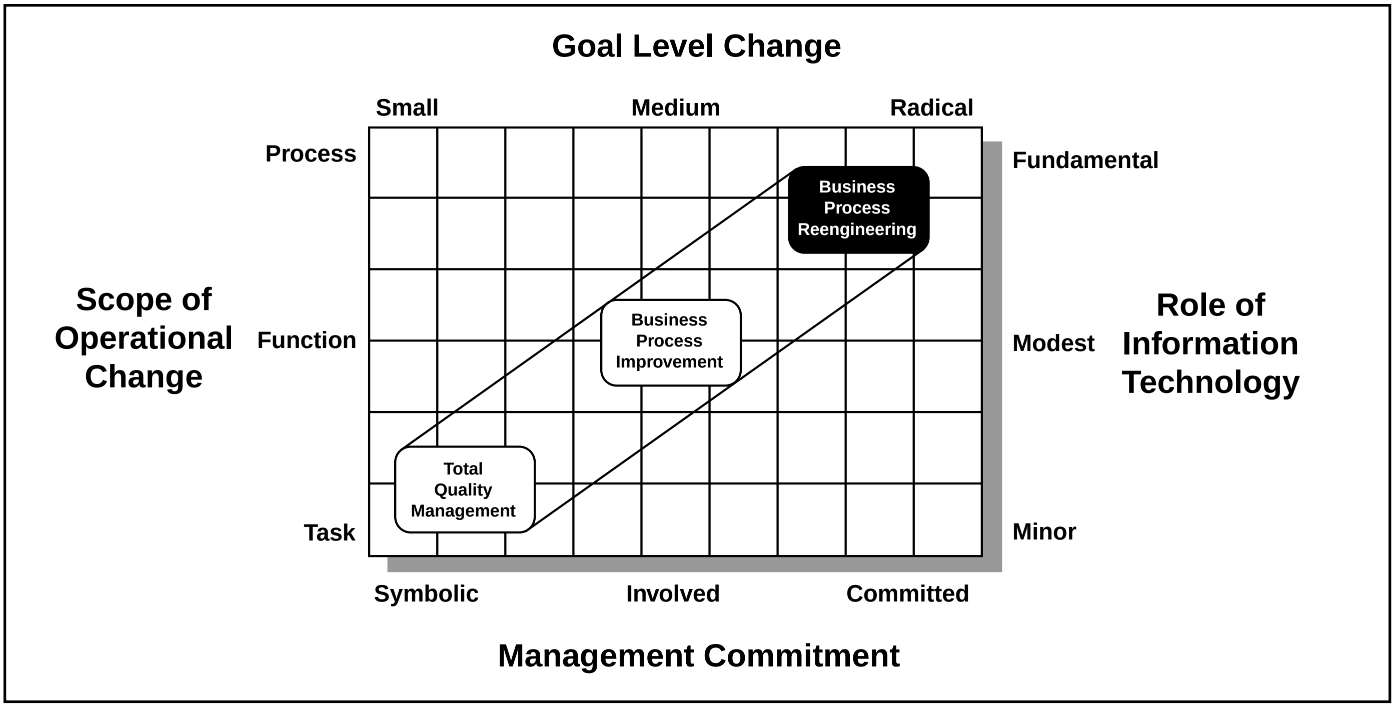
Understanding Business Process Reengineering

BPR is a relatively new term for a combination of techniques, some of which have been used for years, to improve an organization's operations. BPR has been defined as "the concept of fundamentally changing the way work is performed in order to achieve radical performance improvements in speed, cost, and quality," or more simply, "the act of fundamentally changing core processes." The extreme nature of BPR is reflected in two works by Dr. Michael Hammer, an originator of the BPR concepts: *Reengineering: Don't Automate, Obliterate,* and *Reengineering the Corporation: A Manifesto for Business Revolution.* Radical, obliterate, and revolution are terms not usually paired with Federal managers or projects, but that is the level of change that serious BPRs are aimed to achieve. Federal managers are just catching up to the private sector, as firms such as Hallmark, IBM Credit, Bell Atlantic, and Taco Bell have already used this technique to substantially improve their operations. However, it is difficult to determine how many BPRs are being undertaken by Federal agencies, as many efforts that are labeled as BPRs may not actually aim for fundamental and radical change goals. Also, Federal adoption of the technique is new enough that very few agencies have fully completed a BPR effort and implemented changes.

The simple illustration of BPR and other managerial change methods shown in the chart on page 2 highlights the anticipated scale of change and the risks involved. OIGs could use this chart to help evaluate whether an agency has embarked on a true BPR and will achieve radical and fundamental change, or whether the effort will fall short and why. In addition, the General Accounting Office is preparing a *BPR Assessment Guide* to provide its evaluators and other Federal auditors with a generic framework to assess how Federal organizations are managing the tasks associated with BPRs.

The expectations BPRs raise are great, and to achieve such change heavy investments must be made. This inherently means the Federal manager must commit significant time, money, and qualified personnel to a potentially risky endeavor. Risky, because many BPRs will fail. In *Reengineering the Corporation,* Dr. Hammer and J. Champy reported that maybe 50 to 70 percent of BPRs do not achieve the dramatic results their sponsors had desired. However, attention to critical success factors that have been identified by BPR experts can help to manage and mitigate potential BPR risks.

(continued on page 2)



A key ingredient of BPRs is the desire for a radical change in end results. Such aggressive new goals would stretch an organization's ability to perform, thus requiring that a new process be designed. BPR goals are typically a magnitude-plus level of change, not a 20 to 30 percent improvement. For example, the Nuclear Regulatory Commission (NRC) is conducting a BPR that seeks to reduce the time for issuing licenses to hospitals, universities, and commercial users of radioactive materials from an average of 84 days to 4 days, while maintaining public safety at its current level. The Department of Commerce (DOC), Patent and Trademark Office, wants to reengineer its activities so that receiving a patent takes only 45 days, instead of the current 20 months.

To power the BPR effort, Federal managers must be committed to the project above the usual "task force meeting group" level. A *Harvard Business Review* article said that 20 to 30 percent of a top manager's time was necessary to personally lead the BPR and shepherd it through the forest of challenges. BPR is a top-down led change effort that often cuts across organizational boundaries, so a manager must believe in it, fight for it, and be able to force its attainment. Committed top management leadership is especially crucial since an agency may be unaware how hard and long the work of a BPR will be. Most BPRs take about 24 to 30 months to design, pilot, implement, and achieve their desired results. In the Federal Government, it has been suggested that this time frame may be longer, possibly 2 to 5 years until measurable results can be observed. One BPR team leader has described the experience as a "marathon-sprint," needing a strong executive to coach it to the finish line successfully.

Besides the top manager's time, BPRs need quality people in sufficient numbers to challenge old assumptions of how to perform work. Successful teams are made up of people with several diverse skills, such as expertise in the current process, information technology, personnel issues, conducting BPRs, etc. The BPR team will be asked to think "outside the box" of how work was accomplished, and develop what should be done based on what customers value. BPR teams are usually instructed to start with a "clean sheet" of paper to develop a "new vision" that achieves a process organized for better outcomes, rather than a process geared toward managing outputs and inputs. High quality staff are needed who can produce this result, and who can then explain it to the rest of the organization and convince them of the new process' merit.

Assigning staff to a BPR will have a cost to the manager in the normal work that cannot be accomplished. For instance, the NRC licensing BPR is requiring 5 percent of the staff and 55 percent of the Fiscal Year 1996 contract dollars from the agency program undertaking it, which comes directly out of the work that those staff would have been performing. Additionally, the NRC is investing in computer "groupware" technology, enabling headquarters and regional staff to talk with each other and share documents through connections in cyberspace, so they can work together on projects from their local offices. NRC management prepared a business case that showed the short-term pain was worth the long-term gain of a new process to justify its BPR.

An Agency BPR's Impact on the OIG

The amount of resources devoted to conducting a BPR and the expectations of impressive new changes the BPR will produce make them a natural candidate for auditing. Let alone whether the goals of the BPR were achieved or not, other issues are certainly worthy of an independent evaluation: how the agency managed the BPR process;

the way it chose the BPR subject, selected contractual assistance, and invested in information technology; and how it got separate organizations to work together. An OIG can provide value to the agency by developing the lessons that should be learned from the agency's attempt(s) at performing BPRs.

In addition, agency decisions to conduct BPRs can and will influence an OIG's annual audit plan, which may have identified programmatic areas now subject to BPR. It may not make sense for the OIG to audit an area where a brand new "clean sheet vision" process will fundamentally change how the agency accomplishes work there. However, the OIG must make a key decision on several potential courses of action. The OIG could continue to audit an area subject to BPR, since BPRs typically take 2 years or more to implement and the audit could be completed with recommendations to improve a process that will still be in use for another year or more. This may be duplicative of the BPR team's effort or wasted time, but on the other hand the BPR might fail as well. The OIG could also wait to see if the BPR really gets off the ground and appears to be heading in a good direction before deciding to take the subject out of the annual plan. This would let the agency know that OIG won't back away from a BPR-targeted area unless real work is begun. Finally, the OIG might want to participate in the BPR.

OIG Participation in a BPR: Pick the Suit That Fits Best

OIG participation in an agency BPR should be tailored to each BPR, with an eye toward fitting several factors into the level of involvement chosen. Every OIG has a unique relationship with its agency, and even with different units in the agency. An OIG may have a strict "arm's length" association with the agency, while another OIG may be more closely involved and proactive. Also, the OIG's philosophy may range the spectrum from compliance-oriented and oversight-driven to that of a consultant or coach to the agency. As any manager, an Inspector General (IG) must weigh available resources and determine if he or she can provide value to the agency by assigning people to a BPR and feel that the OIG receives value in return. Finally, the OIG must determine whether the agency process that is the BPR subject is an important area or the dollars and staff being devoted to it are significant enough to warrant a certain level of OIG involvement. For any given BPR and OIG, there is likely to be a different suit that is the correct fit.

An appropriate and comfortable role for the OIG oriented toward the traditional oversight function could be to "monitor" the BPR. At the minimum, an OIG cannot afford to be unaware of a BPR's goals and the resources being devoted to it by the agency, in case the IG is requested to testify about the BPR should it fail and dollars are placed at risk. Assigning OIG staff to occasionally interact with the agency's BPR team, via attendance at meetings or through document review, should yield a baseline of information about the BPR that would probably suffice for most monitoring needs.

An OIG could envision a role as an advisor or mentor to the BPR team. This would need more effort from the OIG, and require a relationship that included trust, openness, and communication between the OIG and the agency. The OIG might have particular knowledge about the subject process of the BPR or have developed generic insights about performing BPRs that it could share with the agency. To be successful, the agency managers must believe that the OIG is actually on the agency's side in trying to improve operations and both parties want to move together toward a common goal.

The most participatory OIG role would be to act as a consultant for the agency. The OIG could be a "contractor" providing specific expertise, or even provide staff as full-fledged members of the BPR team. For example, many OIGs have skills in developing and refining meaningful performance measures, which are an integral part of a BPR. As a participant on the BPR team, OIG staff can provide a fresh perspective on problems with the old system that agency staff may not have, and be valuable in thinking "outside the box" to develop a vision for the new process. Almost all OIGs of the 10 Air Force Command groups have reengineered their roles and become coaches to Air Force operational units conducting self-assessments. A unit reviews its operations according to modified Malcolm Balridge Quality Award criteria. The OIGs then critique the assessment's quality, and may use operational strengths identified as a benchmark measure for other Air Force units.

For an alternative role on a more continuing basis, OIGs could act as a repository of agency knowledge on BPRs. Agencies need a focal point to capture information, experience, and lessons from their BPR projects, which may be conducted by various organizations that are widely separated and not in communication with each other in large agencies. The Department of Defense has an office that is performing this kind of role. An OIG could offer guidance to agency BPR teams on avoiding the common errors that most often lead to failure, and offer advice on the methodology, standards, and success factors that have been effective for previous agency BPRs. An OIG could also become a reference source for organizations or BPR teams. An OIG may know, for example, who is good at process mapping, or benchmarking, or identifying the best information resource system that suits a new process. The DOC OIG has developed an expertise with information systems that was recently called upon by DOC during the renegotiation of a prime contract for Next Generation Weather Radar, a success story of agency-OIG relations.

Gains to an OIG by Participating in BPRs

There are several ways that an OIG can collect value through participating in agency BPR efforts, which corresponds to the level of the OIG's involvement. First, an OIG can deliver a timely assessment of an obviously high

(continued on page 4)

visibility issue. This could be a useful tool for helping agency leadership decide whether to support the BPR, and could help the BPR team in its initial work. Second, the OIG can realize a more proactive presence than the traditional OIG role by working with the agency to develop positive change from the inside rather than reporting recommendations from the outside. Working with agency management to replace a process they fully agree is broken could help foster the common bond that the OIG and managers are both interested in improving the agency's programs and demonstrating that the OIG isn't restricted to the "gotcha" game. Third, based upon increased OIG confidence in the value of the BPR technique and agency management's demonstrated commitment to change, the effective coverage of agency operations in need of oversight and auditing by the OIG may be increased. With a small staff investment, an OIG can feel assured of positive change in a program being reengineered without assigning a full audit team to review the program.

Fourth, by partaking in a BPR as an advisor or participant, an OIG can ensure that key issues are included in the BPR effort. In this way, the OIG may be able to finally resolve some long-standing problems it had identified and reported previously, but that never seemed to be addressed or fixed by the agency. Finally, OIG insights developed through close interaction with the BPR could lead to identification of follow-up work for an OIG, including subjects which the agency readily agrees warrant OIG evaluation. We have discussed other gains throughout this paper, and as OIGs and Federal agencies gather experience with using BPRs, there will surely be other positives that come from OIG participation.

Limitations of OIG Involvement in BPRs

On the other hand, there are significant limitations to OIG interactions with agency BPRs that an OIG needs to consider when determining its level of involvement. Any factor by itself could potentially hurt an OIG, or could seriously damage the BPR's chances for success.

Of concern to all OIGs is the perceived or real threat to their independence, which must be guarded against. A close working relationship with an agency on a BPR is not a risk-free activity and could present a perception problem at the least. However, this does not mean that active participation should be ruled out as a matter of course, because thoughtful managers can find ways to work together without compromising their individual roles and responsibilities.

Equally important, probably more so to agency managers, is the concern that participation by OIG staff does not produce a "chilling" effect that might damage the potential for the BPR's success. This effect could be made manifest on agency management or on the BPR team members. Agency management may be hesitant to try a BPR if it feels constrained in dedicating resources to an expensive undertaking or in obtaining certain results. Management might believe OIG involvement could lead to a report with extensive inside information on an unsuccessful BPR. It would be an unfortunate result if a potentially valuable management tool with wide usage in the private sector is taken away from Federal managers because of an anticipated OIG action. Also, a crucial aspect of the BPR technique is the BPR team's development of a new process vision from a "clean sheet of paper." Inappropriate OIG participation might wrinkle the clean sheet through insistence that the new process address problems of the old, but no longer relevant, process. Damage in this phase would likely be fatal to the BPR's chances for success.

A practical limitation to highly active OIG involvement is common almost everywhere in Government today--can the OIG afford to devote precious resources to a BPR? BPRs are time-consuming projects that generally require a full commitment from their members, possibly for a longer period of time than an OIG usually assigns its audit staff to a project. Given budget constraints and other priorities, the OIG must decide if the value from BPR participation is best maximized at various levels of participation. An interesting dilemma could occur where the agency and the BPR would benefit by the OIG's participation but the OIG would not receive a corresponding value, thus creating a true test for showing the OIG's commitment to assisting the agency.

Conclusion: It's a New Day, Go for the Win-Win

BPR is change, radical change. The IG Vision Statement says: "We are agents of positive change striving for continuous improvement in our agencies' management and program operations and in our own offices." OIGs should feel compelled to be knowledgeable about the BPR process, how the process is used in their agencies, and what the OIGs can do to ensure its success. With the encouragement of the National Performance Review reports and the framework of the IG Vision Statement, it's a new day for OIGs to move forward into more collaboration with agency managers to improve programs, and go beyond the compliance-oriented oversight foundation laid down in the IG Act of 1978.

Some form of participation in BPRs is a proactive means to affect positive change in the agency. It can be argued that providing insights to the Federal manager as a process is designed and developed is more beneficial to the public than reactively reporting on its problems at a later time. Observation of, and involvement in, BPRs also allows for greater effective coverage of agency programs by leveraging limited OIG resources. As the OIG feels comfortable that BPRs will improve their target programs, OIG attention and resources can move to other programs.

The Statement of Reinvention Principles of the IG Vision Statement includes two declarations aptly suited to encouraging some form of OIG participation in BPRs on a case-by-case basis: "Be innovative and question existing procedures and suggest improvements," and "Build relationships with program managers based on a shared commitment to improving program operations and effectiveness." Working with the agency in a BPR is a clear embodiment of these principles by the OIG.

The challenge for the OIG is choosing the most valuable role for itself and the agency. The OIG, with agency management, should evaluate its most effective role on a case-by-case basis. This evaluation needs to take into account the BPR subject, resource implications, and the readiness and ability of the OIG and agency to work together. There is no formula for determining the level of participation between an OIG and an agency BPR, and the OIG should be receptive to a range of possibilities. With careful selection and positive handling, the OIG's involvement will result in a win-win for OIG and the agency, and by extension for the Government as a whole and the public.

Sources for Information on BPRs

There is a growing body of literature that discusses reengineering. The following is a selected list of writings that may be useful to OIGs:

Carr, D.K. and others. *BreakPoint: Business Process Redesign.* Arlington, VA: Coopers & Lybrand, 1992.

Caudle, S.L. *Government Business Process Reengineering: Agency Survey Results.* Washington, D.C.: National Academy of Public Administration, 1994.

----- *Reengineering for Results.* Washington, D.C.: National Academy of Public Administration, 1994.

----- *Reengineering for Results: Update.* Washington, D.C.: Alliance for Reinventing Government, National Academy of Public Administration, 1995.

Goss, T., Pascale, R., and Athos, A. "The Reinvention Roller Coaster: Risking the Present for a Powerful Future." *Harvard Business Review*, 1993, 71 (6), 97-108.

Hall, G., Rosenthal, J., and Wade, J. "How to Make Reengineering Really Work." *Harvard Business Review*, 1993, 71 (6), 119-131.

Hammer, M. "Reengineering Work: Don't Automate, Obliterate." *Harvard Business Review*, July-August 1990, 104-112.

Hammer, M. and Champy, J. *Reengineering the Corporation.* New York: HarperCollins Publishers, 1993.

Hyde, A.C. "A Primer on Process Reengineering." *The Public Manager,* 1994, 24 (1), 55-68.

Linden, R.M. *Seamless Government: A Practical Guide to Re-Engineering in the Public Sector.* San Francisco: Jossey Bass Publishers, 1994.

----- "Reengineering to Capture the Customer's Voice." *The Public Manager,* 1994, 23 (2), 47-50.

U.S. General Accounting Office. *Business Process Reengineering Assessment Guide.* Exposure Draft, August 9, 1995.

U.S. General Services Administration. *Federal Government Business Process Reengineering: Lessons Learned.* KAP-94-2-I, February 1994.

Yoemans, M. "Need Help with BPR? DoD Offers Tools and Experience." *OPM Message to the Senior Executive Service.* SES-95-08, September, 1995. ❑

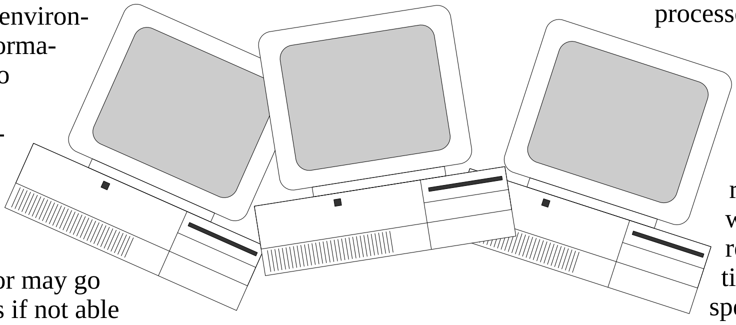
Are Auditors Ready For The Electronic Parade?

by Paul C. Hoshall

"...there is a Computer Revolution going on, and if you don't adapt to the changing climate, you will go the way of the dinosaurs, who became extinct almost overnight as a result of their inability to operate fax machines." (Dave Barry, "Window Shopping," Washington Post Magazine*, August 27, 1995)*

Paul C. Hoshall, Director, Benefits, Information Resources Management and Financial Management, Office of Inspector General, Department of Veterans Affairs

Dave's tongue in cheek statement was in an article aimed at what he termed "technological morons"- "low-tech" individuals who carry out their everyday routines without the use of computers. While his analogy is obviously for humorous effect, the issue of extinction due to the inability to cope with a changing environment is very real. The entire audit community faces a need for significant adaptation as it attempts to operate in an increasingly automated environment. As automated information becomes strategic to decision making, and as more and more information is generated, stored, transmitted, received, acknowledged, and manipulated electronically, the auditor may go the way of the dinosaurs if not able to deal effectively with this rapidly evolving environment.



Auditors' Electronic Evolution Slow

Auditors' electronic evolution has been relatively slow in relation to the fundamental environmental shifts in the way their organizations use automation. Historically, auditors have been effective because activities reviewed involved the two things they were very familiar with--people and paper. No matter what was done with the computer, the auditor still had some credible external evidence to look at, such as manually recorded source documents, and generally some flesh and blood person to talk to who had generated, processed, and/or reviewed, whatever transaction/activity with which they were concerned. Auditors have generally limited their analysis of computer-related controls to those considered necessary to judge the level of data testing needed to determine the reliability of the computer-processed data they relied upon to accomplish their assignment objectives. The exception would be those reviews that specifically focused on the development or operation of a specific computer application system, a data center, or other computer-related activities.

Auditing Standards and Procedures Need Clarification

Government auditing standards and procedures consistently refer to the auditor validating computer-processed data against external source records. Reviews of general and application controls are called for where the reliability of a computer-based system is the primary objective of the audit. System reviews, which concentrate on the working of the system and allow reliance on system controls over time, are called for in cases where a specific set of computer-based data is used for many different assignments during an extended period. Limited reviews, which determine whether certain specific required information has been entered and processed correctly but which do not comprehensively examine system controls, are called for in cases where the system data is not needed for more than a few audits and where the computerized data is not the source record and is substantiated by significant other information. However, the standards do not effectively deal with the situation where the computerized data is the source record, and is not substantiated by significant other information. This "paperless" processing, where source information is generated,

(continued on page 8)

processed, and retained in automated form and there is no alternative to reliance on computer controls and electronic data, will become the norm and not the exception.

In the Very Near Future, Paper And People Will Go Away

They won't actually cease to exist, just cease to exist or significantly decrease in importance as primary control mechanisms in the processing of information. To illustrate this premise, here's a scenario describing a typical transaction that everyone is familiar with--buying an item. A typical procurement process may involve the following activities:

Identification of the need for the item.
Generation of the request for the item.
Review and approval of the request.
Request for quotes from interested suppliers.
Evaluation of quotes and initiation of a purchase order.
Review and approval of the purchase order.
Transmission of the purchase order to the selected supplier.
Agreement by the supplier to the terms of the order.
Shipment of the item by the supplier.
Receipt of item by the purchaser.
Generation of a receiving report.
Invoice for payment by the supplier.
Matching of the purchase order to the receiving report.
Approval for payment and money management.
Payment to the supplier.

In the "paperless" processing environment, this procurement might be accomplished in the following manner. A person identifies a need for an item, and fills in a predefined form on a personal computer or network terminal. The request is passed electronically to the section supervisor, where it is approved electronically. The request is then processed for administrative review (control point official, procurement official, etc.) and approved electronically. Assuming that alternate sources need to be evaluated, an electronic request for quotation is formed and sent out electronically to listings to which suppliers have access. Several suppliers respond to the request electronically and the responses are returned to the evaluation official. The responses are evaluated, a source is selected, and an electronic purchase order is transmitted to the selected supplier. The supplier agrees to the terms of the purchase order and electronically confirms the order, including quantities, prices, and shipping information. The supplier's agreement is sent electronically to the requester and an electronic pending purchase order is posted in the requester's system. The supplier ships the goods, the requester receives them, scans the shipping bar codes and shipper information, and initiates an electronic receiving report. The receiving report is matched automatically with the purchase order, and an appropriate payment is automatically scheduled to avoid interest but maximize use of Government funds. The payment is electronically transmitted to be deposited in the supplier's bank account, and an electronic remittance advice is transmitted to the supplier. From a technology standpoint, how much original source documentation must be generated and maintained outside of the computer? None!

The scenario can be made more automated if the assumption is made that the needed item is ordered automatically from an approved supplier when a particular inventory level is reached, with pre-approved purchase thresholds programmed into the computer that allow purchase requests to flow automatically. The invoice for payment could be eliminated by using the receipt of goods to trigger an automatic payment sequence.

The Audit Trail Will Continue to Change

Obviously, there will still be anecdotal evidence around, and there will still be people to talk to about parts of this particular process. If this were a procurement of a particular non-expendable item, there may be physical evidence of what was received. There may still be external hard-copy, signed and dated pieces of paper that are used for pieces of the process. There may still be specific hard-copy requirements for legal documents, at least until the law generally recognizes electronic documents as appropriate substitutes. Most, and eventually all, of the audit trail related to the actual process will reside in the automated environment, and may very well be scattered throughout multiple computer environments and systems located in many different geographic locations, each of which uses its own proprietary coding, data base, environmental, and management structures.

In some departments, a significant portion of procurements can already be processed electronically. The biggest pending technical issue (with a target date of January 1997) is widespread electronic solicitation and approval of electronic quotations.

This is just one of the myriad of activities that are being profoundly affected by the integration of the computer into all aspects of Government operations. Are there people still involved in this process? Yes, for now. How effective can they be in controlling the process? To a great extent, that will depend on the effectiveness of the electronic controls present in the multiple parts of the process. Can the auditor evaluate these activities without understanding how the process operates, identifying where the control mechanisms are supposed to be, and ensuring that they are operating effectively? No! As this electronic environmental revolution rushes forward, the audit community needs to take a long, hard look at what must be done so that effective audits continue. The top audit concerns must be clearly understood, the major technologies affecting the audit community critically examined, and the bottom line addressed realistically.

Top Audit Concerns

The top audit concerns are not new, but they must be clearly understood and considered on every assignment. They are:

Security.

Physical (fences/locks/guards).

Personal recognition.

Logic (delegations of authority, challenge/response systems, multiple level access controls, electronic signatures, encryption).

Audit Trail Integrity (completeness, accuracy, accountability, generation, protection and retention).

Reliability of Data (completeness--all relevant data elements and records are contained in the universe; authenticity--processed data matches factual information contained in source records; and accuracy of processing--all relevant records are completely processed and the processing meets the intended objectives).

The Top 10 Technology Issues

In 1994, The American Institute of Certified Public Accountants' Information Technology Research Subcommittee and the Practices Subcommittee set out the top 10 technologies that they consider will have a significant effect on business and the accounting profession. All of these will require some change in how the audit community performs its work. Collectively, they will fundamentally change the information that auditors must rely on to complete their evaluations. I have added some of the key issues that need to be considered for each technology.

Electronic Data Interchange (EDI): Automatic, electronic execution of business transactions between two business partners. EDI is rapidly evolving as Government moves toward an open trading environment that will result in many more vendors doing business electronically. Key issues that need to be considered include security, encryption, audit trail integrity, message authentication, and end user controls.

Area Networks: Computers at different locations linked by data communications technology to share computer resources. Many different machines, operating systems, management organizations, and users talking to one another, sharing information, and transacting business. Two commonly identified types are local area and wide area networks. Key issues include security, audit trail integrity, and data reliability.

Cooperative and Client Server Computing: Distribution of processing functions between two or more computers. Again, many different machines, operating systems, management organizations, and users talking to one another, sharing information, and transacting business. Processing and resources are shared among servers involved or distributed between work stations and servers. Key issues include software version control and data reliability.

Image Processing: Converting paper images through scanning. May include identifying blocks of information for document identification, indexing, retrieval, and further processing, such as auditing and matching. Key issues include security, editing, indexing, storage, and processing cycle integrity.

Quick Response: Business strategy that attempts to identify and meet customer demands. May include attempts to reduce the amount of inventory in the merchandise pipeline or maximize efficiency of moving merchandise from raw materials to customers. Key issues include dependency and contingency planning.

Distributed Databases: Logically related data distributed over geographically dispersed locations. Data is typically stored nearest to the point of use, with a network linking databases. Key issues include synchronization, data reliability, and fail-safe/ contingency planning.

Relational Databases: Sets of tables related to each other through the use of keys. Each table stores data about a particular entity, and users interact by means of a query language. Key issues include discretionary access, audit capabilities, privilege management, cooperative systems, and integrity controls.

Communication Technologies: Various technologies are used to enable communications systems to talk to one another, controlling timing, format, routing, and completeness of messages. Key issues include security, dependency, and contingency planning.

Local Area Network (LAN) Interoperability: Interconnection of networks by various technical means, such as bridges, routers, and gateways. This permits LAN users to communicate with users in other offices, buildings, cities, states, and countries. Key issues include security, synchronization, accountability, monitoring, and contingency planning.

Automatic Identification: Method of providing instantaneous knowledge of material flow (e.g., bar coding). Key issues include security, data reliability, and transaction trail integrity.

Fundamental Change from Traditional Audit Evidence

These technologies are key to the evolution to "paperless" processing, where paper documents and handwritten signatures will no longer be either necessary or desired in the normal course of business. They permit and encourage the interconnection of the entire public and private sectors so that it will no longer be necessary to generate a piece of paper to communicate what is wanted, agreed to, and accomplished. There will be a fundamental

(continued on page 10)

change from traditional audit evidence, and the source documentation needed for an auditor’s examination will now be found in both the general processing environment and the programmed application.

Specific Changes in Audit Evidence

The source document may now only be in automated form, and may even be automatically generated inside the computer by the program itself. Origination of a transaction may no longer be a separate activity. Authorization will rely on electronic personal representation, with increased security required, as well as some form of controlling the transaction after authorization. (Processing will be invisible without using the computer, requiring a complete audit trail and proper environmental and programmed controls.) Output will be mostly in electronic format, either displayed or transmitted, and error handling will depend on proper system messages, pending files, and clearance mechanisms. Auditors will have to ensure proper retention of electronic media, such as master files, transaction files, system files, exception files, and communication logs. Segregation of duties will be enforced internally. In many cases, manuals and instructions will be in electronic format, including on-line help, automated libraries, e-mail instructions, programmed code, and systems procedures. The electronic information trail will contain the only verifiable source of the who (electronic identification), what (transaction content), when (time stamps, system/software logs) and where (terminal identifications, communications sessions) that have for so long been verifiable elsewhere.

The Bottom Line

In an article on radical reengineering for internal audit, published in the Volume III, 1995 issue of the *Journal of the Information Systems Audit & Control Association,* Ross Wescott of the Portland General Electric Company discussed three reasons to consider radical change in the audit department—to save audit jobs, increase audit value, and bring greater demand for audit services. Among the other points made in his article, Mr. Wescott stated that, “Access without proficiency is like having a key to a door with no visible lock; entry is impossible. Whether you are using computer-assisted audit techniques, specialized audit software, mainframe, workgroup, or local area networks, each member of the audit staff should have access to and be proficient in some aspect of its use....Training without application is shallow. Access without training is frustrating. An application without access or training collects dust.”

To continue to be effective, the entire audit community must become electronically competent. The electronic environment will soon be integrated into all aspects of organizations being reviewed. Auditors will no longer be able to view activities, information or controls separate from the computer environment, nor rely on the “people and paper” method of auditing. To participate, the audit community must have adequate trained resources to apply to this significantly different environment. There are three choices: hire for it, train for it, or contract for it.

Forward march! ❑

Casting The Net: Reinventing The Hotline – Using The Power Of The Internet

by Ralph McNamara and Jerry Lawson

Ralph McNamara,
Assistant Inspector General
for Investigations, National Archives
and Records Administration

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

Once exotic, Internet e-mail is becoming mainstream. Millions of users of systems such as America Online, Prodigy, CompuServe and now the Microsoft Network access the Internet. Many Government agencies provide their employees with access to Internet e-mail. As the number of people with the ability to use the Internet continues to increase, so does the attractiveness of using an e-mail hotline to supplement the conventional telephone hotline.

The concept of e-mail hotlines offers Offices of Inspector General (OIG) a new set of possibilities and challenges not present with conventional telephone hotlines. The possibilities are exciting to those familiar with the technology and the fundamental principles of hotline operation. The challenges strike at the heart of some of the basic tenets of any hotline operation.

An e-mail hotline offers the following advantages:

- Provides a means for reporting allegations that is more attractive to some prospective complainants.
- Allows complainants to reach the hotline anytime and get some immediate feedback.
- Records information received automatically and accurately.
- As more and more Government information becomes computerized, an e-mail hotline makes it easier in many cases for complainants to submit detailed information in support of their allegations, in the form of an e-mail "attachment."
- Can make it easier for complainants to remain anonymous and, in some cases, makes it more likely that OIG personnel will be able to maintain a continuing dialogue with a complainant.
- Makes communicating with the hotline significantly easier and cheaper for complainants in geographically dispersed organizations.
- Inexpensive and easy to set up.
- Not labor intensive to operate.

Some people prefer to deal directly with a human bank teller, while others prefer dealing with an automated teller machine. E-mail hotlines are likely to be more effective than telephone hotlines with the latter personality type.

Sophisticated e-mail software (Novell Groupwise, for example) can be programmed to send a standard reply immediately to any messages received. While it is not very personal, this gives complainants almost instant feedback. At a minimum this could be a confirmation that the message has been received and an assurance that it will be evaluated as soon as possible.

Practical Experience with the E-mail Hotline

E-mail hotlines are not totally new in the OIG community. The Department of Defense (DOD) is a leader in using this new technology. The DOD e-mail hotline was begun in 1995, opening a new method of reporting fraud, waste, abuse, and mismanagement to a vast number of customers via the Internet.

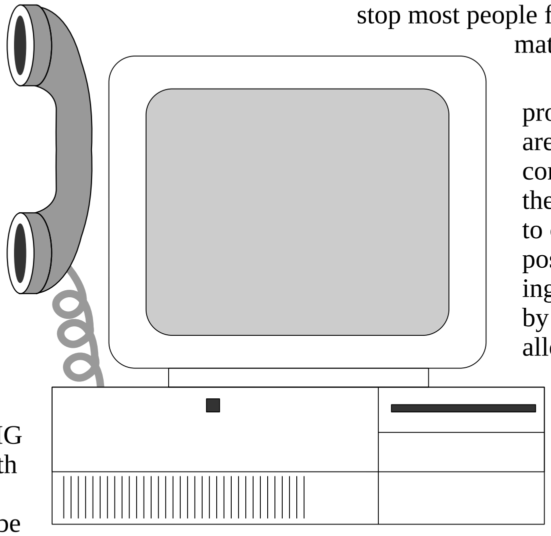
The project was the offshoot of a Congressional request for information about the use of e-mail for reporting allegations to hotlines. Prospective complainants with access to e-mail can now report suspected agency problems directly from their home computers to the largest fraud, waste, abuse, and mismanagement hotline in the world. The Defense Hotline, through the DOD OIG, opened the gate to the Internet and entered the new world of the cyberspace hotline.

(continued on page 12)

Charles St. Cyr, Acting Director, Defense Hotline, reports that as of September 1995, the hotline received approximately 36 complaints via the e-mail hotline—approximately one per week since it started in January 1995. While this would be a bumper crop in some agencies, Mr. St. Cyr considers this to be a low number relative to the size of DOD, where over 15,000 hotline contacts occur annually. He believes more publicity might serve to promote the cyberspace hotline.

In fact, no hotline will work unless you get the word out to your target audience. The Defense Hotline puts its Internet address on confirmation letters back to complainants who have submitted allegations. However, to maximize the effectiveness of an e-mail hotline, the Internet address should also be placed on hotline posters, pamphlets, and any other medium that promotes the hotline's toll-free telephone number.

E-mail hotlines are not unique to the public sector. One investigative consulting firm, Decision Strategies International, offers its corporate customers a service it calls TipNet. The company's newsletter states: "The TipNet service is set up to receive anonymous e-mail as well as encrypted e-mail using Pretty Good Privacy (PGP) public key encryption software. These features, coupled with Decision Strategies' ability to have two-way written communication with tipsters, reduce the need for operators to transcribe telephone conversations or recordings."



The National Archives and Records Administration (NARA) OIG has established an e-mail hotline with the option for anonymity, but not encryption as of this writing. It can be accessed through the following Uniform Resource Locator (URL): http://www.nara.gov/ig/hotline.html.

Perceived E-mail hotline disadvantages include:

- Unreliability—message might be delivered to the wrong address.
- Regular Internet e-mail is not secure—message could be intercepted.
- With regular Internet e-mail, the complainant loses confidentiality.

Two of these perceived disadvantages are based largely on inaccurate impressions, while modern technology offers us the opportunity to transform the third perceived disadvantage into a major advantage.

The fear of unreliable delivery is largely based on an incorrect perception. It is not unusual for Internet e-mail to fail to be delivered as intended, for any number of reasons, but when this happens, ordinarily the system responds in one of two ways: it "bounces" the e-mail back to the sender, or it forwards the undeliverable mail to a person who has been designated the e-mail "Postmaster" at the domain of the intended recipient.

The former situation is annoying but it is not a problem for confidentiality purposes. The second situation is rare. Statistics on undelivered e-mail are hard to come by, but in the book, *Mastering the Internet*, by Glee Harrah Cady and Pat McGregor (Sybex, 1995), Ms. McGregor estimates that in her experience as Postmaster at the University of Michigan, only about 0.25% of the e-mail traffic had problems that caused it to be routed to the Postmaster. It is much more likely that your fax will wind up being delivered to the wrong recipient than your e-mail.

In the authors' view, the fear of lack of security of Internet e-mail is often exaggerated. Certainly, systems administrators who are so inclined can access e-mail traveling through their systems. Furthermore, those with the necessary access, equipment, and technical knowledge can intercept Internet e-mail in transit. However, conventional phones can also be tapped. This possibility does not stop most people from freely discussing fairly sensitive matters over the telephone.

It is necessary to put the security problem into perspective. Certainly, there are some situations when it is unwise to communicate by unsecured e-mail, just as there are some situations when it is unwise to communicate by telephone, fax, or even postal mail. However, if you are encouraging complainants to communicate with you by telephone, there is little point in not allowing the use of e-mail as well. If you need a high level of secured communication on your e-mail hotline, you can make it extremely secure by using public key encryption. (See box on page 13.)

The problem of loss of confidentiality can easily be solved by using modern technology. In fact, improved confidentiality is one of the biggest advantages that a properly managed e-mail hotline has over its conventional voice counterparts.

Maintaining confidentiality is a top priority with many hotline callers. Often, their fear of being identified leads them to restrict their contacts, to the great disadvantage of auditors and investigators trying to follow up on the information they provided. Some agencies try to assuage such fears by assigning Deep Throat style code names, but this is clumsy and of doubtful effectiveness. Even worse, it does not allow the auditor or investigator to contact the informant to ask follow up questions.

These problems can be solved by using anonymous "remailers." These are third parties that voluntarily serve as intermediaries for people who wish to keep their identities private. To use one of these services, you format your e-mail as specified, and mail it to the remailer. The remailer's computer assigns a unique pseudonym to the

(continued on page 14)

An Encryption Primer for OIG Personnel

There are many ways of encoding, or encrypting e-mail so that it will be secure in transit. Both hardware and software methods are in use. The most exciting development in this field in recent years has been the introduction of public key encryption (sometimes referred to as RSA encryption, after the initials of Ron Rivest, Adi Shamir, and Len Adleman, the three Massachusetts Institute of Technology professors who developed and patented the technique).

With conventional encryption it is necessary to secretly distribute a password to anyone who wants to send or receive an encrypted message. Secure password distribution can be difficult in some situations.

Public key encryption is more flexible and powerful because it does not use a conventional password. Instead, the user's software creates two lengthy keys. These appear to be random collections of letters and numbers. One principle is at the heart of the system: a message encoded with either of the keys can only be decoded with the other.

One of the keys is designated the public key, the other the private key. The private key is kept secret. The public key may be distributed openly and widely. If anyone wants to send you a private message, he or she does not need to share a password with you—he or she merely encodes the message using your public key. Only you can decode it, because only you have the matching private key.

Besides easier key management, public key encryption offers another major advantage: the digital signature. Remember, either of the two keys can be used to decode a message encoded by the other. Therefore, if you want someone to be able to verify that a message came from you, and only from you, you can encode it with your private key. Then, anyone can verify that it is authentic, because your public key--and only your public key--can decode it.

By far the most popular public key encryption program today is a package called Pretty Good Privacy, or PGP, put together by Phil Zimmerman. The owners of the underlying patents have consented to make the package available free for personal noncommercial use. You can obtain a list of places to obtain the software (in a file named getpgp.asc) from the following ftp sites: ftp.csn.net/mpj or ftp.netcom.com/pub/mpj. There are programs that work with the DOS version of PGP to make it easier to use: WinFront is free and WinPGP is shareware ($45). For commercial (including Government use), the only licensed PGP distributor is Viacrypt, e-mail to viacrypt@acm.org, or (602) 944-0773. There are versions for many operating systems.

How secure is PGP? This depends on the length of the key that you select. Even short keys are very difficult to break. It is generally believed that moderate length keys will strain the resources of even the renowned National Security Agency. Long keys are believed to be secure from any technology that will be available in the next few decades.

PGP and other powerful encryption programs are controversial. Some people believe that the Government should be able to decipher all communications, so strong encryption programs should be outlawed. These people support a system with a built in “backdoor,” like the much-debated “Clipper Chip” (which the Government appears to be abandoning). However, while it is illegal to export strong encryption programs outside the country (they are classified as “munitions” under a World War II vintage law), it is perfectly legal to use them in this country. If your organization has auditors or investigators overseas, they can take PGP abroad if they obtain an export license from the Department of State. The Defense Hotline has just started using e-mail to send case referrals to field elements for inquiry using encryption. More case referrals to field elements are planned and, in the future, case completion reports (inquiry findings) will be returned to the Defense Hotline via the Internet.

If your organization ever needs to transmit highly sensitive information, public key encryption is an option worth considering. Used properly, it is an easy and inexpensive way of making your e-mail communications much more secure than using conventional telephones, postal mail or even private couriers.

Even if your agency does not adopt the use of public key encryption on its hotline, OIG personnel should have a general understanding of the concept, for two reasons. First, the increasing popularity of public key encryption with the public makes it likely that OIG auditors and investigators will come across it during the course of their work. Second, public key encryption can be a valuable administrative tool inside OIGs. It allows, for example, sending highly sensitive electronic referrals to field offices for inquiry and receiving sensitive progress/final reports via the Internet. Information sent in this manner can be transmitted more securely than by any other method of communication commonly used in the business world today. ❑

sender, then strips the sender's address from the message and forwards it to the intended recipient. The recipient knows that the message came through the anonymous remailer, but has no way of knowing the original sender.

This procedure obviously has benefits for both hotline complainants and hotline operators. The complainant can be very confident of maintaining confidentiality. The hotline operator benefits by receiving more complaints. However, the biggest benefit for the hotline operator is easy two-way communication with a complainant who wishes to remain anonymous. If the complainant originally used a remailer that supports replies, and not all do, the hotline operator can send a reply back to the anonymous remailer, using the unique pseudonym. The remailer's computer forwards the reply to the complainant, who retains confidentiality.

Suggestions for Successful E-mail Hotline Operation

- Publicize the e-mail hotline address adequately. To supplement the methods suggested above, consider the use of a site on the Internet's World Wide Web. This method is a particularly effective way to publicize an e-mail hotline, since the people who can reach your Web site are almost certain to have access to e-mail and to be comfortable using it. In the advertising industry, they would be called "qualified prospects." At a Web site, you can even include "hotlinks" to give the users instant "point and click" access to information about remailer sites, or even the remailer sites themselves. Several OIGs, including the Departments of Justice, Housing and Urban Development, and Education and the National Aeronautics and Space Administration have established such sites.
- Provide prospective complainants with information about anonymous remailers. In all promotional material where you mention your e-mail hotline, include an explanation of how users can get further information on anonymous remailers.
- Set up the account's e-mail address in the form hotline@agency.gov, not sam.smith@agency.gov. Your agency systems operator or Internet service provider should easily be able to set up an "alias," so that mail to the hotline@agency.gov address will be routed to a designated person.
- Consider opening an e-mail account with a commercial Internet service provider, instead of going through your agency's local area network. This should provide a small extra measure of security, as system operators and others frequently have access to e-mail being delivered within the agency. In the Washington, DC area, you can open an account with full Internet access, including e-mail, for $15 to $30 a month. Many Internet service providers advertise in the business section of local newspapers.

Anonymous Remailers

It is normally easy for the recipient of an e-mail message to identify the sender's account, and usually the sender. This information is contained in the header of the e-mail message. Third-party anonymous remailers provide a way of sending e-mail yet maintaining your privacy.

They work like this: you send your message, along with the address of the intended recipient, to a "remailer program." This automatically strips your name and address, and assigns you a random pseudonym. It then remails your message to the intended recipient. All the recipient knows is that the message came from an anonymous remailer. He or she does not know from whom or where it originated.

Some remailers allow the recipient of such a message to respond. These remailers maintain a secret, automated database of real sender names and code names. One of the most popular remailers, located in Finland, runs on a computer named anon.penet.fi. Their code names are always the letters an, followed by a number, so if you used this system, your coded e-mail address would be something like an93471@anon.penet.fi. The anonymous remailer would forward any mail sent to that coded address to you.

Anonymous remailers are often not very stable, probably because they are not commercial operations. For more information about remailers, you can send e-mail to:

help@anon.penet.fi
or remailer@soda.csa.berkeley.edu

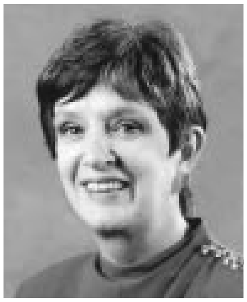
For the Berkeley addresses, use the phrase remailer-info in the subject line. "Robots" at each address answer automatically.

Conclusion

The use of Internet e-mail hotlines to supplement conventional voice hotlines opens a promising new avenue for receiving high quality, useful information. In some ways, the e-mail hotline is superior to the voice hotline. As with a conventional voice hotline, professional operation and effective publicity are the keys to success for an e-mail hotline. ❑

Paperless Processing At SSA

by Mary Ann Dufresne



Mary Ann Dufresne,
Project Coordinator,
Office of Strategic Management,
Social Security Administration

The Social Security Administration (SSA) is an organization strongly committed to "world class" service for the American public. Under the leadership of Commissioner Shirley Chater, "good enough for Government work" means nothing but the best for our customers.

Like all Federal agencies, SSA is faced with the mandates of downsizing and streamlining and an overall austere budget climate. That is making it difficult to fund service improvements and is challenging Agency officials to find breakthrough strategies to achieve service goals and cut costs. These factors were key to the 1992 SSA decision which defined paperless processing as one of the Agency's five strategic priorities. SSA is also a pioneer in reengineering, with a sweeping redesign of our most resource intensive claims process, the disability process, well underway. Many of the service improvements and resource savings in the Disability Redesign are based on the claim being handled in a paperless environment.

The Business Arguments for Paperless

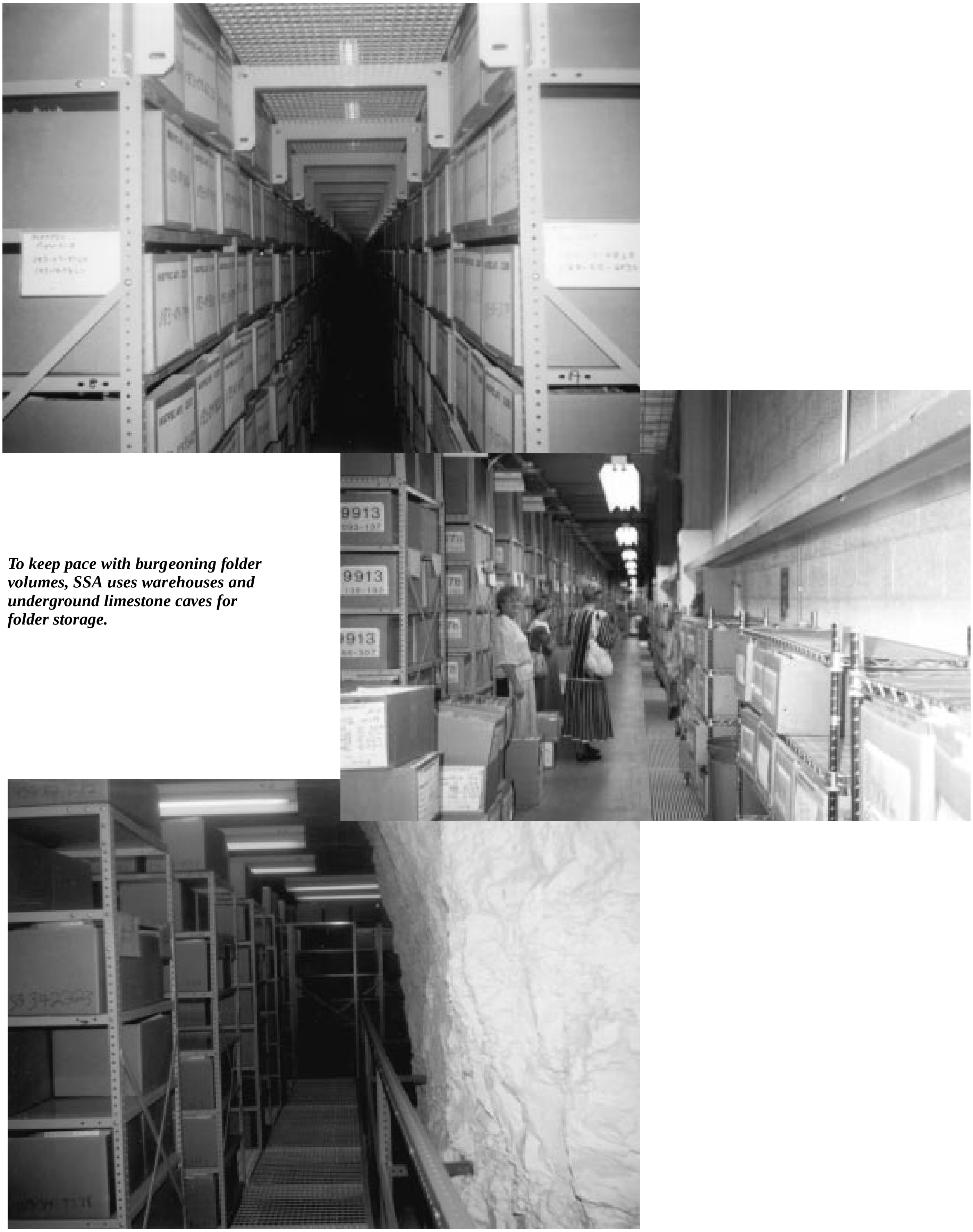
Janice Warden, SSA's Deputy Commissioner for Operations, is one of the leaders in the Agency's drive to become paperless. Ms. Warden manages the 50,000 employees who deliver direct service to the public. She also foots the bill for paper handling and storage. Some of the paper-related problems that she faces are:

- Paper files cannot move quickly through multi-step business processes. Transportation and queuing points inevitably delay completion of service transactions.
- Sixty million people call SSA's 800 number every year. They want information on the spot about their records, and they want immediate action on their Social Security problems. That requires that the caller's record be available on-line, not in a paper file stored at a remote location.
- Customers are telling SSA they want to do business without traveling to a local Social Security office. The typical customer wants telephone service, but many want Internet, kiosk, and other types of remote service--even for sensitive transactions like claims applications and access to confidential information. Signature requirements must be resolved before SSA can deliver what these customers want.
- In 1992, SSA had 80 million paper claims folders stored in prime office space, warehouses, underground caves, and Federal Records Centers. Storage facilities were overflowing. Despite significant attention to management of folders, the sheer volume caused a logistical nightmare, and finding a given file was not a trivial challenge. Worse, demographic forecasts suggested that folder volume would double in 5 years.
- Costs relating to paper handling keep rising. Folder storage costs are just the tip of the iceberg, accounting for only 10 percent of SSA's annual tab of $300 million for paper-related costs. The real expenses are in handling--packaging, mailing, and filing--to which literally thousands of SSA workyears are dedicated.

Ms. Warden wants to move aggressively to becoming a paperless agency. She says: "My dream is to have all this paper-based information available electronically and to reprogram that $300 million to direct service for our customers."

While all components at SSA are excited about paperless, the Office of Inspector General (OIG) staff are also keenly aware of the risks. Olive Franklin, Acting Assistant Inspector General for Investigations, says: "We are very positive about paperless. But we need to recognize that paper records act as a deterrent against fraud. It will be harder to win fraud cases in Court without verifiable conflicting statements that are found on paper records. As we move into highly sensitive areas, like signatures on application forms, we need to incorporate legally sufficient safeguards. OIG staff look forward to helping SSA operating components develop a paperless strategy that deters fraud, preserves fraud cases for investigators, and works for frontline service staff."

(continued on page 16)



To keep pace with burgeoning folder volumes, SSA uses warehouses and underground limestone caves for folder storage.

The Paperless Strategy

The paperless initiative is an "all-hands" effort for the Agency. As first steps, a 1992 task force representing all SSA interests studied paper-related problems and costs, pinpointed targets of opportunity and defined a comprehensive program that would eliminate paper recordkeeping over a 10-year period. The strategy provided for some quick fixes, some intermediate-range policy initiatives and a number of technology changes that could be phased in gradually over the 10-year planning horizon. SSA line components then took the lead for specific projects, and paperless success became everyone's business.

Early Wins

SSA has achieved a lot since the paperless strategy was formulated in 1992. Here are the major success stories so far.

The Discard Project: Janice Warden led an effort to improve the training and procedures that tell SSA operating staff what can be discarded under current policy. Staff were asked to apply the new guidance and to discard superfluous paper documents as they processed each transaction. During a 3-month study period, staff discarded enough paper to create a stack reaching from the base to the top of the Grand Canyon. The effort was so successful that black plastic recycling bags are now standard issue for SSA operating staff.

Social Security Number (SSN) Applications: In the past, SSA retained paper SSN applications even though the data from these forms are recorded to electronic files and the documents themselves are microfilmed for processing. Paper was retained to ensure that SSA could successfully prosecute in this fraud-prone area. In an outstanding example of cooperation between the OIG and operating components, the OIG was able to profile likely fraud situations. Accordingly, SSA changed retention policies and now discards all but 30,000 of the 18 million SSN applications filed every year.

On-line Claims Process: Every year SSA takes over 3 million claims for retirement or survivors' benefits. In 1992, the average claims file contained 16 pages of paper documents. Today, the average file contains only a 2-page signed application. Supporting documents (like birth and death certificates) are excerpted and recorded electronically. The next challenge: Electronic signatures!

Seven-Year Retention Rule: Historically, SSA had retained paper claims documents for the lifetime of the beneficiary's entitlement, plus another 5 years. Typically, that meant a 20-plus year retention. Analysis conducted under the auspices of the paperless initiative showed that the paper was referenced very infrequently and almost exclusively for fraud investigation. SSA's General Counsel, OIG and program components jointly agreed that everyone's needs could be met by keeping documentation for only 7 years. SSA is now in the process of destroying tens of millions of paper folders over 7 years old.

Annual Wage Reporting: SSA's Earnings Modernization Project, which supports establishing and maintaining records of workers' earnings, was implemented in 1995. In the new process, the 250 million reports received annually from employers that report earnings are imaged upon receipt and processed electronically. The paperless process is so efficient that SSA now needs only one of the three large data operations centers that were dedicated to annual wage reporting in the past. The other two centers have been "re-missioned" and are now answering 800 number calls, contributing directly to world class customer service.

As the project managers, it is clear to us that the biggest accomplishment has been a history-making cultural shift. In 1992, most people said, "We'll never be paperless; there are too many obstacles." Now the conversation around paperless is about when and how.

More Technology in the Offing

The next few years will likely ring in even more significant technological changes. Here are the highlights:

Imaging: In one module of the Chicago processing center, SSA is piloting use of imaging technology. In that module, all incoming paper is imaged at the point of receipt, then processed and filed electronically. If the pilot is successful, it has the potential to eliminate all paper recordkeeping for SSA's retirement and survivors' claims process. So far, the pilot looks promising. Productivity and processing time have been improving for several months, and clerical work is drying up. The big question to be answered in the pilot: Will productivity improvements be enough to justify national implementation of this costly technology? SSA expects to have answers in 1996.

National Infrastructure: As a foundation for future technological change, SSA is now in the process of replacing an aged network of 60,000 "dumb" terminals with "intelligent" workstations and local area networks. The schedule calls for an award this year and national rollout over the next 2 years. This basic infrastructure will be a critical enabler for imaging, for the fully automated disability process now under development and for other improvements targeting paper.

Direct Access: Responding to public demands for a wide range of choices for doing business, SSA has an aggressive Electronic Service Delivery initiative underway and will be a pioneer in the use of Internet and kiosk. In a pilot planned for 1996, the showcase application will give customers remote access to their personal earnings histories and projected Social Security benefits. Another application will give companies a convenient on-line facility for Certificates of Coverage which exempt overseas employees in 17 countries from foreign Social Security taxes. SSA hopes not only to please customers but to cut into the resources now being expended to respond to tens of thousands of such requests received annually on paper.

(continued on page 18)

The author demonstrates a paperless success story: SSA operating instructions used to fill several bookcases. Now they are stored on a single CD-ROM disk accessible on-line.

Certificates of Coverage save American corporations $400 million annually.

Moving into these risky new environments clearly calls for safeguards, and SSA plans to provide them. Joan Hash, SSA's Systems Security Officer, puts things in perspective: "In a paperless environment, public key cryptography provides for very strong controls supporting data integrity and nonrepudiation. It also provides for a signature that is highly verifiable. Use of imaging will also be very important for retaining historical information to effectively support analysis of potential fraud or abuse situations. This, coupled with the ability to query a variety of on-line databases for security and integrity purposes, will go a long way in providing for a sound security infrastructure without the use of paper."

Big Challenges Ahead

Some of our most difficult work is just getting started. The major remaining barriers to paperless processing are medical evidence of disability (which accounts for over half of residual paper records) and signature documentation. The special sensitivity of these records adds to the automation challenge.

The vision for medical evidence sees SSA drawing upon the electronic records maintained by the medical community as it moves into the automation world. SSA is already receiving evidence electronically from a few providers on a pilot basis. Confidentiality safeguards, including public/private key encryption, are an important dimension of the pilot. Discussions with the Veterans Benefits Administration around sharing medical records with SSA electronically are very promising and could pave the way for significant paper elimination and improved disability service over the next few years. Projections are that electronic medical recordkeeping will be routine--albeit not universal--by the year 2000, and SSA is positioning itself to take advantage of developments as they occur.

Last but certainly not least, SSA is turning its attention to signature documentation. Selecting technologies and controls to make electronic signatures safe will require careful risk and cost/benefit analysis as well as creative partnering between investigators, attorneys, security staff, and operating components. Many fear that the legal community will not keep pace with technology. SSA's General Counsel, Arthur Fried, is much more optimistic. Fried says: "In 1851 the Supreme Court approved replacement of a wax seal to authenticate a document with use of an impression of the seal directly on paper. (Pillow v. Roberts, 54 U.S. 472.) Someday soon, use of handwritten signatures on paper will seem just as quaint as the wax seal does today."

The Future of Paperless

While there is much to be done, SSA continues to be enthusiastic and confident about what can be accomplished with the kind of teamwork that has been the hallmark of the paperless initiative so far. Our invitation to you: Come see us in 5 years! ❑

Let Me Task Your Wares: Acquisition Reform

by Joseph E. Vengrin

Joseph E. Vengrin,
Assistant Inspector General
for Audit Services, Audit Policy
Oversight, Department of Health
and Human Services

To better meet the needs of its audit customers, the Department of Health and Human Services (HHS) Office of Inspector General (OIG), in conjunction with the Department's Assistant Secretary for Management and Budget (ASMB), reinvented its procurement methods for acquiring the services of independent auditors. These two offices developed a convenient, cost-effective, and innovative fixed-price task order mechanism that helps ensure the audit needs of HHS agencies are met timely and efficiently in instances where OIG resources are not available.

This new procurement mechanism not only instills marketplace competition into the procurement process, but also streamlines the process itself, thus ensuring more timely audits. The OIG still ensures that contracted audits are performed in accordance with Government auditing standards.

New Method of Procuring Audit Services Can Result in More Cost Efficient and Timely Audits

The OIG does not have the necessary resources to meet all of the audit needs of its customers. This is not a new phenomenon, it is something that the OIG has dealt with for several years. If OIG resources were not available, the OIG would use funds to contract with independent audit firms. Inevitably, some audits had to be postponed due to lack of staff or contract funds. In addition, audits that were performed under contract may not have been the most cost efficient due to lack of marketplace competition in the procurement process.

Clearly, there was an opportunity to more effectively acquire the services of independent audit firms, an opportunity that was recognized by ASMB and OIG. For instance, multiple HHS agencies were not only processing duplicative contracts for audit services but the process itself was cumbersome, typically taking about 6 months to complete.

With the enactment of the Federal Acquisition Streamlining Act of 1994 (FASA), many of the complexities of the procurement process were eliminated. The FASA authorized the expanded use of "task order contracts." These innovative devices allow for the award of one overall competitive contract to provide a line of credit with a maximum ceiling to purchase services through performance devices called task orders. Each order must be within the scope, period, and maximum dollar value of the contract, and should clearly describe all services to be performed.

Types of audit services that may be requested under this task order arrangement runs the gamut, from financially-related audits to review of computer system controls--in other words, any audit that lends itself to a standard audit guide and has a definable audit scope (and thus a readily "estimable" audit cost). Audit support services may include financial statement audits; pre-award contract proposal reviews; accounting system surveys; financial capability reviews; financial management system reviews; cost-incurred contract audits; audits of grants; internal control reviews; audits of computer-based and financial systems; internal accounting and computer security control reviews; indirect cost reviews; and Medicare Administrative Cost Audits; etc.

When we first began using the task order process, contractors were selected within a specific geographical area. This turned out to be a problem since only the selected independent audit firm responsible for that geographic area could bid, thus ruling out the benefits of marketplace competition.

The system developed jointly by the OIG and ASMB drastically improves the procurement process by instilling much needed marketplace competition. Using full and open competition, the ASMB awarded a task order contract to 14 audit firms that the OIG has evaluated as technically qualified. Each of the 14 firms is now permitted to compete for individual task orders regardless of the geographical area in which the audit is to be conducted, a sharp contrast to the one task order-one bid method that was previously in effect. In general, awards will be made to the lowest bidder, thus ensuring the most cost efficient audit.

Because of the competition that now exists for each task order, cost savings are anticipated. Equally important,

(continued on page 20)

however, is that audit timeliness and quality will not suffer. In fact, the timeliness of audits is expected to improve under the new mechanism.

Responsibilities of the HHS and the OIG

When audit resources are not available to meet a specific audit need of a HHS agency, the agency requesting the audit can opt to have the audit conducted under contract. In this case, the requesting agency (in consultation with the OIG) is responsible for preparing the statement of work, which, in addition to describing the purpose and scope of the audit, includes the dollar value of the project or contract to be audited; the task order period of performance; the location of records to be reviewed; a description of its key reasons for requesting the audit (i.e., the nature of its concerns); an estimate of the level-of-effort required to conduct the audit; and a reference to any prior, related audit reports. Also, the HHS agency will, of course, furnish the name, address and phone number of its task monitor; the name and address of its own paying office; and its own appropriation data.

The OIG is responsible for approving the statement of work and forwarding it to ASMB's contracting office for the development and award of a task order. Any questions on the completion of the statement of work are directed to the OIG. The OIG is also responsible for absorbing the cost relating to: (1) administration of the task order contracts; (2) the technical assistance it provides HHS on audit strategies; and (3) its oversight of contractor performance, including reviews to ensure that the audit report is a professional, quality product that meets Government auditing standards. To ensure that the requested audit services are of high quality, the OIG not only reviews the work performed but, together with ASMB, conducts a customer satisfaction survey to evaluate contractor performance.

Both the HHS agency requesting the audit services and a local OIG representative serve as the task monitor for the particular task order. In coordination with the overall OIG project officer, they keep track of contractor performance from a technical standpoint to ensure that the audit meets customer needs. Any changes to the task order (e.g., work falling outside the general purview of the task order work statement) need to be authorized by ASMB's contracting office after consulting with the OIG project officer.

Conclusion

When OIG resources are not available, this new mechanism for purchasing audit services, first and foremost, is a step towards meeting the audit needs of all HHS timely and efficiently. The HHS agencies now have the flexibility to choose between a postponement of the audit until OIG resources become available or contracting with an independent audit firm. The HHS agencies are assured that: (1) the cost of the contracted audit will be reasonable due to marketplace competition; and (2) the audit will be in compliance with Government auditing standards due to OIG oversight.

The use of these competitively-priced, high-quality, nonfederal auditors complements the Department's OIG auditors, HHS agency cost advisory officials, and internal management-related analysts--exemplifying the kind of synergy and teamwork that helps HHS and the OIG to meet their program and mission goals. ❏

Operation Safe Home

by Susan Gaffney

by Susan Gaffney,
Inspector General, Department of Housing and Urban Development

On February 4, 1994, Vice President Al Gore, Attorney General Janet Reno, Secretary of Housing and Urban Development Henry Cisneros, former Treasury Secretary Lloyd Bentsen, and former National Drug Control Policy Director Lee Brown announced "Operation Safe Home" (OSH) in a joint press conference at The White House.

The announcement resulted from a question posed months earlier by Secretary Cisneros. Secretary Cisneros asked the Department of Housing and Urban Development (HUD) Inspector General, Susan Gaffney, whether the HUD Office of Inspector General (OIG) could take a more proactive stance in identifying and combatting major types of crime that were undermining HUD programs. The OIG senior staff had no difficulty identifying three major types of crime affecting HUD programs:

- violent crime in public and assisted housing;
- fraud in the administration of public housing; and
- illegal diversion of revenues (also known as equity skimming) from multifamily insured projects.

The more difficult question was: how could the OIG, with its very limited resources, make a substantial contribution toward reducing the incidence of these crimes? Three OIG task forces, comprised of field and headquarters staff, were convened to consider the question. Their answers were remarkably similar: the OIG had to be willing to (1) engage in new kinds of work; (2) leverage our resources by focusing other law enforcement agencies, as well as HUD and HUD partners, on these crimes; (3) enhance our deterrent effect by publicizing our enforcement successes; and (4) make a real and substantial long-term commitment to the effort.

Based on these concepts, the task forces drew up plans in each of the three areas and suggested to the Secretary that the overall effort be labeled Operation Safe Home. The label was important: the OIG wanted to be sure that we never lost sight of our real objective, which is decent, safe, and sanitary housing for HUD beneficiaries.

In the 2 years since its announcement, Operation Safe Home has led the HUD OIG down some unconventional paths. While we have had notable successes, the mission remains daunting. The one clear lesson we have learned is that the HUD OIG occupies a very special niche between the law enforcement and the HUD program communities; and we can and should use this niche to the benefit of all.

Violent Crime In Public and Assisted Housing

Despite the fact that HUD spends almost $20 billion a year for public and assisted housing, much of this housing has become a major locus of violent crime--with law-abiding residents, many of them elderly, terrorized by drug and gang activity. OIG audit work over the years had shown that the rising tide of violence could be attributed, in part, to poor communication/cooperation between housing authorities and local law enforcement, inadequate emphasis on crime prevention (as opposed to law enforcement), and fragmented Federal, State, and local law enforcement efforts.

Accordingly, the OSH initiative was structured to combat the level of violent crime within public and assisted housing, and enhance the quality of life within such complexes via three simultaneous approaches:

- collaborative law enforcement efforts focused on reducing the level of violent crime activities occurring within public and assisted housing;
- collaboration between law enforcement agencies and public housing managers and residents in devising methods to prevent violent crime; and
- HUD programmatic initiatives specifically geared to preventing crime.

Immediately after the announcement of OSH, OIG Special Agents in Charge (SACs) briefed the U.S. Attorneys on the OSH effort. The U.S. Attorneys were solicited for their assistance and support in developing anti-crime initiatives at selected public and assisted housing sites within their districts.

U.S. Attorneys were simultaneously instructed by Attorney General Reno to develop operational plans for reducing violent crime in their districts. These instructions included U.S. Attorney-led "law enforcement coordinating

(continued on page 22)

committees" (LECCs) composed of representatives of all major Federal, State and local law enforcement agencies within their jurisdictions. The HUD OIG was included in the composition of the LECCs. This provided the OIG with an opportunity to solicit broad support from other law enforcement agencies via the re-focusing of some existing anti-crime initiatives into those areas containing public and assisted housing sites.

In addition, OIG SACs sought out their counterparts at the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco and Firearms (ATF), U.S. Secret Service (USSS) and other Federal, State and local law enforcement agencies to discuss mutual concerns about drug and violent crime activities within public and assisted housing locations throughout their districts. These efforts were designed to encourage these agencies to consider adjusting the focus of some of their ongoing investigative efforts into the more crime-ridden public and assisted housing sites, and to initiate law enforcement operations specifically targeted within such locations.

Simultaneously, the OIG started working with HUD managers to define program initiatives that would support Operation Safe Home.

As a result of this outreach, over the past 2 years the OIG has become a participant in over 100 law enforcement task forces; assumed significant responsibility for relocating witnesses of violent crime; sponsored a dialogue among police chiefs, the Department of Justice, and HUD program managers; and developed an anti-crime legislative proposal.

Law Enforcement Task Forces

OIG participation in law enforcement task forces has been a significant departure from the traditional role of OIG Special Agents in investigating white-collar crime. It has required that OIG Special Agents enhance their previous law enforcement training with additional skills in tactical operations, as well as the uses and handling of confidential sources in covert investigations. OIG Special Agents are now routinely assigned as full participants to DEA, ATF, FBI-led task forces. They also participate in a number of State/local police operations that are designed as short-term initiatives highly focused within publicly funded residential complexes.

Since the inception of OSH, OIG Special Agents have participated in over 100 task force initiatives that have been either focused exclusively in publicly funded housing, or have been expanded from their original scope to include publicly funded housing. Some Federal task forces of national scope, such as the FBI's "Safe Streets" and ATF's "Project Uptown", now include components that have dedicated agents addressing gang, drug and gun crimes within public housing locations.

OIG agents have directly participated in law enforcement operations executing the service of over 700 search warrants, and they have participated in making over 6,800 arrests in and around public and assisted housing sites. In the course of these operations, they have become involved in joint seizures of drugs valued at almost $3 million, over $1 million in cash and over 550 weapons, including 49 assault rifles and 56 shotguns.

More importantly, in specific areas, the task forces on which OIG agents worked have succeeded in removing entire gangs that terrorized residents, thereby reducing the violence and allowing housing authorities to reclaim the units and returning to residents a sense of community. There is a general consensus among law enforcement agencies as to the long-term futility of enforcement operations in permanently reducing the level of drug and violent crime activities in targeted locations without a correspondingly appropriate effort to counteract the destruction of the underlying social fabric within the communities. We have learned that it is only when local management and the residents reclaim their neighborhood that the criminal element finds it difficult to re-enter.

OSH initiatives that have met with success include cooperative efforts of law enforcement with housing authority management in Boston, Washington DC, and Atlanta.

Mission Hill, Boston, MA

In the Mission Hill housing complex, which has the highest crime rate within the Boston Housing Authority, residents had to escort their children to school carrying baseball bats. The area was an open-air drug market populated by street gangs who terrorized the residents, defaced and destroyed residential buildings and took over the playground for their market.

HUD OIG, working with Boston Housing Police, Boston Municipal Police, as well as DEA and ATF, and Housing Authority executive management, provided intense attention to the immediate area with follow-up action. On September 14, 1994, law enforcement officers from the combined agencies arrested approximately 120 persons in a 24-hour operation designed to remove the criminal element from the area.

Simultaneous to the arrests, Housing Authority personnel reclaimed the playground by using a bulldozer to shove the garbage out of the way before installing new equipment. They replaced damaged doors and windows and installed new locks to residential buildings. They initiated a campaign to paint, repair and restore the efficiency of the buildings and the sense of neighborhood. Housing Authority personnel and Boston Police have remained committed to maintaining a visible presence in the area.

Residents who have been interviewed by media, a year later, maintain that they now feel much safer in their neighborhood and can sit outside and enjoy their homes. In addition, existing documentation shows that between September 1993 and March 1994, there were 1,460 calls for police service in the area, whereas for the same period, the following year, after the law enforcement operation, there were only 655. Further, the nature of the calls changed, as evidenced in the reduction from the 375 emergency calls to police made during the first period to only 104 during the year later, a decrease of over 72 percent.

Kelly Miller, Department of Public Housing, Washington, DC

The Kelly Miller apartment complex, under the management of the DC Housing Authority, was the focus of a year-long intensive effort on the part of ATF, HUD OIG, Washington Metropolitan Police, along with Housing Authority management. Kelly Miller was a complex under the rule of a violent drug gang. The law enforcement components, acting under ATF's Project Uptown, spent 10 months documenting the gang's activities via covert drug purchases. The teams videotaped transactions with the goal of developing sufficient Federal evidence to support long prison terms for gang members.

By May 1995, approximately 20 gang members had been arrested on Federal charges. More than 100 Housing Authority personnel also descended on the complex in major renovation efforts and eviction action was taken against those residents whose apartments were used by the drug gang as their distribution centers. Both the management of the DC Housing Authority, as well as ATF, are enforcing their commitments to remain vigilantly on the scene, and this same concept is being applied to other specifically targeted locations of the DC Housing Authority.

John Hope Homes, Atlanta Housing Authority, Atlanta, GA

In February 1995, ATF announced the apprehension of 14 members of the Miami Boys street gang, who had a history of murder and intimidation, in connection with their drug activities. They were based within Atlanta Housing Authority residential communities, specifically, John Hope Homes. The 18-month investigation utilized various investigative techniques, including evidence/drug purchases made at an undercover unit provided through OIG. In addition, an OIG agent participated in the covert aspects of the field work.

The Miami Boys were involved in a struggle to control drug sales. One incident involved a drive-by shooting by gang members armed with an AK-47 assault rifle, killing one person and wounding five others. The gang members also committed home-invasion robberies in Fulton County by impersonating police officers allegedly conducting a raid at the residence.

Gang members are awaiting sentencing upon their Federal pleas; however, Atlanta Housing Authority administration has already evicted them. In addition, maintenance personnel have gone into John Hope Homes, replacing doors, windows and locks and putting new security measures in place.

Witness Relocation

Just prior to the announcement of OSH, FBI Director Louis Freeh brought HUD a problem with far-reaching consequences: on many occasions, U.S. Attorneys and local prosecutors were stymied in their efforts to vigorously prosecute the violent criminals terrorizing HUD-funded residential communities. Residents of public housing who had direct knowledge of violent crimes were unwilling to come forward to assist police because the perpetrators of the violence would intimidate the witnesses by threats against them and/or their families. Cases were documented in which potential witnesses were killed, wounded or assaulted before they had any opportunity to speak to law enforcement. Director Freeh asked Secretary Cisneros if there was any way these witnesses/residents could be relocated in order to remove them from imminent danger. The OIG and HUD program managers collaborated to address Director Freeh's concern as part of OSH.

Since the inception of OSH, HUD OIG has facilitated the relocation of 183 witnesses/families using other available HUD-funded residential property. The management of other housing authorities and managers of other HUD programs have cooperated with the OIG in providing residential units to which witnesses can be relocated. The vast majority of relocations have been effected at the request of other Federal law enforcement agencies, and with the concurrence of appropriate U.S. Attorneys. This is a relocation effort only and OIG does not provide protection services for threatened witnesses. Further, this is usually temporary housing provided until either the U.S. Marshals Service program takes over the witness, other arrangements are made with the prosecutor's office, or until prosecutive efforts have been completed.

To illustrate the importance of this effort, U.S. Attorneys have successfully prosecuted gangs in the metropolitan areas of Boston, Hartford, New York, Washington DC, and Atlanta on the testimony of persons who were threatened by gangs and then relocated by HUD OIG.

Dialogue between Police Chiefs, Department of Justice and HUD Program Managers

To improve relationships between housing authorities and local law enforcement, the OIG and the International Association of Chiefs of Police (IACP) have sponsored two conferences of Department of Justice (DOJ) officials, HUD program managers, and 10 representative Chiefs of Police. The unprecedented dialogue between HUD program managers and the Chiefs allowed the identification of numerous issues that are impeding effective housing authority/law enforcement relationships. The OIG is now working with the IACP and HUD program officials to develop variations of these conferences to be held at the local level.

(continued on page 24)

Legislative Proposal

With OSH, we have learned of the frustrations of law enforcement entities in addressing violent crime, especially within the context of publicly funded housing. The newest aspect of our evolving OSH methodology involves finding avenues to convey our experiences to both Departmental and Congressional leadership.

We have experienced the frustration of arresting violent criminals, only to see them remain in HUD-funded units, apparently indefinitely, pending eviction proceedings controlled by municipal courts.

We have questioned the ease with which those with criminal convictions, especially for crimes of drugs and violence, obtain admission to publicly funded housing.

We have come to question three existing Federal legislative impediments to screening and evictions that (1) provide administrative grievance rights to residents, unnecessarily extending any eviction process; (2) fail to place responsibility on any applicant or resident for their disclosure of current illegal drug use; and (3) limit public housing access to criminal conviction information available through the National Crime Information Center (NCIC).

We have listened to the complaints of Chiefs of Police, as well as witnessed the detrimental effect of housing drug/alcohol addicted persons, classified as disabled, in our senior citizen communities.

Finally, we have witnessed the apparent futility of programs geared solely towards prosecution, under which the most up-and-coming drug gang immediately emerges to fill any void created by the arrest and removal of the prior one.

In response to these concerns, OIG staff developed proposed legislative remedies to address each of the apparent short-comings. The Secretary forwarded the OIG's proposed legislative package to the Congress for its deliberation.

Fraud In Public Housing Administration

Over the years, the viability of the public housing program has been undermined by a perception of widespread fraud and corruption in local public housing authorities. OIG audits and investigations have not only led to successful prosecutions and financial recoveries, but also to Congressional hearings into mismanagement and corruption in publicly funded housing. With the initiation of OSH however, a new level of audit and investigative endeavor was developed.

OIG initiated a series of "fraud probes" focused within a sampling of housing authorities. Probes are limited reviews, jointly conducted by the Offices of Audit and Investigation, designed to quickly test the fiscal integrity and procurement process in specific housing authorities. Housing authorities targeted were selected from a pool of medium size authorities not having received OIG audit attention in the immediate past.

Secondly, OIG obtained a commitment from the FBI and DOJ as to the need to establish priorities among fraud investigations that were either ongoing, or as were developed by the probe teams.

Initial probe efforts involved OIG work at 44 public housing authorities, many of which could not have been reached through traditional audit work. These probes did not reveal a significant number of serious discrepancies, representing a positive result for the public housing program. At the same time, probes directed at housing authorities already under investigation have had significant results. For instance, cases in Washington, DC, and Irvington, NJ, were subsequently brought to indictment and conviction with the aid of probe results, and a second phase of investigation in those matters occurred based on findings of the probe teams.

Also, the joint DOJ/FBI/OIG commitment to pursue allegations of fraud and corruption within publicly funded housing has met with success. The OIG's *Semiannual Report to the Congress* for the period ending September 30, 1995, documents that there have been 94 indictments and 68 convictions of fraud matters within public housing authorities since OSH began. These prosecutions have resulted in fines and restitutions ordered by the courts totalling in excess of $867,000.

Examples of the types of cases developed and prosecuted include the following:

- Twelve individuals were prosecuted in a contract/procurement bribery case at the Baltimore Municipal Housing Authority. Eight contractors paid illegal gratuities to three Housing Authority personnel and one state official in exchange for their preferable treatment in the award of construction contracts.
- Two employees of the Housing Authority of Nogales, AZ, were convicted along with a bank employee for their roles in a 10-year conspiracy of diverting rental assistance funds from the Authority to their own uses. Their scheme resulted in the diversion of approximately $240,000 of Section 8 funds from the Authority and the extortion of $10,000 from program applicants and participants.
- Ten persons, five of whom were employees of the Wash-ington DC Housing Authority, were convicted in a bribery scheme in which applicants least likely to be able to afford a residential unit at the Housing Authority had to pay gratuities to Housing Authority personnel in order to receive their units.
- The former Executive Director of the Spokane, WA Indian Housing Authority was convicted and ordered to make restitution of almost $13,000 he embezzled from Authority accounts.

Equity Skimming in FHA Multifamily Housing

For years, the HUD OIG has warned the Department about the high risk of significant defaults within its Multifamily insurance portfolio. This portfolio consists of HUD's outstanding obligations via underwriting mortgage insurance for residential apartment complexes that are owned and managed by private entities. In the event such a complex defaults on its mortgage to a financial institution, HUD pays the insurance claim.

Equity skimming plays a significant part in the realization of losses to the Federal Housing Administration insurance funds. Equity skimming is the willful misuse of any part of the rents, assets, proceeds, income or other funds derived from the property covered by the mortgage.

Apart from the fairly obvious financial losses that HUD incurs when owners collect rents but do not pay the mortgage, equity skimming generally has other insidious implications. Most notably, living conditions deteriorate for the tenants as funds intended to maintain, replace or repair living units are diverted for the personal use of owners. Another side effect noted in multifamily complexes, especially in urban areas, is that as they fall into default the incidents of violent crime increase.

Despite these very serious consequences of multifamily equity skimming, HUD's track record in pursuing equity skimming cases developed by OIG auditors was poor. As part of Operation Safe Home, the OIG determined to mount a campaign against equity skimming by 1) focusing on affirmative civil enforcement opportunities; 2) referring civil cases directly to U.S. Attorneys, rather than (as had been the practice) through HUD's Office of General Counsel; and 3) empowering OIG auditors to make the civil referrals without involvement by the OIG Office of Investigations. This last point was deemed critical, as civil cases tended to languish in the Office of Investigations while agents focused on high priority criminal cases.

OIG staff has worked closely with the Department of Justice in this effort. We have been in contact with all 94 United States Attorneys and have participated in conferences with Civil Assistant U.S. Attorneys from around the country. The outreach has paid off: since the initiation of OSH, OIG auditors, working with Assistant U.S. Attorneys from DOJ's Affirmative Civil Enforcement Unit, have pursued aggressive, affirmative litigation to stop owners and management agents from illegally diverting funding. Ninety-seven cases are currently in varying stages of civil and/or criminal prosecution with DOJ. An additional 39 cases have been closed, returning to HUD over $34 million via 34 civil settlements and 5 judgments.

Examples of OSH results include the following:

- In the Southeast, an OIG audit identified questionable disbursements totalling over $913,000 in distribution of project funds while the mortgage was in default. The owner made disbursements to himself from funds borrowed for debt service and guaranteed by the project, along with other ineligible and unsupported disbursements. On receipt of a demand letter from a U.S. Attorney, and to avoid Federal suit, the owner agreed to personally pay a mutually acceptable percentage of the ineligible distributions identified in the audit. As the subject already is repaying other Federal debts at a rate of 20% of the amount he owes, the U.S Attorney held the reimbursement of these funds to 20%.
- A settlement agreement was reached with Burnham Plaza Associates in Chicago, IL, in which restitution of $300,000 is to be made. The complex went into default in 1988 and was assigned to HUD by 1990. However, an OIG audit disclosed that over $264,000 was improperly withdrawn after default.
- In Rutherford, NJ, the owners of 16 projects located in four states agreed to a final settlement and repaid HUD over $648,000. The project owners misused the funds while the mortgages for the four projects were in default and had been assigned to HUD.
- The owner of Lambert Park Apartments in Bath, ME recently signed a stipulation agreement with the Assistant U.S. Attorney under which diverted project funds will be repaid. A 1993 OIG audit of the complex disclosed that the former owner diverted $224,349 from project operating funds. The project was foreclosed by HUD in January 1993. DOJ has received an initial payment of $50,000 that will go back into the complex.

In addition, the OSH equity skimming initiative has had the happy result of improving understanding and cooperation between OIG auditors and agents. In the past, auditor frustration about slow action on their referrals tended to focus on the role of the OIG agents. Now that OIG auditors are dealing directly with U.S. Attorneys on equity skimming civil referrals, they have gained some empathy for their agent colleagues.

Like everyone else in Federal service, OIG is all too aware of the increased demands placed on limited assets. We are being told to do more with less. In the HUD OIG, we envision OSH as exactly the form of initiative called for in today's business and social environment. It is creatively using limited audit and investigative resources by combining the skills, efforts and funds of multiple agencies in a common goal.

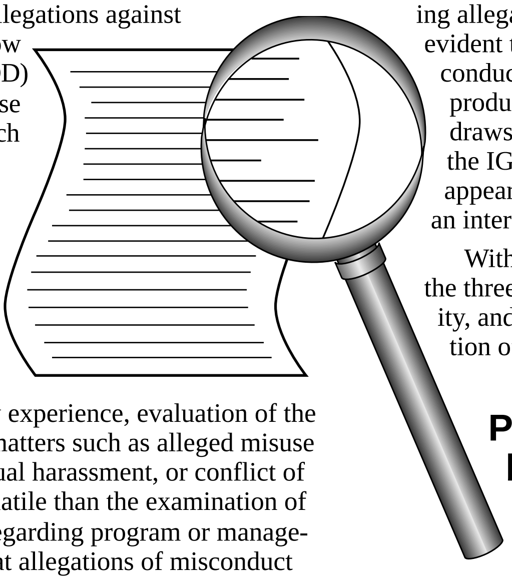
We believe that by sharing our resources, commitment and vision in common focus with our counterparts on reducing violent crime, public housing administration fraud, and multifamily equity skimming, we can make a positive change in federally Funded housing. We can enhance the quality of life, not only within those specific communities we target, but throughout the communities of the Nation.❏

Addressing Allegations Against Senior Officials

by Derek Vander Schaaf

Derek Vander Schaaf, Deputy Inspector General, Department of Defense

No potential perils to an Inspector General (IG) are greater than those inherent in addressing allegations of misconduct by senior officials within the IG's department or agency. In this article, I identify some of the risks to an IG in conducting investigations of allegations against senior officials, and discuss how the Department of Defense (DOD) IG has sought to overcome those risks. In the process, I will touch on the policies and procedures we in the DOD Office of Inspector General (OIG) use in addressing this aspect of our mission.



I begin with some observations about the business of investigating alleged misconduct by senior officials. In my experience, evaluation of the conduct of senior officials in matters such as alleged misuse of Government resources, sexual harassment, or conflict of interest, is inherently more volatile than the examination of the same officials' decisions regarding program or management issues. The mere fact that allegations of misconduct have been made can have a substantial effect on the subject's personal reputation and professional standing. This heightened sensitivity manifests itself in much stronger emotional responses on the part of those involved and their supporters than arise in other matters.

In light of the high positions that the subjects hold in the department, pressures on an IG to "tilt" in collecting or evaluating evidence regarding misconduct by senior officials can become significant. These pressures become especially strong when the IG is required to examine the actions of a political appointee, or when misconduct by the senior official is likely to be seen as a stain on the entire agency or organization. Within the DOD, this aspect is particularly prevalent when the official is a well known three or four star admiral or general and, thus, the reputation of the military service itself is somehow seen to be at risk.

Investigations of alleged misconduct by senior officials frequently generate significant media and Congressional attention due to the subject matter and the people involved. While any investigation, audit, or inspection can become a matter of interest outside the agency, OIG reports that substantiate misconduct by senior officials are far more likely to become matters of public note than other OIG products, including criminal investigations.

Due to these and other emotional influences in examining allegations against senior officials, it should be readily evident that the IG's task is twofold. First, the IG must conduct a thorough, objective investigation and must produce a report that fully and fairly reports the facts and draws reasonable conclusions from those facts. Second, the IG must perform the investigation in a manner which appears equitable if challenges are raised by parties with an interest in the outcome of the investigation.

With this background, I will try to identify and discuss the three major generic criticisms--independence, objectivity, and competence--which arise incident to the investigation of allegations of misconduct by senior officials.

Peril 1. The IG's independence becomes an issue.

Challenges to the IG's independence are especially common in the investigation of allegations against the IG's fellow senior officials. After all, we are an integral part of the department in which we work and are likely to be viewed by those outside the department as not credible when "taking on" a senior official within the organization. In this regard, the size of the DOD benefits the DOD IG because the vast majority of senior officials do not have prominence throughout the department, nor do they have the kind of relationship with the Secretary of Defense that lends itself to this charge.[1] Still, for the DOD IG, allegations against senior officials,

[1] Our definition of senior official comprises some 1,000 active duty flag officers, 1,500 members of the Senior Executive Service, political appointees and several hundred Reserve and National Guard flag officers.

(continued on page 28)

especially against the most senior civilian officials, present a heightened exposure to charges that the IG lacks independence.

Most importantly, in deciding whether to investigate a matter, we approach the question from the perspective of whether our independence would be open to serious challenge if the inquiry clears the subject of wrongdoing. Answering this question is important because our experience is that independence issues do not arise in cases where the IG substantiates the allegations under examination. Rather, we have found that allegations challenging an IG's independence invariably come from complainants or others who are dissatisfied with our conclusion that a senior official did not engage in the alleged misconduct. The perception of independence from the person being investigated is the most important asset a statutory IG has and we do everything possible to preserve that asset. When we exonerate an official, our finding has a degree of credibility that other investigative and inspection organizations in DOD simply cannot duplicate.

The key to this problem is for the OIG to protect its independence (and all that goes with being independent) at all costs. An IG must make sure that he/she truly has access to all personnel and records and must immediately challenge any attempts to limit such access. It is also important that the IG do absolutely nothing in his or her other activities--auditing, inspecting, or evaluating--that gives the media, the Congress, or the public reason to believe that the IG's office is anything but independent.

Experience has shown that retaining independence is harder in administrative investigations than in criminal investigations where a Department of Justice (DOJ) official, generally a U.S. Attorney, enters the process as a "disinterested" third party to guide and supervise the investigation. Also it is more difficult to conduct independent investigations of high level personnel in the smaller departments and agencies than in the larger ones. In other words, as the size of the organization decreases, the perception of the IG's independence is more vulnerable to challenge.

At the DOD OIG, we have implemented several policies to ensure that we retain and demonstrate our independence. We have a policy to refer to the Federal Bureau of Investigation, the Law Enforcement Committee of the President's Council on Integrity and Efficiency, the General Accounting Office, or other appropriate office, any allegation presented to us against the IG's superiors, the Secretary and Deputy Secretary of Defense.

In determining which matters will be investigated by the DOD OIG, we operate on the principle that suborganizations (the military departments and defense agencies) should generally not attempt to investigate "themselves," especially when the subject of the investigation carries enough stature that a finding of wrongdoing or poor performance will be viewed as a "stain" on the organization.

A review of the administrative senior official inquiries that the DOD OIG has conducted in the past 2 years shows a number of common factors where we have retained responsibility. Specifically, we have tended to assume jurisdiction on cases as follows:

- Cases involving officials senior to the Service IG's chain of command and/or serving in positions that may otherwise call into question the objectivity of the Service IG to investigate the matter.
- Cases where a complaint is made regarding the investigation conducted by a Service IG of a senior official.
- Reprisal cases involving senior officials.
- Cases where a Member of Congress has specifically requested that the DOD IG retain investigative responsibility.
- Cases involving senior officials in the Office of the Secretary of Defense, defense agencies, and Joint Commands.
- Cases of special interest to the DOD IG.

As a further demonstration of our independence, prior to issuing a final report, the DOD OIG generally does not provide factual information developed during the investigation to department officials, and certainly not to Members of Congress, complainants or the media, nor do we solicit their comments regarding our proposed conclusions and recommendations. This policy enables us to avoid providing incomplete information, either incriminating or exculpatory, that may be subject to revision later in the investigation. Of equal importance, the policy serves to preclude the appearance that we are in some way negotiating our findings with DOD management or other interested parties.

Peril 2. The IG's objectivity becomes an issue.

This peril can arise in a variety of forms, such as allegations that the IG has somehow lost perspective and, consequently, either has made a "mountain out of a molehill" (from the perspective of those who are unhappy with investigations that substantiate the complaint) or that the IG has not adequately addressed all aspects of the complaint (from those who do not like results that clear the subject). Other types of complaints about IG objectivity are that the investigation was conducted in a manner that was not fair to the complainant or to the subject, or that the IG has a stake in the outcome of the investigation.

The DOD OIG has developed a number of procedures to ensure objectivity in our investigations of senior officials. First, we do not conduct criminal investigations of allegations which, if substantiated, are highly unlikely to result in prosecution. The overall size of the DOD also provides us with the "luxury" of having a separate investigative unit to conduct administrative investigations of senior officials. Thus, we do not "criminalize" the relatively "minor" complaints we receive regarding alleged misconduct by senior officials even though, in a technical sense, there may be a criminal statute that could be applied. This requires us to make an early determination as to whether the allegation(s) we are pursuing, if proven, would likely result in a criminal prosecution. For those matters where we believe that there is a "reasonable or likely" prosecutive interest, we conduct the investigation in the same manner as other criminal investigations, utilizing our criminal investigators. In all cases, we are sensitive to the need to inform the DOJ Public Integrity Section and to coordinate with our criminal investigative organizations.

However, for those matters not likely to have prosecution as an outcome, we conduct the inquiry in a slightly different manner in order to best marshal the facts and conclusions for administrative resolution. We have developed a separate policies and procedures manual to cover these administrative investigations and are, of course, attuned to the fact that the nature of an investigation, such as a conflict of interest matter, can quickly change.

Second, the IG personally signs all reports of investigation or other memoranda containing the results of noncriminal investigations regarding senior officials. This practice clearly establishes the IG's personal approval of the investigation and the report. At the same time, the IG does not get personally involved in conducting the investigation. Thus, the IG avoids being "too close to the forest" yet still ensures that the investigation is thorough and the report is fair, accurate, and balanced. The IG's final review is especially important where the nature of the allegation requires the investigators to evaluate motives for actions rather than merely to determine if certain actions took place. By remaining apart from the investigation and by bringing to the final review an appreciation of the environment in which senior officials serve, the IG can ensure that the reports neither overstate nor understate the matters at issue.

Despite our best efforts, this does not mean that our reports are necessarily well accepted by either the subject of the investigation, the subject's supervisor, or the deciding official. A recent report by an outside advisory board[2] studying investigative capability of the DOD was critical of aspects of our process for conducting investigations of senior officials. They felt that we needed to provide the subject of our reports access to the underlying information and give the subject an opportunity to comment on the report before it goes to his or her "boss" for action. In this regard, we do give the subject of the investigation a second interview in which the investigator relates the general findings and conclusions of the investigation and gives the subject an opportunity to again present matters for our consideration and to identify an exculpatory witness or documents that we may not have considered. We do not, however, normally provide specific information concerning "who told us what" to either the subject or the deciding official in order to preserve the confidentiality of persons who provide us information or evidence. On the other hand, we will provide our supporting data to the official responsible for carrying out the disciplinary action if the subject challenges specific facts contained in the report.

Finally, as indicated above, the DOD IG declines to investigate matters either where the IG had earlier taken a position on the subject matter of the inquiry or where the senior official whose actions are at issue can be reasonably viewed as having a close relationship to the IG.

Peril 3. The IG's competence becomes an issue.

This peril is encountered when allegations are made that the IG conducted a poor investigation or issued a flawed report. In our experience, this peril usually is presented in cases in which we substantiate the alleged misconduct. More often than not, the allegations arise from other senior officials who are allies of the subject and who are seeking to discredit the investigation or the investigators in order to deflect attention from the senior official whose conduct we examined.[3]

Because the resolution of noncriminal investigations rests with agency officials rather than with the DOJ and the courts, the DOD OIG has developed a number of procedures which differ from the procedures in criminal investigations. First, we provide timely notice to the senior official's superior of the initiation of our investigation and inform that official that we expect him/her to notify the subject. Although we reserve the determination to defer all notifications in order to preclude destruction of documents or other forms of obstruction, we very rarely defer notification of our investigation. Notification to the superior and the subject demonstrates a forthrightness that has served us well in gaining cooperation and access to information. Thus, we use an approach that is much more open than the covert and restrictive procedures often used in criminal investigations. For example, we do not surveil people, use consensual monitoring, or obtain and execute search warrants. However, we have occasionally used IG subpoenas, handwriting experts, and polygraphers.

Second, we tape-record and prepare verbatim transcripts of all interviews except those which are minor in nature. We provide a copy of the transcript or a duplicate tape to subjects and witnesses who ask us to do so. The transcripts are valuable in the event that an issue arises regarding what occurred during the interviews. They have been especially helpful in eliminating the classic disputes in which a witness or subject asserts that the investigators did not accurately report the results of a particular interview.

Third, we usually conduct interviews of the subject both early and late in the investigation. The early interview takes place after we have interviewed the complainant and

[2] *Report of the Advisory Board on the Investigative Capability of the Department of Defense,* Volume 1, U.S. Government Printing Office, pages 77-87.

[3] The corollary to this allegation is that if the IG cannot properly address allegations regarding senior officials, there is reason to question the quality of the IG's work in other areas.

(continued on page 30)

done some preliminary work. The purpose of the interview is to determine the subject's response to the allegations. The early interview affords the subject the opportunity to admit, explain, or deny the facts at issue and to identify witnesses and documents we should consider during the investigation. The late interview occurs after the investigative work has been completed. At this interview, we advise the subject of the investigator's (but not the IG's) tentative conclusions and solicit any additional comments or information he or she wishes to provide. Prior to completing our report, we pursue any new information which the subject supplies during the final interview.

Fourth, we obtain assistance from experts elsewhere in DOD and the Executive Branch as needed to ensure the quality of our investigation and the correctness of our conclusions. Thus, we have solicited the views of specialists in agencies ranging from the Office of Government Ethics to the Federal Aviation Administration when matters at issue have been beyond our expertise. In such cases, we note our use of the experts in the report of investigation.

Fifth, while the standard of proof in administrative matters is preponderance of the evidence, we have found that disciplinary officials often operate on a de facto standard of mathematical certainty. Thus, in preparing the report of investigation, we recognize that any ambiguity or loophole may be viewed as a basis to discredit the findings of the report. All reports undergo legal review. Our practice of multiple reviews of each report, while sometimes time consuming, has served the DOD OIG well by ensuring the correctness of our final reports.

Sixth, we issue final reports to the head of the DOD component or agency. When warranted, we may recommend consideration of appropriate disciplinary action; however, we do not recommend a specific form of action.

Seventh, as a rule the IG does not engage in dialogue with the subject or the subject's counsel prior to issuance of a final report. As previously noted, if a subject contests a factual matter in our report, we generally give the disciplinary official(s) the evidence supporting the fact at issue. Our determination in individual cases is predicated on whether release of the factual basis could lead to some form of reprisal against the witness, especially where the witness is a subordinate of the subject senior official and the senior official likely will remain a supervisor of the witness after completion of the process.

Eighth, the DOD OIG does not issue press releases regarding our noncriminal investigations of senior officials and does not participate in press conferences held by the military departments or defense agencies relating to the results of our investigations.

Conclusion

The investigation of allegations against senior officials is of critical importance and, to a large degree, influences the overall reputation of each OIG. Success in this area of responsibility comes only with a dedication to fairness, thoroughness, scrupulous review and, most importantly, a willingness to let the chips fall where they may. Despite all our effort and attention to detail, I have yet to find an administrative investigation that was conducted perfectly or a written report that could not have been improved. There simply is no such thing as a perfect investigation. We must do our utmost to ensure that all administrative investigations are fundamentally fair from the standpoint of getting the facts right, in the right perspective, and in giving the individual involved an opportunity to make his/her case to the OIG investigator and to the deciding management official. ❏

Legal Eagles: Ethics

“Statutory and Regulatory Responsibilities: Who Does What, When, and to Whom”

by Maryann Lawrence Grodin and Alexandra B. Keith

Maryann Lawrence Grodin, Counsel, Office of Inspector General, Nuclear Regulatory Commission

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

Introduction

The substance of this article was previously presented in lectures to ethics attorneys at the Interagency Ethics Council on May 4, 1995, and the Office of Government Ethics (OGE) Annual Conference on September 13, 1995. The citations of statutory and regulatory prerequisites that define the roles of Federal attorneys serving in ethics and Office of Inspector General (OIG) positions were published (without copyright restrictions) in the August 1995, *Federal Ethics Report* in an article titled, “The Role of Inspectors General in Ethics: Inspector General Counsel and Ethics Counsel Interface.”

The purpose of our article is to share with the OIG community the legal guidance and practical insights gained in research on the topic of the relationship between the OIG mission and function and those of the Ethics Counsel/ Designated Agency Ethics Official (DAEO).

Our goal is to provide an overview, analysis and perspective on the Inspector General (IG) Counsel/Ethics Counsel/DAEO relationship. In addition to identifying relevant statutes and policies, we intend to clarify common misunderstandings such as miscasting DAEOs in the role of “enforcers” of ethics statutes or as investigators of ethics violations.

The IG’s Authority to Investigate

The IG Act of 1978, (“the Act”), 5 U.S.C. app.3, authorizes IGs to conduct criminal, civil, and administrative investigations. This broad investigative authority is the same for the Presidentially-appointed IGs, generally at the larger departments and agencies, and the agency head-appointed IGs at the generally smaller “designated Federal entities.”

The IGs’ investigative authority is found in several places in the Act. First, section 2(1) of the Act authorizes IGs: “to conduct and supervise audits and investigations relating to the programs and operations of (their agencies;).”

Section 7(a) provides that an IG may receive and investigate complaints or information from employees about an array of activities. These are described as activities that could constitute a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a danger to the public health and safety.

Section 4 requires the IGs to report to the Attorney General when they have reasonable grounds to believe that there is a violation of Federal criminal law. IGs interpret this section to mean referrals for prosecution. Thus, an IG will usually, although not always, finish investigating an allegation and determine whether it can be substantiated before presenting evidence of a violation of Federal criminal law to the Department of Justice (DOJ) or an Assistant United States Attorney for prosecution.

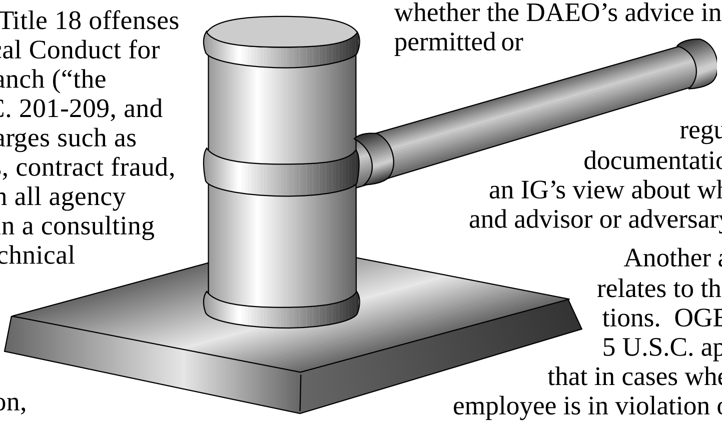
In order to carry out their investigative authority, IGs are given some helpful law enforcement tools. For example, section 6(a)(1) of the Act permits IGs to access all records, reports, documents, etc., available to the agency relating to the programs and operations for which the IG has responsibility. IGs interpret this section to mean that anything the agency can access, the IG can access also. With the exception of certain national security information at the Departments of the Treasury and Defense, agency IGs can ask for and obtain any record that the agency has or could get. If the agency does not have the material, then the IG can subpoena it if it is held privately. If the record is in the custody of another Federal entity, the IG may not issue a subpoena, but may request the information, and the other agency is to furnish the information and any assistance.

(continued on page 32)

IGs do not have testimonial subpoena authority. They may require agency employees to speak with them about official matters within the confines of the Constitutional privilege against self- incrimination. However, IGs cannot subpoena a private citizen to speak with OIG agents. Neither do IGs, without special statutory authority or deputation, carry guns, make arrests, or serve warrants.

Section 6(a)(2) of the Act allows IGs, "to make such investigations and reports relating to the administration of the programs and operations of the applicable establishment as are .... necessary and desirable." Thus, as investigations are completed, IGs may issue reports and make recommendations for prosecution, administrative discipline, systemic internal controls, or anything else that would help the agency improve operations, fight fraud, or save money.

IGs often investigate allegations of ethical misconduct. These include the Title 18 offenses on which the Standards of Ethical Conduct for Employees of the Executive Branch ("the Standards") are based, 18 U.S.C. 201-209, and traditional public corruption charges such as bribery, acceptance of gratuities, contract fraud, and conspiracy. As they do with all agency employees, DAEOs may serve in a consulting role for OIG investigators on technical issues of ethics law. OIG agents and counsel might both consult the DAEO, within the confines of the Privacy Act, about what constitutes a violation, whether a violation has occurred, and what remedy or corrective action is usual within the agency.



The DAEO's Role

Title 5 Code of Federal Regulations (CFR), Part 2600 implements 5 U.S.C. app. 5, the (Ethics in Government Act of 1978), the statute that created OGE as the authority to oversee ethics regulation in the Executive Branch. As the agency responsible for directing ethics programs in executive departments and agencies, OGE issues rules, directives and advisory opinions on ethics matters. Pursuant to the authority in titles II and IV of the Ethics in Government Act of 1978 (Pub. L. 95-521, as amended), OGE directs the administration of agency ethics programs and agency DAEOs. Further, 5 CFR 2638.201 et.seq. directs that the DAEO shall coordinate and manage the agency's ethics program. The DAEO has a different role than the IG. The DAEO mission is generally directed to preventive legal assistance.

The duties of the DAEO are described in 5 CFR 2635.203 to include liaison with OGE, review of financial disclosure reports (one of the most unappreciated and tedious tasks in Government), initiation and maintenance of ethical education and training programs, and monitoring of administrative actions and sanctions.

A critical function of the DAEO is to develop and provide counseling as part of a program of formal advice to all agency employees on ethics and Standards matters, including post-employment questions. Imparting consistent advice to employees and communication regarding administrative actions is the DAEO's function that has the potential to ensure a positive connection with the OIG. The most critical aspect of this function--and the source of most frequent controversy between the two offices--is documentation of advice given to employees. Written records evidencing the facts conveyed by a subject employee and limitations and restrictions identified in the ethics advice given in response to those facts, are the most pivotal records relied upon either by the employee for defense or for the OIG and DOJ in prosecution.

Friction between IGs and DAEOs is virtually unavoidable when written records of advice relevant to an allegation are not available. In these cases, disputed testimony about whether the DAEO's advice indicated the activity was permitted or prohibited is inevitable, and can compromise potential for prosecution. The regularity and specificity of documentation of ethics advice can color an IG's view about whether the DAEO is an ally and advisor or adversary, or worse, a subject.

Another area of responsibility which relates to the OIG is that of investigations. OGE responsibilities reflected in 5 U.S.C. app. 5 §402 f(2)(A)(ii), provide that in cases where he or she believes an employee is in violation of a conflict of interest or Standards regulation, the OGE Director, as a NON-DELEGABLE (emphasis added) function, may recommend that the agency head investigate possible violations and take disciplinary action. In these cases what normally happens is that the agency head asks the OIG to investigate. The provision that confers jurisdiction on the OIG in these cases is §402 f (5), which provides that, "Nothing in this title shall be considered to allow the Director to make any finding that a provision of Title 18 U.S.C. or any criminal law ...has been or is being violated." In addition to being outside the jurisdiction and scope of employment of a DAEO, an agency ethics attorney who acts to investigate allegations of wrongdoing could incur personal liability. (See, Federal Tort Claims Act, 28 U.S.C. § 2670 et.seq., which allows for indemnification of Government employees only for actions taken "within the scope" of their employment.) For this and the reasons discussed below, the single correct response for a DAEO to make to an allegation is referral to the IG!

Where IGs' and DAEOs' Authorities Intersect

The Federal ethics regulations recognize a special relationship between DAEOs and IGs. In carrying out their agency ethics programs, DAEOs are required by the Standards to review information developed by the OIG or other auditors. 5 CFR 2638.203. The purpose of such review may be to determine whether there is a need for revising the agency's supplemental Standards of Conduct or taking corrective action to remedy actual or potential conflict of interest situations. Thus, if an OIG audit identifies a recurrent conflict situation unique to the agency that is not addressed by the Standards, then the DAEO might consider a curative supplemental regulation. If an OIG investigation finds that an agency contracting officer has violated the Standards by purchasing stock in a firm with which the agency contracts, the DAEO might be asked by management to recommend appropriate remedial or corrective action.

The Standards also encourage DAEOs to "utilize" the OIG's services, to refer matters to the IG and accept matters referred by the IG, when appropriate. DAEOs are in an excellent position to refer to the IG allegations of criminal or civil ethics violations that they encounter in their daily work, including violations of Standards.

When employees come to the DAEO for prospective ethics advice, there is usually no need to refer the matter to the IG. However, when agency employees inform the DAEO of past transgressions, or explain what prospective mischief they are planning no matter what the DAEO's advice, then the DAEO is obligated to report to the IG. Such reports or referrals must be timely to be useful to the IG. The DAEO should not wait and see whether the planned violation occurs or whether he or she can persuade the employee to do otherwise.

DAEOs need the IGs because they have no authority to undertake investigations on their own. Neither may a DAEO offer an agency employee the protection of attorney-client privilege. The agency's internal investigative authority resides with the IG, and the DAEO should refer all information, documentary and otherwise, to the IG when he or she receives information of a violation or planned violation, pursuant to the Standards and the agency's own regulations.

IGs also utilize DAEOs. They may refer to DAEOs audit or investigative findings that the agency is not conducting its ethics program properly, e.g., employees are not receiving their confidential ethics forms and are not filling them out properly or in a timely manner. The DAEO can then take systemic action to correct the program. On an individual level, the IG may refer to the DAEO for counseling an employee who has violated or is about to violate an ethics rule, e.g., the employee referred to above who has purchased the stock that puts him in a conflict position, and the IG has determined not to pursue criminal or civil prosecution.

Reporting Requirements

Reporting requirements are imposed upon both OIGs and DAEOs. In accordance with 5 U.S.C. app. 5 §402 (e)(2), the Director of OGE has promulgated regulations at 5 CFR §2638.603 requiring that agencies provide notification to the OGE Director when criminal referrals are made to the DOJ in accordance with 28 U.S.C. § 535. This is usually accomplished by OIG submission of OGE Form 202 (7/94), "Notification of Conflict of Interest Referral" at the time formal referral is made to the DOJ. The form indicates that it is to be used in cases involving possible violation of 18 U.S.C. §§203, 205, 207-209 by current or former Executive Branch employees. Under §4(d) of the IG Act, OIGs are required to report violations of Federal criminal law to DOJ.

Reciprocally, agency officials, including DAEOs, are required to report wrongdoing to the OIG under the authority of Executive Order 12674 as well as agency regulations and directives.

How OIGs and DAEOs Can Work Together Better

Two areas where OIGs and DAEOs can enhance the effectiveness of both missions are communication and training. One particularly worthwhile communication vehicle is news articles on ethics topics in agency newsletters. These keep the OIG, and everyone else in the agency, aware of current ethics issues from the DAEO perspective. Combining mandatory ethics training with OIG integrity awareness briefings can be effective in making ethics regulations clear and comprehensible to all employees. Having both the rules and the consequences of not following them illustrated in one presentation also encourages compliance with ethics statutes and regulations. It also gives insight into problem areas within the agency and facilitates identification of remedies.

DAEOs and IGs both endeavor to prevent fraud, waste and abuse in Government agency's programs and operations. Understanding and respecting each other's statutory roles in that effort will allow for more efficient accomplishment of those goals. Continuing to educate each other will make it happen more effectively.

The views expressed in this article are those of the authors alone and are not intended to reflect those of the Nuclear Regulatory Commission, its OIG nor that of the National Credit Union Administration or its OIG. ❑

Aspects Of The IG Act: Independence-- The Bedrock Of Inspectors General

by John C. Martin

John C. Martin,
Inspector General,
Environmental Protection Agency

You might have heard the saying "the best thing about something can also be the worst thing!" In my view, that saying is a perfect fit for the independence of an Inspector General (IG) and his or her office. Why is it the best thing? Because we can do our difficult and challenging work with a freedom that has few parallels in Government today. Why is it the worst thing? Because with this freedom comes an awesome responsibility to do right--that is, both to do right things, and to do things right.

Our audit work can be a powerful tool for positive change or it can be negative and even destructive if it's not done well and leads to faulty conclusions. Our investigative work has the potential to ferret out wrongdoing and bring those responsible to justice. It can also be a tool that helps the innocent clear his or her good name. On the other hand, the simple fact that an investigation is being conducted can cast a shadow of doubt over someone's reputation. If the investigation was misguided to begin with or conducted in an unprofessional manner, permanent damage can be done without any justification. Sometimes, lives can even be put at risk. So in short, with independence comes a lot of responsibility.

Perhaps our greatest responsibility is the duty to say "no" to the powerful who attempt to get us to follow a course that isn't right. When the pressure is on, it's usually easy to say "yes." We can crank up our audit or investigative machine and leave no stone unturned, but at what risk and with what damage on the way? We must be willing to say "no" or "no more" whenever we recognize that there is no real basis for an allegation but that others are attempting to use our powers for their own ends. Some situations are more difficult to handle than others.

When we conduct criminal investigations we enjoy the benefits of working as a partner with the Department of Justice under discreet conditions that may even include grand jury secrecy requirements. But when we do administrative inquiries, we stand alone in the spotlight, most often as the only investigative unit in a department or agency that does not have law enforcement as its primary mission. That puts the "heat" squarely on us and makes it even more important that we do high quality, impartial work.

What is the practical meaning of independence and is it complete or absolute? The IG Act of 1978 and its amendments clearly established IG operations as independent entities within their parent organizations. The essence of this independence is captured in Section 3 of our charter, although other provisions which give us operational independence are woven throughout the document. Some of these operational authorities include: a separate appropriation, so that funds cannot be removed from our accounts by our agency; a separate authority to "select, appoint and employ" all of our own personnel; separate legal counsel and separate administrative functions (personnel, finance, etc.) to the extent we desire to utilize them; complete access to all the records of the agency; freedom to issue any reports we believe are necessary and desirable; and subpoena power for books and records. These authorities give us great autonomy and should not be taken for granted.

But, as I said earlier, the heart of our independence is stated in Section 3 of the IG Act which says simply yet powerfully that the IG can't be prevented "from initiating, carrying out, or completing any audit or investigation ...." The sentence immediately preceding this strong statement of authority does say that the IG "shall report to and be under the general supervision of the head..." of the agency.

Yet, if the IG can't be prevented from doing his or her work, what do the terms "report to" and "general supervision" really mean? First, it means that the agency head can have a prime role in selecting a new IG when a vacancy occurs. Second, it means that the agency head can evaluate the IG's performance each year, if the IG is a member of the career service. Third, and most important it means the agency head can directly influence the size of the IG's operation by making budget decisions each year as the IG's budget moves through the appropriations process. Each of these situations represents the legitimate exercise of authority by an agency head.

Is this a perfect situation? No. The nature of our work inevitably places us into conflict with key staff in our own agency who can try to influence us by using the agency head's authority which I just described. The conflict may

(continued on page 36)

even involve the agency head personally. Yet none of these powers are so strong that they cancel out our own authority to do our job.

And there are safeguards. The Office of Management and Budget (OMB) plays a vital role in helping to ensure that retaliatory actions are neutralized. The various oversight and appropriations Committees of Congress play an important part as well. Are these safeguards perfect? No again. OMB's efforts may be too little or too late. The Committees of Congress may not have the interest or desire to "rescue" an IG's office, particularly if they haven't had a good working relationship with it in the past. But, even with these flaws, there is no question that independence has been firmly established as a prime component of the IG's operation both through law and past practice.

How does independence square with the philosophy of this Administration that we should act in a more cooperative way with agency management to solve problems? I don't see any conflict with our audit work. A cooperative solution to problems has always been the preferable way for us to pursue our work. The course we can follow has two parts. First, we can involve management in the selection of our audit projects so we're certain that we're pursuing the most valuable and important issues. Second, though, we must actually do our work in an independent and objective manner. The facts are the facts and we should report them as such. How to use those facts and what they mean to crafting a solution to a problem leads us to the cooperative approach that we should all be seeking.

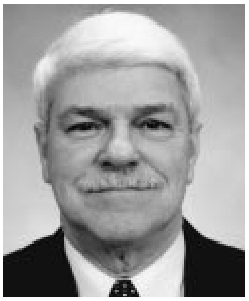
Investigations are a more sensitive matter because their objective is to determine the guilt or innocence of particular people who may have violated a law or administrative regulation. This work is more confrontational by its nature with a very high risk to the subject of the inquiry. Therefore, we must pay particular attention to ensuring that investigations are performed in an impartial manner without influence from those with a stake in their outcome.

I'm one who believes that the IG Act of 1978 was carefully crafted with a great deal of foresight. Of all the parts of this Act that help us do our job, none is more important than independence. It creates the bedrock on which everything else rests. Yet with independence comes responsibility, so we must always be good stewards--much is expected from those to whom much is given. ❏

The Power Of One: IGnet

by Michael Bromwich, John Dye, and Jenny Banner Wheeler

Michael Bromwich, Inspector General, Department of Justice



John Dye, Deputy Assistant Inspector General for Auditing, Small Business Administration

Jenny Banner Wheeler, Special Assistant to the Inspector General, Department of Health and Human Services

Conceived a little over 2 years ago by my former Assistant Inspector General (AIG) for Investigations, Jerry Bullock, and a supporting cast representing other Offices of Inspector General (OIG), IGnet is now part of the ever growing worldwide communication network, the Internet. During its infancy, it had one basic mission--to provide public access to OIG documents and to facilitate communication between OIGs. Today, under the direction of John Dye, Deputy AIG for Auditing, Small Business Administration (SBA), and Jenny Banner Wheeler, Special Assistant to the Inspector General (IG), Department of Health and Human Services, IGnet has dramatically changed and its scope has significantly expanded. Not only is IGnet steadily working to meet the original mission, it is also working to answer the often asked question, "How can the Internet help me do my job?" and the frequently expressed concern that auditors, inspectors, and investigators can't afford to "surf" the Internet to find useful information. In this article, I will outline the capabilities of IGnet and hope that you will find the possibilities as exciting as I do.

Increased Communications

How do you reach 500 auditors, investigators, or inspectors quickly if you need assistance or advice on a particular subject? IGnet's mailing lists are the answer. Internet-based mailing lists transform person-to-person communications to group communications. When you send a message to a mailing list it is broadcast to everyone who has chosen to subscribe to the mailing list. The more people who choose to participate, the greater your capacity to gather information and answers to questions.

IGnet has established mailing lists for each OIG functional area (audits, investigations, and inspections) as well as one for management issues and another which focuses on computer technology. Subscribers to any OIG mailing list must first register with the IGnet Director by supplying the following information (send to: jedye@fred.net):

IGnet Mailing List Registration

Name:
Title:
Agency/Organization:
Address:
Phone:
Fax:
E-mail Address:

Although registration is required, IGnet mailing lists are open to any individual in the audit, inspections, or investigations profession. IGnet describes this extended professional family as the "OIG community."

(continued on page 38)

Tools to do the Job

One of the beauties of the Internet is quick and easy access to resources and research materials on-line. If a person doesn't have a place to start, however, much time can be spent wading through the wealth of information available. This is where IGnet is so valuable. With the advent of the IGnet "Homepage," research materials and related networks are readily available. The Homepage is located on a World Wide Web server at the SBA. Such servers support graphical layouts and hotlink capability. These hotlinks allow a person to move from one place on the Internet to another with a click of a mouse button.

The IGnet Homepage contains an audit and inspections resource list, an investigations resource list, and a cumulative Internet resource library. As an example, the audit and inspections resource list is subdivided into 14 sub-categories:

Information from the OIGs.

Training.

Audits Standards & Related Policies.

U.S. General Accounting Office Information.

Related Audit Agencies & Organizations.

Evaluation % Inspector Related Internet Sites.

Federal Laws and Regulations.

Legislative Information.

Government Documents.

Information Technology.

Other Federal Internet Sites.

Other Related Networks.

Network Indexes/Locators.

Internet Search Engines.

Under each of these sub-categories, hotlinks to the resources are provided. These hotlinks give you on-line access to such resources as: the Yellow Book, answers to the May 1995 CPA exam, the Office of Internal Audit-City of Albuquerque, New Mexico, General Accounting Office reports, the Code of Federal Regulations, full text of legislation and related floor or committee actions, the Superintendent of Documents at the Government Printing Office, the Internal Auditing Network, and the State and Local Servers Index.

The investigations resource list has a similar architecture. In this case, the hotlinks provide access to investigative related items including: the Inspector General Criminal Investigator Academy schedule, the Federal Law Enforcement Training Center Legal Update Series, National Criminal Justice Reference Sites, and Copnet and Cybercop (both are law enforcement networks/databases).

Since the inception of IGnet's Homepage in June 1995, IGnet's library resource list has grown exponentially. As new resources are identified, they are included in the lists. At least once a week changes are made to the library lists--so there is always something new to find. As a result of these libraries, OIG staff have more timely access to needed information and costs associated with maintaining hard copy libraries are reduced.

Public Information

The Administration has stated that one of its goals is to provide greater public access to Government documents. Congress is also supportive of this effort. In a letter to John Koskinen, Deputy Director for Management, Office of Management and Budget, dated March 10, 1995, Senator Joseph Lieberman of Connecticut stated:

> "It has come to my attention that some executive branch agencies are offering the public access to their Inspector Generals' reports through on-line computer services. As a member of the Senate Governmental Affairs Committee, I want to express my strong support for this practice, and to encourage every Inspector General's office to make this service available if possible.
>
> By posting their findings on the Internet for all the public to see, the Inspectors General can bring taxpayers that much closer to the inner workings of the programs they are paying for. The net result should be a more participatory, and more accountable, Federal Government."

In that spirit, IGnet also provides a venue for electronically publishing OIG documents. Currently IGnet provides access to audit, inspection, and semiannual reports from more than 20 offices. These reports are presented as either executive summaries, with a contact name and number for requesting a printed copy, or in full text. In addition to standard reports, other relevant OIG documents (e.g., testimony, special fraud alerts, press releases, and published articles) are provided. Because of the diversity and depth of the material, IGnet has already gained recognition as a high content web site.

The technology supporting electronic publishing is evolving rapidly and will allow for document distribution in a variety of formats. IGnet is already capable of supporting the evolving methods of distribution and stands ready to support increased report libraries. IGnet's ability to accomplish its public service mission is limited only by the number of documents it receives from the President's Council on Integrity and Efficiency (PCIE)/Executive Council on Integrity and Efficiency community. I strongly urge all offices to participate to the maximum extent possible. Not only will the electronic distribution of documents increase public awareness regarding OIG activities, but it will also increase work product communication among the OIGs and potentially reduce the resources necessary to produce and distribute printed documents.

The Hows

As I stated previously, the IGnet Homepage is part of the World Wide Web. To obtain access to the IGnet Homepage you must have access to a graphical web client such as Mosaic or Netscape, but you can also access it through the Lynx text based system (although you will miss the graphical advantage). In addition, Web access is now being provided through commercial services (e.g., America Online, CompuServe, and Prodigy). To gain access, point your client to:

http://www.sbaonline.sba.gov/ignet

For those who don’t have Web access, IGnet also provides a Gopher Service. The Gopher differs from the Homepage in that it presents information in a hierarchial manner rather than providing hotlinks. It can be accessed by typing in the following:

gopher: //gopher.sbaonline.sba.gov/ignet

The Future

The possibilities for IGnet are endless. The Homepage libraries will continue to grow as relevant Internet sites are identified and as more resources become available. The number and diversity of OIG reports and related documents will also expand as offices adopt and establish procedures for electronic distribution. To facilitate public access, plans are underway to implement individual OIG “subpages” within the IGnet Homepage structure.

OIG office-to-office communication, or the process of establishing the complete virtual OIG community, will also continue to develop. The ultimate goal is to have 100 percent OIG representation on the mailing lists. As more people subscribe and begin to use the mailing lists for inter-office communications, the discussions and content of the messages will become more robust, relevant, and useful. Mailing list maturity, however, is limited by OIG staff access to the Internet. Until Internet connectivity reaches the auditors’, investigators’, and inspectors’ desktop computers, the mailing lists will not achieve their ultimate potential.

The bottom line--the future is bright; IGnet has come a long way since inception and it can only get better.

Conclusion

As you can see, the benefits of IGnet are numerous. Most importantly, IGnet enables the OIG community to overcome restrictions of time and geography. It provides better, quicker, and more efficient access to old sources of information; additionally, it provides access to a world of new information and communication sources.

IGnet has certainly developed quickly to date. But to ultimately succeed in meeting its mission, the entire OIG community must endorse its utilization and encourage broad-based participation. The use of IGnet, both as a research tool and a means of disseminating public documents needs to be institutionalized; this can only occur through top management support. I strongly urge the community to endorse and embrace this effective communication tool.

Finally, I would like to thank the members of the PCIE IGnet Task Force, the IGnet Executive Committee, the OIG representatives to the IGnet Core Team, and the Information Resources Management Offices at the SBA and the Department of Justice for their support in ensuring the ultimate success of this endeavor. ❑

Partners Against Crime Part II: State Federal Partnership

by Thomas D. Roslewicz and M. Ben Jackson, Jr.

Thomas D. Roslewicz, Deputy Inspector General for Audit Services Department of Health and Human Services

M. Ben Jackson, Jr., Audit Manager, Health Care Financing Audit Division, Department of Health and Human Services

Do more with less! Recreate your processes! Streamline and save costs! Sound familiar?

The National Performance Review, and continually shrinking budgets and resources, have caused Government agencies to rethink how they operate. Downsizing Government is an all too familiar term to Federal managers. The impact from these streamlining initiatives is being felt by all of us as these cost cutting actions shape how Government will operate in the foreseeable future. Although these changes represent significant challenges, rethinking how to accomplish our missions can provide opportunities for Federal Inspectors General (IG) to create new methods of attacking fraud, waste and abuse.

We asked ourselves in the Department of Health and Human Services, Office of Inspector General (HHS OIG), what could we do differently to address the need for audit coverage of the continually expanding HHS programs? Our answer is to form partnerships with State Auditors as a starting point.

One of HHS' largest growth components involves health care within the Medicare and Medicaid programs. We can all relate to the expenditures for hospital stays, doctor visits, and prescription drugs—all have risen appreciably in the last few years. Within HHS, the Health Care Financing Administration (HCFA) administers the Medicare program which provides health services for mostly elderly folks who are Social Security beneficiaries. The HCFA also oversees the Medicaid program which is a jointly funded Federal/State health care system operated by each State government. Both of these programs are similar in that they pay claims of providers of health care services (doctors, hospitals, laboratory companies, etc.) to entitled beneficiaries. This article focuses on our partnerships with State Auditors to expand audit coverage of the Medicaid program.

Medicaid Costs Continue to Skyrocket - Necessitating the Need for Continued Audit Coverage

The Federal and State governments are concerned about the skyrocketing rate of Medicaid spending, and their budgets are overburdened with increased expenditures. There has been increased interest in the Medicaid program in both the private and public sectors. There is a consensus that current spending trends are unsustainable for the Federal and State governments.

Medicaid outlays have risen at a dramatic pace, causing Medicaid spending to become the fastest rising portion of the Federal and State budgets. In Federal Fiscal Year 1994, Medicaid spending increased 9 percent to $138.6 billion ($78.6 billion Federal share and $60 billion States' share). Since 1984 Medicaid expenditures have increased 385 percent. It is expected that these expenditures will reach $152 billion by 1997 and will exceed $180 billion by the year 2000. Out of every dollar of Medicaid expenditures, 96 cents are paid to providers. The remainder goes for program administration.

Medicaid Audits of the Past

Traditionally, HHS OIG auditors performed retrospective, compliance-type reviews of the Medicaid program. These included reviews of State agencies' implementation of, and compliance with State plan provisions. The reviews often identified significant amounts of unallowable costs with recommendations that the particular State government return funds to the Federal Treasury. Continued downsizing and budget constraints have, in recent years, caused the HHS/OIG to rethink how to best use its limited resources and at the same time continue to provide the necessary audit coverage needed in this important health area.

(continued on page 42)

Forming Partnerships

In this new era of Government operations, our office explored ways to increase the amount of audit resources available to audit the Medicaid program by partnering with State Auditors and moving away from traditional compliance audits. We viewed partnerships as a way to propose potential audit issues to State Auditors which focus on identifying future savings related to changes that can be made in health care policies and Medicaid State plans. Other possible joint audits involve dollar recoveries of overpayments made to providers of services (doctors, hospitals, laboratory companies, etc.) where both the Federal and State governments benefit.

We recognized that State Auditors, as part of the Single Audit Act, performed a significant amount of audit work which included determining whether Medicaid program funds were properly expended and reported. What we did not know was the amount of effort State Auditors devoted to performance audits of the Medicaid program. As a result, our initial goal was to determine whether we could develop partnerships where we could first identify the number and types of performance audits completed by the State Auditors and use those results in our work planning for audit coverage in other States.

In an effort to broaden audit coverage, we also wanted to form partnerships with State Auditors to share the methods used and results achieved in our past Medicare and Medicaid audits which led to a more effective, efficient and economical delivery of health care services. This shared information may provide State Auditors with leads for audits of health care provider operations and Medicaid agencies' systems for paying health care providers. We also envision State Auditors sharing their audit methods and results with us to use in performing Medicare audits.

However, we realized early on that the thrust of any proposed partnership should not be to identify and recommend only recovery of unallowable costs from State agencies. Instead, the partnerships needed to focus on issues that would result in program improvements and reductions in the cost of providing health services--something that would benefit both the Federal and State governments. We realized this would be no small task!

Partnership Efforts Have Been Formalized

Over the past 2 years, under the guidance of June Gibbs Brown, Inspector General at HHS, we have promoted our partnership ideas by meeting with State Auditors both individually and at national forums. Because of the interest expressed during our meetings, we decided to formalize our efforts by developing a booklet entitled *Partnership Plan, Federal State Joint Audits of the Medicaid Program*. This booklet was transmitted to all State Governors and State Auditors. The objectives of the booklet are to:

- highlight a partnership plan for joint Federal/State audits that can positively influence the control of Medicaid costs,
- present successful OIG Medicare and Medicaid reviews and issues that will serve as a starting point for the partnership, and
- solicit ideas that will contribute to the success of the partnership.

Successful Partnerships with State Auditors

We have succeeded in forming partnerships with many State Auditors/Comptrollers. The Louisiana Legislative Auditor, with our assistance, built on work previously performed by our office in the Medicaid Drug Rebate program and issued a report recommending corrective actions to the State Medicaid agency. The North Carolina State Auditor and our office also jointly issued a report on a similar review. These reviews showed weaknesses in internal controls and adjudication of drug rebates in disputes. The New York State Comptroller and the OIG are currently working to establish continuing Medicaid/Medicare data matches so that inappropriate payments to vendors for services rendered to dually eligible beneficiaries can be readily identified.

Our office has also worked with the National State Auditors Association on a nationwide review of the Medicaid Prescription Drug Program in eight participating States: Maryland, Delaware, Iowa, Michigan, Missouri, Ohio, Texas and Utah. The Maryland State Auditor was the lead on this project which involved reviews of: controls over drug rebates, use of therapeutically equivalent generic drugs, limitations on prescriptions for ulcer treatment drugs to dosages recommended by manufacturers and mail order delivery system for maintenance drugs. Individual State Auditors have issued their reports and a consolidated report was issued in June 1995.

The OIG initiated a highly productive joint project with the Massachusetts State Auditor. The objective of this project was to determine the propriety of payments made by the Massachusetts State Medicaid agency to providers of clinical laboratory tests. This project stemmed from the OIG's success with similar reviews in the Medicare program. Computer applications have identified a significant number of potential overpayments for laboratory services paid during 1992 and 1993. Our office worked with the Massachusetts State Auditor to quantify the total amount of overpayments.

This project was expanded to include Louisiana, North Carolina, Texas and Utah. The final report for Louisiana, which identified estimated overpayments of $ 1.1 million, was issued in August 1995. In September 1995, the Utah State Auditor's office began a similar review of laboratory services using computer matches that were provided by our office. The North Carolina State Auditor's office has completed a similar review with OIG staff. The Texas State Auditor completed a review of laboratory services, which also included a review of hospital transfers and non-physician services. Further, we are continuing to contact other State Auditors to invite them to participate in joint audits of laboratory services.

We also initiated contacts with other State Auditors/ State Inspector Generals in Washington, Montana, New Mexico, California, and South Dakota to pursue issues included in our "Partnership Plan."

Future Partnership Efforts

We believe that our partnering efforts have been a success. Together we have been able to provide audit coverage over areas and issues which we might not otherwise have been able to accomplish given our shrinking resources. We plan to continue our current efforts and explore how we may use this partnering concept in other areas of work such as the welfare and health research areas.

Partnering: Can it Work for All IGs?

We are delighted with the joint work performed to date with our colleagues in the State Auditor offices. We believe that all OIGs are looking for opportunities to combine forces as they address their missions. Our experience has been that we needed to be open and willing to explore new ways of doing audits. We entered into discussions enthusiastically and gave freely of our experiences that focused on the issue at hand. We attempted to appreciate the other person's point of view. We did not view the performance of audits as a parochial activity or get involved in turf battles. We were willing to offer assistance to all audit organizations that could help us accomplish our mission. We did not worry about who received primary credit for issuing the reports but gained satisfaction from knowing that we are in fact doing "more with less" in the best interest of the Government and the public. And, lastly, we wanted to be a team, and a partner. ❏

Rounding up the Good Old Boys: Sexual Harassment

by Beth Serepca

Beth Serepca,
Senior Auditor, Office
of Inspector General,
Department of the Treasury

The boss came into her office one day, just after she had led a very successful meeting involving several million dollars in questioned costs. He had a question for her, he said, smiling. He wanted to know if she had deliberately not worn a bra in order to make sure that the men were eating out of her hand.

Sound like a grade B Hollywood movie? This situation really happened—not to me, but to another female internal auditor. Sexual harassment, like other kinds of sexual abuse, is about power, not sex, which is why both males and females can be the harasser. The harasser wants to force another to feel or act a certain way.

Because I haven't personally experienced sexual harassment, I've not always been aware of the seriousness and pervasiveness of this problem. As an auditor for the Federal Government, however, I've now reviewed a number of sexual harassment allegations, and I've learned a great deal.

At some point I began to wonder how widespread this problem was among internal auditors. With funding from the Washington, DC Chapter of the Institute of Internal Auditors (IIA) and the IIA Research Foundation, I conducted a survey of internal auditors in private industry and Government to determine whether their work environments are free from fear of sexual harassment. Questionnaires were sent to 1,000 internal auditors; I received responses from 514.

I was shocked by the findings of this study. Twenty-four percent (121 of 514) of the internal auditors reported that they had been sexually harassed. As indicated in the following chart, a male supervisor was most often reported to be the harasser, followed by a male coworker. The table below shows the gender of the harassers and the relationship of the harasser to the victims:

	MALE	FEMALE	MALE AND/OR FEMALE
Supervisor	42%	3%	
Friend	1%	2%	
Coworker	20%	8%	
Harassed More Than Once By More Than One Person			13%

The respondents in this study were predominantly white (415 out of 514) followed by African American (54 out of 514), in the 26- to 40-year old age group. Participants included 244 males and 229 females. The majority of the respondents indicated that they were married, although they were not asked whether or not they were married when the sexual harassment occurred.

Of the 121 internal auditors who had been victims of sexual harassment, 78 percent were women. The most likely victim in this pool of respondents was shown to be a white female, aged 26-40 years old, employed in private industry.

Even pregnant women apparently aren't immune to being harassed. Two women wrote that men "came on to them" during work hours even though their pregnancies were obvious.

Thirty-five percent of the victims had been harassed, either verbally, physically, or both, in their own offices. In many situations the harassment occurred more than once.

One of the most distressing findings was that 36 percent of the respondents answered "no" when asked if they had informed anyone about the harassment. I couldn't help but wonder how, if professional auditors couldn't assert themselves in these situations, others with less knowledge and information about sexual harassment could be expected to do so. According to many written comments, as well as four telephone interviews, victims generally did not assert themselves because they did not want to be "perceived as a trouble maker" or because "they would not be believed anyway." One of the most revealing

(continued on page 46)

statistics indicated that some employees opted to leave their jobs rather than to try to deal with the harassment situation.

Government internal auditors were more likely to report harassment than private industry internal auditors, the study showed. Further, more Government employees reported that their employers had a formal written policy for sexual harassment than did respondents in private industry.

But while some organizations are taking steps to confront sexual harassment issues, incidents of reported sexual harassment are increasing. Moreover, 70 percent of the respondents in this study stated that sexual harassment is an underreported problem.

In my opinion, internal auditors and their employers need to be aware of the extensive risks that underlie sexual harassment incidents and take decisive steps to eliminate the problem. Obviously, internal auditors must, first of all, clearly understand sexual harassment. On a personal level, they must be sensitive to how others perceive their behavior and be willing to modify behavior that is perceived to be offensive. On an organizational level, internal auditors should ensure that sexual harassment policies are in place and enforced and that appropriate training is provided.

Sixty percent of the respondents, 119 women and 188 men, had received sexual harassment training. Such training is of critical importance. It enables employees to recognize when they are being harassed and when their own behavior constitutes harassment. Employers need to recognize what constitutes harassment in order to prevent it from occurring and to stop it immediately when it does occur.

Type of Harassment	
Verbal	44%
Physical	15%
Visual	4%
More Than One Type	37%

Both personally and professionally, I'm appalled by sexual harassment. No employee should have to endure unwanted workplace attention, whether it be in the form of innuendos, jokes, gestures, or touching. I not only believe that sexual harassment should be eliminated, but that perpetrators should be severely punished—perhaps by termination—for the first offense. I'm looking forward to the time when I don't have to audit any more sexual harassment allegations.❑

WIFLE Presents Awards to Donald Mancuso and Diane Hill

Reprinted from various sources

The Interagency Committee on Women in Federal Law Enforcement (WIFLE), sponsored by the Department of Justice and the Department of the Treasury, was established by Executive Order in 1978 to develop an information sharing network for women in Federal law enforcement. The committee in composed of representatives from over 35 Federal agencies with law enforcement responsibilities.

In June 1995, WIFLE presented Donald Mancuso, Assistant Inspector General for Investigations and Director, Defense Criminal Investigative Service (DCIS), with the Doris R. McCrosson Manager Award, and Diane Hill, Special Agent, Department of Housing and Urban Development (HUD), OIG, with the Julie Y. Cross Memorial Award.

The Doris R. McCrosson Award

Selection for the prestigious Doris R. McCrosson Award is based upon a recipient's exceptional accomplishments in one or more of the following categories related to women's issues: role in breaking barriers, enhancement of promotional opportunities, fostering of recruitment efforts, and support of career development. Mr. Mancuso's selection was based on his demonstrated commitment to women in Federal law enforcement. He implemented gender neutral assignment policies for all special agent positions within the DCIS. Under the management of Mr. Mancuso, numerous high level positions have been filled by women, including the Director, Investigative Support Directorate, Assistant Special Agents in Charge, Resident Agents in Charge, and others.

Donald Mancuso, Assistant Inspector General for Investigations, Office of Inspector General and Director, Defense Criminal Investigative Service, Office of Inspector General, Department of Defense.

Mr. Mancuso developed a program to use the GS-1801 investigative analyst series position as a bridge between the agent and non-agent positions within DCIS. He is responsible for hiring four women for these bridge positions. Recognizing the need to recruit more females and minorities from a cross section of society, Mr. Mancuso instituted a recruiting campaign that used professional organizations to assist in recruiting women and minorities for DCIS special agent positions. The effort resulted in the hiring of 5 African American and 11 white female special agents. Mr. Mancuso also recognized the need for increasing the opportunities for female special agents to attend training conferences, specialized schooling and career management training. He directed the establishment of a formal career progression training program for female special agents.

Mr. Mancuso was also instrumental in developing an Adopt-A-School program at Mount Vernon Elementary School in Alexandria, Virginia. This program provides male and female white and minority DCIS personnel for mentoring at an "at risk" school. The program also allows DCIS to foster a positive image for law enforcement and provides an opportunity to showcase females and minorities in successful non-traditional roles within law enforcement.

The WIFLE awards committee selected Mr. Mancuso for the Doris R. McCrosson Award because of his extraordinary dedication to the values of fairness and respect for women. He was cited for serving as an example to those whose efforts he leads. He was recognized as a proven leader, a consummate professional and an articulate and innovative manager who has made a significant and far-reaching contribution to the success of women in Federal law enforcement.

(continued on page 48)

Pictured left to right: Patrick J. Neri, Assistant Inspector General for Investigations; Susan Gaffney, Inspector General; Diane Hill, Special Agent, Boston District Office; and Raymond A. Carolan, Special Agent in Charge, Boston District Office; Office of Inspector General, Department of Housing and Urban Development.

The Julie Y. Cross Memorial Award

The Julie Y. Cross Memorial Award is given each year to a full-time woman law enforcement agent or officer in the Federal Government on the basis of her accomplishments in one or more of the following categories: an exceptional heroic achievement, sustained superior performance, or outstanding leadership qualities. Special Agent Diane Hill received this award for demonstrating a high level of dedication and commitment to her job through working fraud and embezzlement investigations related to HUD funds, as well as arresting drug dealers that plague public housing residents.

On one "Operation Safe Home" assignment, Agent Hill, assigned as a multi-agency task force member, was making drug buys in high density HUD subsidized neighborhoods. During one incident, she found herself having to assist an Alcohol,Tobacco and Firearms agent who had a weapon pointed at him. Agent Hill didn't hesitate to put herself at risk and went to the aid of the agent. The suspect eventually dropped the weapon and submitted to arrest. Agent Hill was recently recognized by the Boston Police Department for service above and beyond the call of duty for work she has accomplished as a team member of the multi-agency task force. The focus of the task force is to seek out and arrest violent fugitives residing in HUD-funded housing sites. Agent Hill has had a positive influence on the team and her demonstrated commitment to her colleague and housing tenants has netted a positive change at housing sites throughout the city of Boston.

In another incident, following the execution of a Federal search warrant for drugs in HUD public housing, two parents were arrested. Their child ran from the apartment into nearby traffic. Agent Hill comforted the child until the child was turned over to relatives. In the next morning's edition of a Boston newspaper, the raid was featured along with a photo of Special Agent Hill assisting the child.

Housing related law enforcement can be unique. Officers must have the ability to use force and discipline in executing search and arrest warrants in drug infested neighborhoods, and still show considerable compassion for innocent victims. Agent Hill has shown continued commitment and courage in her work and has been recognized by fellow agents and officers for these qualities.❑

This Gun For Hire

by George Opfer

George Opfer, Inspector General Office of Inspector General, Federal Emergency Management Agency

Just before dawn on August 25, 1992, Hurricane Andrew exploded on to the Florida coast with a vengeance, a short 25 miles south of downtown Miami. Andrew then tore across the rest of Florida with winds gusting up to 160 miles per hour and finally flew up the Gulf of Mexico into Louisiana and several other Southern states before again heading out to sea. In its wake, normal life as it was previously experienced seemed to have all but vanished. Andrew left behind many lost lives and incredible carnage. Thousands were made homeless and millions more faced weeks without power and utilities to their households. Water service was severely damaged and required heroic efforts to restore. Schools experienced extensive delays in opening, and local officials were required to impose a dusk-to-dawn curfew to protect against looting.

A brief 2 years later, on the other side of the continent, a second major natural disaster hit without warning. This time it was an earthquake and its target was Northridge, California. Again, as before, tremendous damage and disruption was left in its wake. Thousands were left homeless and the lives of several communities were turned upside down. Little did anyone realize that the recovery effort needed to restore normalcy would take many months to achieve and cost billions of dollars in Federal disaster funds.

As is the case following any major disaster, several hundred employees from various Federal and local agencies were immediately dispatched to the scene following both Hurricane Andrew and the Northridge earthquake to begin the arduous job of cleaning up. To assist in the monumental task of restoring order following these and other disasters, the Federal Emergency Management Agency (FEMA) had previously developed and put into operation the Disaster Assistance Employee (DAE) Program which established a permanent cadre of temporary employees recruited for a limited term of duty. These employees were considered to be "permanent, temporary" who were added to the ranks of FEMA full time employees on a time specific basis to assist in the essential functions of recovery following a disaster. They returned to their domiciles when their services were no longer needed. DAEs were hired and trained to perform disaster field activities directly related to specific disasters. They were not considered an alternative to using full time staff; but rather, they were an augmentation to full time staff solely for disaster related activities.

The authority for the DAE Program is found in Section 306(b)(1) of the Robert T. Stafford Act Disaster Relief and Emergency Act, Public Law 93-288, as amended, which states that Federal agencies, in carrying out the purposes of the Act may:

> "...appoint and fix the compensation of...such temporary personnel as may be necessary, without regard to the provisions of Title 5, United States Code, governing appointments in competitive service."

There were two categories of DAEs, local hires and reservists. Local hires were generally recruited locally and employed for a period of 120 days, which could be renewed if necessary. Reservists were maintained on the FEMA personnel rolls for a 24-month period expiring September 30 of every even-numbered year, but were automatically reappointed at the end of the 2-year appointment period, if needed. Salaries were set at the prevailing local rate, based on the specific duties of the job for the 2-year appointment period. All DAEs were ineligible for Federal health benefits, life insurance, and leave. Many, however, were covered by the Social Security System, therefore, deductions were regularly made to the Federal Insurance Contribution Act (FICA).

The FEMA Office of Inspector General (OIG) also deployed DAEs as auditors and investigators to participate in the recovery process. Numerous audit reviews and fraud investigations were conducted by OIG DAEs following Hurricane Andrew and the Northridge earthquake, resulting in 57 arrests and indictments, and significantly contributing to the OIG's collection of $5.6 million in fines, restitutions, civil judgments, cost savings and recoveries during that period of time. Much like full time OIG employees, DAE investigators received and assessed allegations of criminal conduct, performed interviews of witnesses and suspects, obtained and reviewed documentation, presented findings to the U.S. Attorney's Office, and assisted in any court related activities.

(continued on page 50)

The DAE program is now being replaced by a more updated version entitled Cadre of On-call Response Employees (CORE) Program. It has just recently been developed and implemented to address the need to staff fixed disaster sites with CORE employees as needed on a more permanent, sustained basis. Unlike in the past, Disaster Filed Offices (DFOs) such as in Miami, Florida and Northridge, California, remain open for much longer periods of time due to the extensive recovery activities needed. CORE staff members will now be recruited for a longer specific term and duty station, not to exceed 4 years, with possible 1 year extensions. CORE employees will be paid according to the General Services (GS) pay levels, and receive full benefits (health, life, retirement, and leave). Unlike the older DAE program, COREs will perform disaster specific assignments in which they have received more comprehensive training. CORE employees are still employed on an as-needed basis, performing disaster work on a time-limited appointment and may be released to a non-pay status when, and if, workloads decrease.

Recruitment for CORE criminal investigators will be generally focused toward experienced Federal law enforcement personnel, including military criminal investigative personnel who have substantial experience interfacing with the Department of Justice attorneys and are knowledgeable of the Federal Rules of Criminal Procedure. Extensive travel will also be required and applicants will be required to spend extended periods in tour-of-duty status. Applicants should have a completed Background Investigation or an update within the last 7 years and be in excellent physical health. In addition, CORE employees will work closely with other Federal law enforcement agencies and most particularly the Small Business Administration (SBA) OIG. Like full time employees, COREs will be deputized Special U.S. Marshals. Recruitment of COREs will begin in early March 1996.

In addition to the recruitment of CORE employees, FEMA has also established the Disaster Temporary Program which provides for the hiring of two other types of temporary employees with distinctly different purposes. The first type are intermittent employees who are primarily utilized for the initial surge staffing. These employees travel to disaster sites from their duty stations (where they reside) and are placed on per diem for the duration of their surge disaster assignment, similar to the former DAE reservist.

The second type are employees who are hired locally for a specific purpose at a fixed disaster site and for a fixed period of duty. These employees will not be on per diem but will be placed on the GS pay schedule and eligible to earn sick and annual leave during their appointment. Both types of employees will be given 1 year assignments with the possibility of a 1 year extension.

SBA’s OIG is also active in responding to disasters by providing loans to victims whose businesses or primary residences were damaged. In the past 5 years, SBA has approved over 213,000 loans for more than $6 billion in disasters such as the Loma Prieta and Northridge earthquakes, Hurricanes Hugo, Andrew, Iniki and Emily, floods in Southern California, Georgia and Texas and the Los Angeles wildfires and civil disturbances. As a result of this unprecedented loan activity, the Congress and the Office of Management and Budget provided the SBA OIG an additional allocation of funds to identify and prosecute fraud arising from these disaster loans.

The SBA’s OIG is utilizing these funds for criminal investigators and auditors on temporary appointments, primarily in Atlanta and Los Angeles. Since 1990, the SBA-OIG has opened 148 criminal investigations involving over 530 subjects with an estimated potential loss of approximately $63 million. Results of these investigations to date include 76 indictments and over $5 million in fines, restitution and penalties.

In the past, DAEs have proved essential to the successful carrying out of the FEMA OIG Mission to promote the economy, effectiveness, and efficiency within the agency while preventing and detecting fraud, waste, and abuse in agency programs and operations. CORE employees should prove a more cost effective way of accomplishing that mission in this time of dwindling budgets.

For more information regarding the Core Program, contact Paul J. Lillis, Assistant Inspector General for Investigations, or his Deputy, Francis W. Curran, at (202) 646-3894 ❑

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

UNITED STATES of AMERICA
EXECUTIVE COUNCIL on INTEGRITY & EFFICIENCY