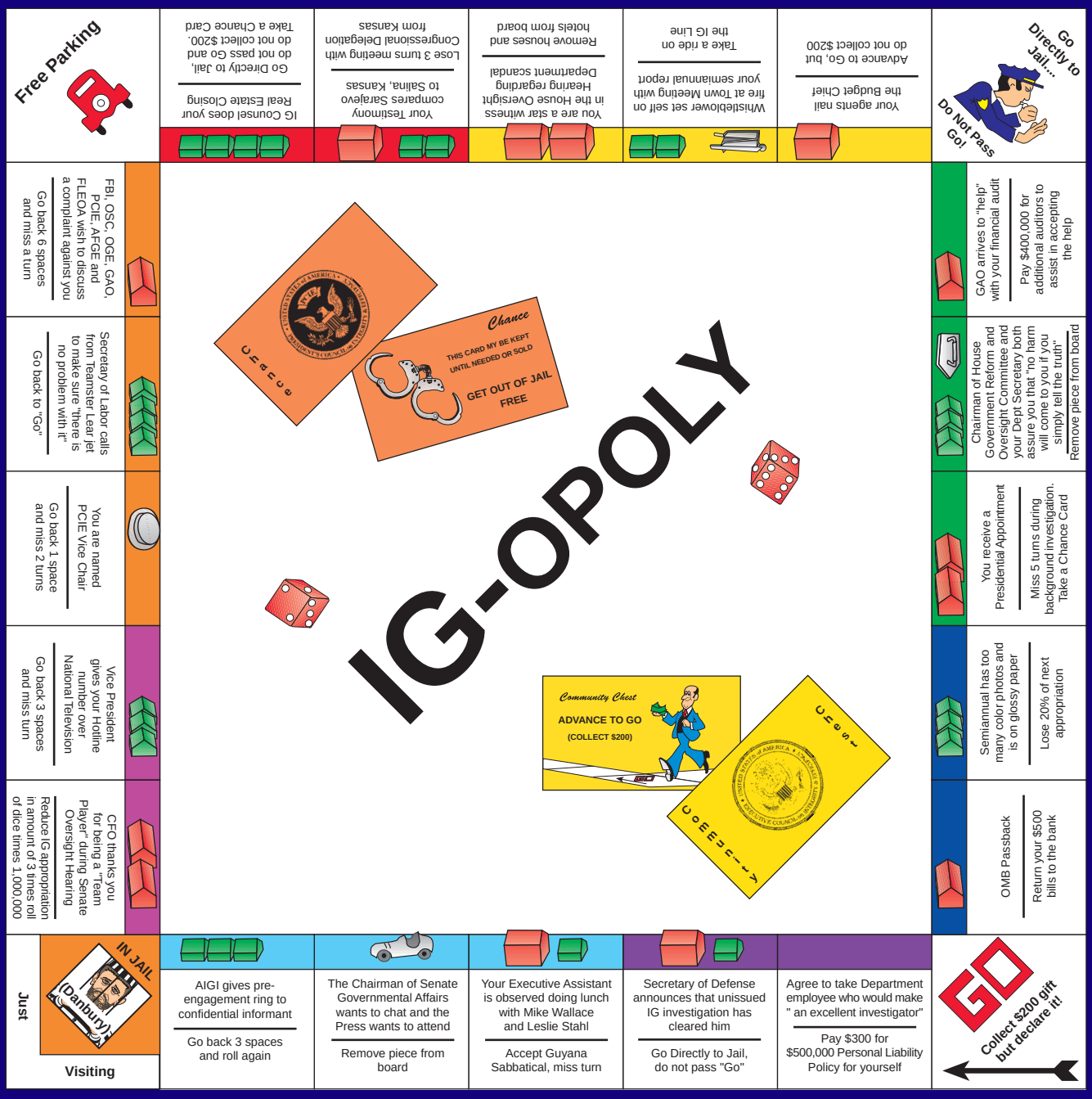
The JOURNAL OF PUBLIC INQUIRY

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES



SUMMER 1997

The Journal of Public Inquiry

Invitation to Contribute Articles

The Journal of Public Inquiry is a publication of the Inspectors General of the United States. We are soliciting articles from participating professionals and scholars on topics important to the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. Articles should be approximately 3–5 pages, single-spaced, and should be submitted to Agapi Doulaveris, Office of the Inspector General, Social Security Administration, Altmeyer Building, Suite 300, 6401 Security Blvd., Baltimore, MD 21235.

The JOURNAL OF PUBLIC INQUIRY

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

Table of Contents

IG Gate – Investigating Major Scandals:

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

Climate That Leads to IG Handling

by Michael R. Bromwich

In the following article, the first of a two-part series, Inspector General Michael R. Bromwich discusses the growing role of IGs in investigating major scandals. In the next issue of the Journal, *Mr. Bromwich will discuss the dynamics and mechanics of conducting a major scandal investigation in an article entitled, "Investigating Major Scandals: The Nuts and Bolts."*

Michael R. Bromwich,
Inspector General,
Department of Justice

Since the Ethics in Government Act was passed in 1978, as one of the lasting legacies of Watergate, Independent Counsels have become an accepted part of our political and legal culture. Iran-Contra, HUD, Whitewater — Independent Counsels appointed over the past 10 years have become synonymous with major investigative efforts undertaken in response to serious allegations of misconduct against high Government officials. Independent Counsels have become an important part of the institutional context within which serious allegations of misconduct are addressed. Indeed, one sure sign that allegations of misconduct have reached a critical mass or velocity is when the more general call for an investigation becomes a demand for the appointment of an Independent Counsel. This is the case whether or not the allegations bear any resemblance to the relatively narrow class of allegations that trigger the process by which an Independent Counsel is appointed.

Also in 1978, the Inspector General Act created Offices of Inspector General (OIGs) throughout the executive branch to promote the efficiency of the Government and to investigate allegations of waste, fraud and abuse. IGs have come to be relied on by their respective agencies and increasingly by the Congress to deal with a wide range of alleged misconduct, including misconduct by high-ranking agency officials. With the Inspector General Act Amendments of 1988, statutory IGs were created in, among other places, the Departments of Justice and the Treasury, which are the homes to the best known and most powerful law enforcement agencies in the country. In the last several years, some of the matters that have drawn the most public attention have dealt with the actions of law enforcement agencies. Ruby Ridge, Waco, Good Ol' Boy Roundup, Federal Bureau of Investigation (FBI) Laboratory — the need for aggressive and reliable executive branch oversight over powerful law enforcement agencies has been highlighted by such matters. Some of these matters have been handled by IGs; some have not. But the overall trend is plainly in the direction of having IGs conduct inquiries of this kind.

Over the course of the last 20 years, the two institutions — Independent Counsels and Inspectors General — have coexisted, each going about its own business. There has been much misinformation and confusion over the Offices of Inspector General, about what they do and about what matters they investigate. This confusion has been deepened by the sheer number of OIGs and the different kinds of activities — investigations, audits, inspections — that they conduct. Over the course of the past several years, various OIGs have conducted the kinds of high-profile matters normally associated with Independent Counsels. In my agency alone, in the past 2 years, we have conducted or are conducting eight such investigations, the details of which will be described in the next issue. I know that this is

(continued on page 2)

not a development restricted to my own agency, because four of the eight have been coordinated with or related to investigations conducted by other OIGs. Having served in Lawrence Walsh's Office of Independent Counsel: Iran-Contra, I have given some thought to what has caused the growing number of major OIG investigations and to the differences between OIG and Independent Counsel investigations.

Inspectors General and Independent Counsel: Convergence?

The fact that OIGs are conducting the kind of high-profile investigations normally associated with Independent Counsels suggests a convergence between the two institutions. While the strongest evidence of this convergence is the number and character of the investigations being undertaken by OIGs, in fact this supposed convergence between OIG and Independent Counsel investigations is more apparent than real. Despite public perception to the contrary, not every allegation of major scandal in an administration or in an agency is subject to the mechanism by which an Independent Counsel is appointed. Instead, the circumstances in which an Independent Counsel may be appointed are quite limited: 1) when there are specific and credible criminal allegations against so-called "covered persons" — i.e., high-ranking officials in the White House and in various departments and agencies of the executive branch; and 2) when the Justice Department's handling of such an investigation would result in a "personal, financial, or political conflict of interest."[1] Three of the four Independent Counsels appointed during the Clinton Administration have been appointed under the "covered persons" provision of the statute — those investigating allegations against former Secretary of Agriculture Mike Espy, former HUD Secretary Henry Cisneros, and the late former Commerce Secretary Ron Brown. The only Independent Counsel appointed under the conflict-of-interest prong relates to the Whitewater investigation.

There are various institutional and policy reasons why Inspectors General, as currently constituted, could not fully replace Independent Counsels. First, while OIGs have power to investigate many of the same matters that cause the appointment of an Independent Counsel, they have no power to prosecute. OIGs have to take their cases to prosecutors in the United States Attorneys' Offices throughout the country, to the Department of Justice's Criminal Division, or to the Criminal Section of the Department's Civil Rights Division, who make the ultimate decisions whether to bring criminal charges. The Independent Counsel statute is designed to shift responsibility for prosecutive decisions in a limited number of cases from the Justice Department to another institution having no personal or political connections to the officials under investigation. Having OIGs investigate such matters does not address the problem the Independent Counsel statute was designed to solve — the identity of the official making the ultimate decision whether to prosecute.

Second, because of the ongoing responsibilities of OIGs, it is difficult for them to juggle multiple resource-intensive investigations while at the same time successfully discharge their other responsibilities. While in the midst of several of these investigations at the same time, I have struggled with the conflict of wanting to make sure I devoted the resources necessary to conduct them well while at the same time making sure we do the other important work we were created to do. Special investigations are an enormous drain on scarce resources. In many cases it would not be possible for an OIG to ensure that the investigation be done as quickly or as fully as may be necessary. There are expectations both inside and outside of one's agency that OIGs will provide broad investigative and audit coverage of their departments; it is the rare case in which displacing resources from such continuing responsibilities is uniformly acceptable to the OIG's own agency, the Congress, or the public.

Finally, the jurisdiction of each OIG is limited to personnel in its agency as well as outsiders associated with its programs and operations. Many high-profile investigations are not neatly contained within an agency or department; they may involve allegations that cross agency boundaries and that involve non-governmental personnel who have nothing to do with the programs and operations of the agency. While we have had generally good experiences coordinating our investigations with other OIGs, it is plainly more difficult to conduct an investigation that exceeds the boundaries of one's own agency. In addition, the absence of testimonial subpoena power limits the ability of an OIG to gather evidence from witnesses outside the agency.

Increasing Resort to Inspectors General: The Reasons

Even though OIGs are not institutionally capable of displacing Independent Counsels, the undeniable fact is that many high-profile matters are being handled by OIGs. There are several reasons for this development. First, there is a greater recognition in the Congress that Inspectors General have the professional staff capable of undertaking such investigations and the objectivity and independence to ensure that the facts and nothing else drive the investigative results. To meet the demand for conducting complex investigations, I have recruited experienced former prosecutors to play key roles. This is both because of their experience as prosecutors in conducting lengthy and difficult investigations and also to enhance the written investigative report that is their final product. No matter how talented OIG investigators and other personnel may be, I believe that lawyers who are trained to synthesize large amounts of information and present it in a persuasive way constitute a

[1] The 1994 version of the legislation also authorized the appointment of an Independent Counsel when there are criminal allegations against a Member of Congress and when the Attorney General determines that it would be in the "public interest" for an Independent Counsel rather than the Justice Department to conduct the investigation. No Independent Counsel has been appointed under this provision.

vital resource in conducting such investigations. In our contacts with Congress, it has become clear that both Members and their staff are comforted by the fact that we are relying on experienced prosecutors to play significant roles in major investigations.

Second, the size of congressional staffs has generally declined over the past 4 years, while the amount of work to be done by both the House and the Senate has not. As a consequence, there has been a general decline in the ability both in the House and Senate to devote scarce congressional staff resources to undertaking major investigations. In addition, the number of personnel detailed from the executive branch to Capitol Hill who can assist in conducting legislative inquiries has dropped as the executive branch has shrunk. While there are obviously allegations of scandal — such as the current allegations of improper campaign fundraising practices in the 1996 election campaign — that cause Congress to mobilize its investigative machinery, the number of such congressional investigations has declined. The more that the Congress develops confidence in the ability of OIGs to conduct such investigations, the more comfortable it will be with monitoring the progress of such investigations rather than seeking to conduct parallel inquiries.

Third, Congress has seen the difficulties created by parallel executive branch and congressional investigations. In Iran-Contra, the grant of immunity by the select congressional committees to central figures including Admiral John Poindexter and Lt. Col. Oliver North ultimately doomed criminal cases brought by Independent Counsel Lawrence Walsh. That vivid memory has led Congress in various instances to stay its hand and to delay the commencement of a congressional inquiry, condense its scope, or both. When we investigated allegations that high-ranking Immigration and Naturalization Service officials deceived a delegation from the Congressional Task Force on Immigration Reform on a fact-finding trip to Miami in June 1995, we had to deal with Congress's desire to hold hearings on the same subject while our investigation was still in progress. Ultimately, Congress agreed to delay hearings that would have greatly complicated our investigation, even though our investigation took nearly a year to complete. Because of the thoroughness and power of our investigative report, Congress ultimately held only a brief hearing at which we reported our investigative results.

Fourth, Congress has recognized that Inspectors General, unlike Independent Counsels, are accountable to Congress. OIGs depend on Congress for funding and are subject to its oversight. This ongoing relationship with Congress means that OIGs must take account of their congressional audience. Many of the major investigations undertaken by my office over the past 2 years have been the result of congressional requests. In other cases, even when the initiation of the investigations has had a different cause, as in our Federal Bureau of Investigation Laboratory investigation, congressional committees have expressed substantial interest in them, have monitored their progress, and in some cases have held hearings when they are completed. Although this relationship between OIGs and Congress could in unscrupulous hands lead to the slanting of investigative results to please a congressional audience, an OIG's long-terms interests will be to temper responsiveness to Congress with a dedication to calling them as they see (and find) them, regardless of Congressional reaction.

Inherent Strengths of Inspector General Investigations

In addition to the explanations offered above for the growing resort to OIGs to conduct sensitive and complex investigations, other factors make it likely that this trend will continue.

First, OIGs have a very substantial advantage in conducting investigations within their agencies based on their strong working knowledge of those agencies. Over time, as an institutional matter, OIGs accumulate a substantial store of institutional knowledge about the way their agencies operate. This knowledge includes the way the agencies' programs work, the way its components work with each other, and the management weaknesses that may already have been studied. When we conducted an investigation into allegations that INS managers deceived a delegation from the Congressional Task Force on Immigration Reform during a fact-finding trip to Miami in June 1995, we could deploy a group of agents and auditors with an extremely strong working knowledge of INS. This knowledge facilitated our investigation in countless ways.

Second, OIGs have employees with varied skills and backgrounds who can contribute to the investigative effort. Investigators, auditors, inspectors, and program analysts may all be capable of making distinctive contributions to a complicated investigation. This can be an enormous advantage when compared, for example, to the need for Independent Counsels to build their staffs from scratch. In complex white-collar investigations, prosecutors frequently seek to obtain the assistance of Internal Revenue Service (IRS) agents to get sophisticated documentary and financial analysis. In my experience, auditors, inspectors, and program analysts have many of the same strengths as IRS agents in being able to comb through and make sense of large numbers of complex documents. Although investigators, auditors, and inspectors have different training, I have found the marriage of their different skills and experiences to be extremely valuable in conducting special investigations. This also provides excellent team-building opportunities for employees who may never have worked with personnel from other parts of the OIG.

Third, OIGs are able to conduct their investigations in ways that ensure that Congress and the public receive the full story of the investigations and the facts found. The purpose of criminal investigations is to determine whether anyone has committed a crime and to bring prosecutions where there is adequate evidence to prove guilt beyond a reasonable doubt. The criminal charges that may result from an investigation may involve only a small percentage of the information that is collected during the investigation.

(continued on page 4)

Introduction of evidence at any trial may be deemed irrelevant to proving specific charges against specific defendants — and yet such evidence may be extremely important in telling the story that puts the activities of the defendant(s) in context. In addition, prosecutors may decide not to pursue certain lines of inquiry because they hold no prospect for developing admissible evidence. Yet those lines of inquiry may be extremely important in drawing a complete picture of the events that gave rise to the request for the investigation. Although Independent Counsels are required to file periodic reports and a substantive final report, the final report is necessarily focused on the path of the criminal investigation, which may not present the full picture of relevant facts.

By contrast, Inspectors General are free to structure and direct their investigations as they deem appropriate and to take an exhaustive look at relevant facts rather than limiting themselves to evidence that can be used in a criminal prosecution. This greater flexibility is extremely useful in providing an accounting of what occurred to agency heads, Congress, and the public. When we were asked to review the role of Justice Department personnel in the Good Ol' Boy Roundup, it was clear that the likelihood that any Justice Department personnel committed any crimes in connection with attending the event was slim. The primary concern of the Attorney General and the Senate Judiciary Committee was whether Justice Department employees engaged in any incidents of racial and other misconduct. Our lengthy report told the story of the Good Ol' Boy Roundup over 16 years, a narrative of historical reconstruction that no criminal prosecution could have accomplished.

Fourth, in the face of allegations of serious misconduct, OIGs may investigate the conduct of personnel ranging from the head of the department or agency down through the ranks to include any employee. OIG jurisdiction includes within its purview misconduct at every level. While the net of Independent Counsel investigations can be cast quite broadly — as the Iran-Contra and Whitewater investigations have been, to provide two examples — it frequently is limited to a single named individual. More importantly, the scope of the Independent Counsel's investigation is framed by the court order appointing the Independent Counsel and the Independent Counsel's construction of that order. Generally, such orders are framed broadly enough to enable the investigation to include not only the named individual or individuals but also those who were involved in the alleged misconduct, but much is left to the discretion of the Independent Counsel. Because ultimately the Independent Counsel is not accountable in any meaningful way to the agency in which the misconduct took place or to the Congress, there is little leverage to ensure that the investigation is framed broadly enough to serve the oversight interests of the Congress and the management interests of the agency.

Fifth, OIG investigations are able to help ensure that agency personnel are held accountable by their continuing presence within the agency. When prosecutors investigate the conduct of agency personnel, their interest frequently begins and ends with their investigation. Prosecutors have no continuing oversight responsibilities over an agency or a part of an agency. It is no part of their mission to improve the operation of Government programs and operations, except insofar as removing corrupt officials accomplishes that purpose as a by-product of the investigation. And in cases where prosecutors develop some evidence of misconduct but not enough to indict those who engaged in it, the ability to take appropriate administrative action is handicapped by the lack of interest prosecutors generally have in the agency administrative process. This general proposition is even more true of Independent Counsels than it is of other prosecutors. They are created for one mission and one mission only; the institution is then disassembled and ceases to exist. Continuing oversight, to the extent it is provided at all, must come from Congress or the agency within which the scandal occurred.

OIGs are quite different in this respect. Although most of the Justice OIG's cases begin as criminal investigations, the distinct minority go forward as criminal prosecutions. A substantial percentage of our caseload is made up of administrative matters that are ultimately referred back to the employing agency for appropriate administrative action. Because of the continuing mission and presence of the OIG, and its broad responsibilities for oversight within the agency, it has an interest in making sure that misconduct investigations are taken seriously by the managers responsible for imposing discipline. If they are not, OIGs have the ability to expose the failure to take appropriate administrative action and to report the failure to Congress and the public. Thus, even where an investigation does not lead to prosecutions, it can serve to ensure that a broad range of agency employees are held accountable. Moreover, IGs make important recommendations for improving the operation of their agencies based on an individual investigation or a series of investigations that has revealed vulnerabilities in the agency's programs or operations. The business of Independent Counsels is limited to taking or declining to take prosecutive action.

Conclusion

The adversary culture that exists in Washington virtually guarantees that allegations of misconduct and gross mismanagement will be directed with great regularity against high-ranking Government officials and controversial Government programs. This is particularly true given the larger trends towards downsizing of Government and the continuing search for wasteful and expensive programs — and in some cases entire agencies — to abolish. Nothing can end a program faster than an investigation that finds it riddled with corruption and characterized by waste and inefficiency.

Because of our independence, autonomy, and other unique institutional advantages, OIGs will continue to receive requests from the Congress and the public to undertake major investigative efforts in high-profile matters. The irony is that the better we acquit ourselves in conducting such investigations, the more likely we are to unleash a torrent of similar work that we may lack the resources to do.❑

Customer Dissatisfaction

by: Sherman M. Funk

Sherman M. Funk, Former Inspector General, Department of State and Arms Control and Disarmament Agency

The normal run of Inspector General (IG) investigative work deals with the detritus of bureaucracy: abuse of power by mid-level officials, false statements on forms, theft of Government money or equipment, fraudulent billings, fraudulent use of Government payments, Hatch Act violations (referred back by the Special Counsel), misuse of Government vehicles or other Government equipment, fraud against the Government by contractors and grantees, etc. Few of these crimes, misdemeanors, and administrative abuses attract significant attention by the media, or on the Hill, or even by senior agency management.

IGs are always irritated when those matters that should generate "outside" interest rarely do so, such as audit, inspection or investigative reports citing wasteful or badly managed programs and operations which cost the taxpayers millions of unnecessary dollars. To be sure, there are a few dogged reporters and a handful of legislators who regularly read or are briefed on IG reports, but their accounts or speeches about waste tend to be ignored. And yet, IGs are frequently used to crack down harder on corrupt Government employees.

The dirty little secret of IGs, however, is that the vast majority of Federal workers are honest, want to do a good job and, as a group, generally are no less efficient that their counterparts in the private sector — despite their having to live with a number of silly and nitpicking regulations which corporate America would not tolerate internally for a moment.

When they have time to think about it, IGs view themselves as conscientious doers of good deeds, dealing daily with what is, in effect, a small but persistent Federal underworld. Their successes usually elicit no glory and few plaudits. It is little wonder, then, that IGs (who, popular conceptions to the contrary, are quite human) dream of taking on a major scandal. They know that the huge publicity arising from such an event will catapult them into their 15 minutes of fame; more important, it will boost the morale of their staffs. They also sense, assuming no repeal of the Law of Averages, that sooner or later this Big Scandal will erupt in their agencies. What they don't know is that when it does, and they have to investigate it, their work will bear out Clare Booth Luce's classic dictum, "No good deed goes unpunished."

The blunt truth is that a truly major scandal in a Government agency which attracts wide media attention, both print and TV, is likely to incorporate political aspects which also attract congressional attention. That, in the nature of things, generates partisan political attention. Given sufficient media and partisan heat, and the involvement of an EX-2 or higher level appointee, the distinct possibility exists that an Independent Counsel will be reviewing the investigation at a later date.

What does all this mean to the IGs? Some of the answer depends on how the relevant investigation was initiated.

Often, an agency head faced with a public outcry or unofficial congressional request (both usually arising from a media story, which in turn usually derives from a leak within the agency), refers the matter to the IG. Because the agency's spokesperson, anxious to deflect heat from his or her boss, is quick to inform the media of this referral, reporters now focus their quest for information on the OIG. In other cases, the IG may have opened an investigation as soon as the potential problem surfaced in media accounts, or earlier, on the basis of internal information obtained by the OIG; in either situation, the agency's spokesperson or the OIG press officer can simply confirm that an investigation is already underway. Also, it is not unlikely that the IG may have had an investigation of this or ancillary matters ongoing for some time, but did

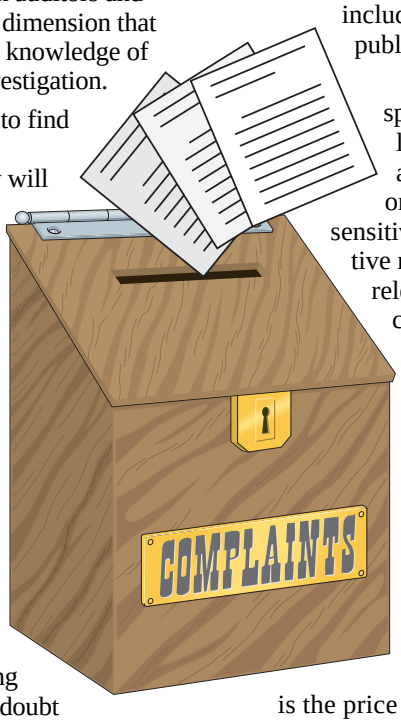
(continued on page 6)

not recognize its Major Scandal potential until the media storm broke. Here too, the appropriate procedure would be a simple acknowledgment that the investigation is in progress — although it might not be injudicious to add that the review had begun some time earlier. An occasionally implied boast is not always out of order.

Regardless of how or when the investigation originated, certain measures should be taken as soon as it is recognized that the OIG has a Major Sandal on its hands. The IG must immediately assume that every bit of data related to the investigation will be microscopically analyzed before long by reporters, congressional staff, legal experts, and eventually the public. This includes interview notes, investigative procedures, methods of review, possible referrals to Justice — everything. All of this may never surface, but it should be assumed that it will and care taken accordingly.

What this means in practice is that only the very best investigative talent should be assigned to the case. If the matter had been initially handled, when it was opened, by agents not in the first rank (and quality is the issue here, not seniority), they should be supplemented by others. Where appropriate, it is a good idea to add top-notch auditors and inspectors to the team; they provide a useful dimension that may prove invaluable if financial analysis or knowledge of programs is a requisite component of the investigation.

Accept as a given that reporters will try to find out what your team finds out, while they are finding it out, if not immediately after. They will interview, or attempt to interview, all of the IG sources; they will obtain, or try to obtain, all of the documents the team obtains. Inasmuch as they lack subpoena power, they will do this through persuasion, appeals to patriotism, bold-faced intimidation and, in the case of some tabloids, appeals to greed. Never underestimate the quality of reporters. Many of them, particularly from the major newspapers and wire services, will be knowledgeable, smart, and tough. And never underestimate the impact of a TV reporter and a cameraman appearing at the office desk or home front door of a source. If the latter is torn between fear of responding to questions on camera and the prospect of being seen nationally on network news, have little doubt of the decision. Thus, whatever transpires between OIG agents and subjects or sources may well be known publicly before it even reaches the IG.



It goes without saying, but it should be said anyway: investigative team members should be cautioned not to discuss the case with anyone outside the OIG. Anyone, including family and friends. The author is not aware of any investigative leak ever coming from an OIG, although when leaks do appear (usually from sources), most people will automatically accuse the OIG. All the OIG can do about such accusations is hunker down and circle the wagons. It comes with the territory.

IGs, no less than other Government officials in this age of reinvention, must strive for customer satisfaction. The special problem facing IGs is that while it is easy to identify who their customers are, it may be hellishly difficult to determine what information should be available to them. On a narrow basis, all personnel in the OIG's agency, from the Secretary/Administrator on down, are IG customers. They have a right, regardless of grade or position, to expect courteous, respectful, and professional conduct from all OIG employees. They have a right to expect searching, independent, objective, professionally competent, and yes, tough audits, inspections, and investigations. That much is beyond question.

But the IG's customer base is wider than the agency. It includes the Department of Justice, other Federal, state, and local law enforcement agencies, other OIGs, the Office of Special Counsel, Office of Government Ethics, professional organizations (e.g., Association of Government Accountants, Federal Investigators Association, American Institute of Certified Public Accountants, Institute of Internal Auditors). Because we live in a democracy where the people and the people's representatives have a basic right to know, it also very much includes the print and TV media, the Congress, including congressional staff and the GAO, and the public at large.

It is this wider customer base which poses the special problem. Obviously, unclassified published audit and inspection reports should be available to anyone who wants a copy, subject only to possible deletion of some procurement-sensitive material. Obviously too, completed investigative reports, suitably redacted for privacy reasons, are releasable. But IGs have an obligation to maintain confidentiality of certain investigative procedures, and to protect sources, especially whistleblowers. When the media are denied full access to all data, or when a congressional staffer is told he or she cannot receive copies of raw interview notes, the IG will have dissatisfied customers. When a senator or representative is told that a particular request must come from a full committee chair, the IG will have another dissatisfied customer. When citizens submit requests for privileged data and are denied, there will be more dissatisfied customers. Such dissatisfaction is the price of being an IG, whose objective should be to gather and report facts, not to be widely loved, or to give away the store trying to placate a vociferous few. Indeed, if either of the latter two is true, the IG is the wrong person for the job.

But it gets worse. If the scandal reaches major proportions, the heat will intensify, particularly if it has (apparently) a political dimension. During the investigation of the Clinton passport matter, the author was called by several Democratic Hill staffers, and by at least two Democratic Members, all of whom issued stern warnings that he should not try to cover up misconduct by the Bush Administration. After he held a press conference upon

publication of the report, during which he said that the passport search was not an organized effort by the White House to uncover dirt on Clinton, Democratic Members accused him flatly of a sell out to protect his job. One year later, ironically, when the author's staff investigated a case where mid-level Clinton appointees rummaged through files of senior Bush Administration appointees and leaked information from them, public accusations were made by Republican Members that he had sold out to the Clinton Administration to keep his job, even though the report recommended, and the Secretary approved, dismissal of the offending officials. No apologies were made in either case when the validity of both reports became apparent. Nor were apologies made by newspapers that had editorialized in error about the author's alleged surrender first to Republican and then to Democratic demands that an investigation should have preordained conclusions.

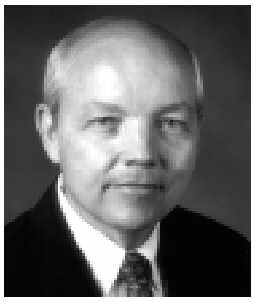
Interestingly, the first press conference ever held by the author as IG concerned an investigation about the leak of economic indicators in advance of their official release. By any definition, this was far more significant than either of the above cases. Billions of dollars on the bond market moved within hours of the leaks; unless the leakers could be identified quickly, the very integrity of Federal statistics was at issue. An all-out investigation, conducted jointly with the Securities and Exchange Commission, resolved the problem. No politics, no senior appointees involved, no "sex" appeal and, at the press conference, virtually no questions. But that was only a scandal, not a Big Scandal. If IGs encounter the latter, with all its hue and cry, the author suggests that their attitude--assuming they are satisfied that they have conducted a comprehensive and professional investigation--should be, to paraphrase Shakespeare, "If this be customer dissatisfaction, make the most of it."

Or, if they are unable to withstand the extent of the dissatisfaction, adhere to Harry Truman's immortal "If you can't take the heat, get out of the kitchen."❑

Statement of John A. Koskinen Before the House Committee on Government Reform and Oversight, February 12, 1997

The Government Performance and Results Act (GPRA) of 1993 requires agencies to develop and institutionalize processes to plan for and measure mission performance. GPRA was enacted 3 1/2 years ago as the result of a bipartisan effort in the Congress, with the support of the Administration, to increase the focus on the results from Government programs and activities. At its simplest, GPRA can be reduced into a single question: What are we getting for the money we are spending? To make GPRA more directly relevant for the thousands of Federal officials who manage programs and activities across Government, GPRA expands this one question into three: What is your program or organization trying to achieve? How will its effectiveness be determined? How is it actually doing? One measure of GPRA's success will be when any Federal manager anywhere can respond knowledgeably to all three questions.

On February 12, 1997, John A. Koskinen, Deputy Director for Management, Office of Management and Budget (OMB) testified before the House Committee on Government Reform and Oversight on the Administration's progress to date in meeting the requirements of the GPRA. The Journal *is providing the text of Mr. Koskinen's testimony for Federal managers information.*



John A. Koskinen,
Deputy Director for Management,
Office of Management and Budget

Mr. Chairman, I am pleased to appear before the Committee this morning to discuss the importance to the Government and the public of the Government Performance and Results Act of 1993 (GPRA) and to provide an assessment of our progress to date in meeting its major requirements. GPRA was enacted 3 1/2 years ago as the result of a bipartisan effort in the Congress, with the support of the Administration, to increase our focus on the results from Government programs and activities. This Committee was one of the leaders in the passage of the Act and we look forward to continuing to work with you and the Congress as we implement this significant legislation.

At its simplest, GPRA can be reduced to a single question: What are we getting for the money we are spending? To make GPRA more directly relevant for the thousands of Federal officials who manage programs and activities across the government, GPRA expands this one question into three: What is your program or organization trying to achieve? How will its effectiveness be determined? How is it actually doing? One measure of GPRA's success will be when any Federal manager anywhere can respond knowledgeably to all three questions.

But having answers to these questions is of great interest to the public as well. As a Government, we face major challenges. This is a time of great fiscal constraint. Tight budget resources demand that every dollar count. During a period of much public skepticism about the Government's ability to do things right, the Government must not only work better, but be shown as working better, if we are to regain public confidence in this institution. We must chart a course that not only sustains our delivery of services to the public, but improves on that delivery while meeting the rightful expectations of its citizens to be treated fairly, responsively, and with good effect. GPRA, if successfully implemented, will support such a result.

Let me now briefly summarize those aspects of GPRA implementation that are our most immediate focus.

Basic Requirements and Timetable

Strategic plans

The basic foundation for what agencies do under GPRA is the agency strategic plan. Agencies are required to send their strategic plans to Congress and OMB by this September 30. When developing its strategic plan, an agency is to consult with Congress and solicit and consider the views of those parties interested in or potentially affected by a plan. OMB has encouraged agencies to begin this consultation soon.

(continued on page 10)

Our guidance to the agencies on preparing and submitting strategic plans notes that the agency letter transmitting the plan to Congress and OMB should describe the consultation that was done, as well as summarizing any views of those outside the Executive branch that present a contrary view to the basic direction of the plan as completed.

The strategic plan spans a multi-year time frame, and is required to include a mission statement, a set of general goals and objectives, and a description of the linkage between these general goals and objectives and the performance goals that will appear in the annual performance plan. The mission statement sets forth the basic purpose for what an agency does programmatically and operationally. The long-term general goals and objectives define what the agency intends to achieve over the time period of the plan, to further its overall mission. The linkage between long-term goals and annual goals is important because the annual goals are commonly used to measure progress in achieving the general goals and objectives.

OMB issued guidance to the agencies in September 1995 on the preparation and submission of strategic plans. This guidance resulted from an OMB/agency collaboration during the Spring and Summer of 1995. In the Summer of 1996, OMB conducted a comprehensive review of the agency strategic planning efforts and the status of their plans. The review's objective was to gauge agency progress in preparing their strategic plans and to identify any concerns with the plans themselves or the process being followed. Agencies provided OMB with certain key parts of their plan for this review which were in a draft or developmental state.

Generally, the agency plans reflected a serious effort and allowed us to conclude that agencies should be able to produce useful and informative strategic plans by this Fall. The review also revealed several challenges. Last summer, most agencies were only beginning to link the general goals and objectives of their plans with the annual performance goals they would be including in their annual performance plan. Further inter-agency coordination on programs or activities that are cross-cutting in nature was necessary and the senior leadership in some agencies had yet to become fully involved in the planning process.

Since then, OMB staff have continued to interact with the agencies as these strategic plans have evolved and we will undertake another systematic review of the agency strategic plans this spring.

Annual Performance Plans

Pursuant to the statute, the first of the agency annual performance plans will be sent to OMB this September. These plans will be for Fiscal Year 1999, and will be submitted with the agency's budget request for that year. The annual performance plans will contain the specific performance goals that the agency intends to achieve in the fiscal year. The statute provides that a subsequent iteration of the annual performance plan is to be sent to Congress concurrently with release of the President's budget.

The agencies and OMB gained valuable experience in preparing annual performance plans through the pilot project phase of GPRA. The statute wisely provided an opportunity for all 14 Cabinet Departments and an equal number of independent agencies to experiment with the implementation of the statute. Over 70 individual pilot projects were established, ranging in size from the entire Internal Revenue Service to small offices and programs within a larger bureau. The performance measurement pilot project phase of GPRA concluded in FY 1996. OMB's May 1997 Report to Congress on GPRA will describe this pilot project phase in greater detail.

In September 1996, OMB initiated a special review of the performance goals that agencies proposed to include in their annual performance plans for FY 1999. This review is still ongoing. The agencies are providing OMB with descriptions of their proposed performance goals, illustrating what will be measured and the nature and type of measurement.

The timing and sequence of these two reviews, one in the Summer of 1996 and the other in the Fall, was by design. The Summer Review concentrated on strategic plans, which are the starting point for annual performance plans. A strategic plan is like a compass pointing to what an agency seeks to achieve over the long-term. Without such a compass, it is difficult to judge whether the annual performance goals are appropriate.

Our experience with the pilot projects and with Summer Review underscored the importance of having a review focused on the annual performance goals. Gaining an early consensus on these goals will not only help assure that they are appropriate and relevant but will allow agencies to measure current performance, creating a baseline from which to set future performance levels or targets.

In another joint collaboration with the agencies, OMB is preparing guidance on the preparation and submission of annual performance plans for FY 1999. The drafting of this guidance is largely complete and the guidance will be issued soon and we expect agencies to produce useful and informative annual performance plans for FY 1999.

Government-wide performance plan

GPRA requires that a Government-wide performance plan be annually prepared and made part of the President's budget. The Government-wide performance plan is based on the agency annual performance plans. The first Government-wide plan will be sent to Congress in February 1998, and cover FY 1999. We will soon begin an effort to design this document, determining what should be included and how it should be presented. In this regard, we would welcome your views on those features that you believe would make this document informative and useful to the Congress.

Program Performance Reports

The agency's program performance report is the annual concluding element of GPRA. These reports are required within 6 months of the end of a fiscal year, and compare

actual performance with the performance goal target levels in the annual performance plan. Where a goal was not met, the agency explains why and describes the actions being taken to achieve the goal in the future. The first program performance reports, for FY 1999, are to be sent to the President and Congress by March 31, 2000.

The performance measurement pilot projects are being used as a test of the program performance reports, and the ability of agencies to generate timely and accurate actual performance data. OMB is considering integrating the GPRA program performance report with each agency's audited financial statement and several other periodic reports to create a single agency accountability report. We expect that the OMB Report to Congress in May will further outline proposals for such a single report.

OMB's GPRA Effort

The OMB-led reviews I have previously outlined are part of the Administration's overall effort to ensure successful implementation of GPRA and indicate the great importance we attach to this effort. Two OMB-wide forums dedicated to performance and GPRA preceded the Government-wide reviews begun last summer. These forums were used to familiarize all OMB staff with the statute and its requirements and to draw upon their experience and suggestions for how it might be successfully implemented. The magnitude of GPRA, its encompassing scope, and its integration with the budget dictate that every major organizational component within OMB have some role in its implementation. To advance the concept of OMB-wide responsibility for GPRA, OMB established a GPRA Implementation Group, whose members are from every OMB office and comprise nearly 10 percent of our total professional staff. The Implementation Group meets regularly to discuss and review GPRA implementation tasks and policies.

In many ways, the best training is having to do it yourself. OMB has been working on its own strategic plan for nearly a year, an effort that has involved all parts and levels of the organization. Later this month, OMB will have a day-long "stand-down" in which all staff will focus on our strategic plan and the goals we propose to establish for our organization.

Valuable help for our Government-wide implementation effort is also coming from several interagency councils which I chair. These are the President's Management Council, whose members are the agency Chief Operating Officers (generally the Deputy Secretary); the Chief Financial Officers' Council; and the President's Council on Integrity and Efficiency, comprised of the agency Inspectors General. Each of these councils has taken leadership for one or more aspects of GPRA implementation, and have developed and disseminated useful techniques and practices to assist the agencies. They are also helping us to develop a unifying framework for bringing together the various laws and initiatives that focus on performance. These include GPRA, the Government Management Reform Act, the Chief Financial Officers Act, the Federal Acquisition Simplification Act, the Federal Managers' Financial Integrity Act, the Inspector General Act, the Clinger-Cohen Act, as well as initiatives originating from the National Performance Review, such as development of customer service standards and performance-based organizations. There is consensus that this integration must be done, and, to the extent practicable, must be meshed into the processes supporting budget preparation, decisions, and execution.

To do this will be a formidable task. But we have no real choice. If managed separately, these various endeavors will lose the synergy and economy of effort that would result from their being fitted together. Failure to coordinate and integrate these laws and initiatives can undercut their effectiveness, create confusion, and introduce frustration and ultimately disinterest among all parties. Put starkly and simply, there are not enough resources within the executive branch to even try carrying out these activities in a non-integrated way.

Sorting through the complexity of these varying performance initiatives has been difficult, but we are making progress in defining a framework for this integration.

Expectations

As noted earlier, we expect agencies to provide useful and informative strategic and annual performance plans within the timeline specified by the Act. However, preparing a good GPRA plan is not an easy task. Indeed, a plan easily prepared is likely to be a superficial plan. Therefore, no one should expect the first plans to be perfect. We should view these first plans as the beginning of a process of improvement and refinement that will evolve over several years. Measures will be modified, better and more appropriate goals will be defined, and performance data will increase in both volume and quality.

Even as performance measures become more refined, we should always bear in mind that using performance measures in the budgeting process will never be an exact science, or even a science at all. Often, an under-performing program will benefit from additional resources, not fewer. Comparing results across program lines will always require political judgments about the relative priorities, for example, of programs for highways and education. And we should not lose sight of the fact that performance information will often be used to adjust the way programs are managed rather than to change the resources provided. Accurate, timely performance information is important in all these situations and this is why the Administration is committed to the successful implementation of GPRA.

As I have said on other occasions, if we are successful, over time, GPRA should disappear. Some may think such a declaration flies in the face of the enthusiasm of this Administration for GPRA. However, if GPRA works as

(continued on page 12)

envisioned, Government managers will absorb it into day-to-day agency administration and program management. For this to happen, we must guard against creating a separate GPRA bureaucracy in each agency that provides the documents and information required by the statute in an effort that is divorced from this day-to-day management of the agency. That's why I suggest that the true measure of the success of GPRA will be the extent to which the concepts of management and good business practices set out in this law become the accepted way that the Government works without reference to any particular statutory framework or requirements.

Conclusion

This concludes my statement, Mr. Chairman. I'd be pleased to take any questions you may have.❑

GPRA: A Catalyst for Enhanced Federal Management Processes

by Thomas G. Kessler and Thomas G. McWeeney

Thomas G. Kessler, DBA, Associate Professor for Central Michigan University's College of Extended Learning

Thomas G. McWeeney, PhD, Executive Director of the Center for Strategic Management

For decades, the Federal Government has relied on the annual budget process as its principal means of resource forecasting, allocation, and control. Although this long-revered process has been mildly criticized over the years, it continues to serve as the "cornerstone" of agency planning and management processes. The Government Performance and Results Act of 1993 (GPRA), however, is intended to substantially change Federal management and accountability processes and practices by requiring agencies to develop strategic plans, link them to budgets, and identify, measure, and report on results. Expectations for this important legislative reform are high: it is anticipated that GPRA will dramatically transform the management operations of most Federal agencies. Consequently, the annual budget process, as an integral component of agency planning and management processes, will undoubtedly be subjected to significant scrutiny and revision as GPRA implementation proceeds.

In order to understand the rationale driving the reform movement, we must analyze traditional Federal planning, budgeting, and performance reporting processes to understand their deficiencies and impetus for reforming them. The purpose of this article is to present an assessment of those processes, outline intended GPRA reforms, and clearly show how they will lead to improved Government operations. Offices of Inspector General can benefit by examining their constituent agency processes and their own internal processes to determine how these reforms will impact activities and operations and take steps to plan and incorporate necessary changes.

The Planning Process

Most Federal agencies and programs engage in some form of strategic planning. To do otherwise would subject them to potential ridicule and criticism for lacking long-range focus and direction. The plans describe external and internal influences, outline mission requirements, list goals and objectives, and identify actions and assignments necessary to meet the goals and objectives.

Research and experience suggests, however, that strategic plans typically are not linked to tactical plans or budgets and do not drive day-to-day organizational activities. Strategic goals and objectives are significantly different from tactical ones, and do not have the same level of urgency or pressure. Tactical activities quickly overtake managers and staff and long-range strategies and tasks are put on hold until there is more time to focus on them. All too often, that time is never available.

Performance Measures

Managers and supervisors are paid to remove obstacles to success, ensure that productivity is high, and "get the job done." They coordinate resources, oversee activities, and produce outputs. Their focus is on managing inputs (labor hours, contractors, travel funds, training, etc.), ensuring that activities are accomplished (projects, initiatives, investigations, audits, processes, etc.), and producing outputs (briefings, reports, regulations, memoranda, arrests, indictments, loans, patents, etc.). Success is measured in terms of meeting planned milestones, using resources optimally, producing a high number of outputs, and producing "high-impact" outputs.

Although these foci seem natural and rational, they lack sufficient emphasis on outcomes and impact. Recent emphasis has been placed on determining if Federal program outputs are achieving their desired impact. For example, Federal efforts to address violations of drug and narcotics laws have resulted in a steady increase in the number of arrests and convictions. Yet the substance abuse problem has not been solved and, in fact, has worsened in recent years. Is continued Federal attention warranted? Outcome-based performance measures enable this problem to be examined from many angles. Are the current strategies effective or should they be adjusted? Are Federal programs focused on the correct core issues? Could the problems be more effectively addressed at the state and local government level? This example demonstrates that output-based performance measures do not provide adequate information for such analysis.

(continued on page 14)

Budget-Based Management

Agencies rely on the annual budget process to forecast, allocate, and control resources. Budget requests are carefully scrutinized by budget analysts, challenged for validity and rigor, and sent forward for senior management consideration only after questions have been adequately addressed. Agency decision-makers review individual program budgets and assess the aggregate budget package. Adjustments are made and the final package is sent to the Office of Management and Budget and, eventually, to the congressional appropriations subcommittee.

Managers use past experience, knowledge of program subject matter, and expectation that workload will remain the same or change, to formulate their budget request. Budget forecasting, however, given the long lead-time required for review and deliberation in the public sector, is decision-making under conditions of uncertainty. Consequently, managers mitigate budget-related program risks by anticipating discretionary funding categories that can be used for unexpected contingencies. As unexpected demands are placed on program resources, budget "games" are used to ensure that program priorities are addressed.

Budget "games" involve shifting funds from object/sub-object classes that have excess funds to those that do not have adequate funding. For example, when staff resign and their positions are vacant the salary that is not expended is accumulated. These lapsed salary funds can subsequently be shifted to cover shortfalls in other areas such as contractual funding, travel, or training. This shifting continues throughout the fiscal year. As the end of the fiscal year approaches, managers ensure that their accounts are entirely expended by acquiring items such as furniture and equipment, computers and software, or training. Year-end spending is necessary to avoid the appearance of having requested too much funding and suffering a future budget reduction.

So What's Wrong With This Picture?

In summary, an assessment of Federal management processes suggests that strategic planning does not drive day-to-day activities, Federal performance measures emphasize activities and outputs rather than outcomes and impact, and the budget process is "gamed" to accommodate unexpected requirements and contingencies. This fairly bleak portrayal of public sector management contrasts with the track record that career civil servants have compiled for getting the job done; and that, after all, is the "bottom line." Examples of Federal success stories are plentiful: men have walked on the moon, tens of thousands have visited Federal parks, the United States military is seen as the best in the world, and air traffic controllers ensure our safety travel every day of the year. If agencies are successful in spite of weak strategic planning processes, performance measures that emphasizes activity rather than results, and budgets that are juggled to meet emergencies and contingencies, imagine what they might accomplish with relevant management tools and processes!

Managing For Results

The National Performance Review concluded that Federal Government operations could be significantly enhanced by promoting entrepreneurial practices, innovative and creative solutions to problems, less red tape, and greater responsiveness and efficiency. Several of these principles were incorporated into GPRA which requires agencies to use the strategic planning process to: (1) state goals as benefits to the U.S. taxpayer, (2) describe strategies to accomplish those goals, and (3) state the program cost for each strategy. The GPRA also requires program performance measures that show how agencies will assess progress in achieving the goals and development and implementation of a formal performance reporting process. This shift in emphasis to cost-benefit analysis is expected to create an atmosphere where managers and staff approach their duties and responsibilities with increased urgency regarding the need to ensure that taxpayers receive excellent benefits for their tax dollar investment in Federal Government.

In order to accomplish this fundamental change, agencies must make significant enhancements to their traditional management and oversight processes. Strategic plans must be linked to tactical activities through the annual budget process. Progress must be accurately assessed using outcome-based performance measures. Most important, an annual performance report must be used to alter strategies, make tough funding trade-offs, and even "pull the plug" on programs that are not achieving desired results. This is a significant cultural change and will require senior management and congressional attention and support in order to succeed.

But the changes will not be easy. The GPRA offers no solution for the impact of politics on Federal programs including the political appointment process and congressional changes in priorities and emphasis. It also does not address the impact of unexpected crises and emergencies such as domestic terrorism or natural disasters on program activities. The greatest threat to GPRA success, however, is the very premise upon which it is based — that agencies and managers should be subject to greater accountability than ever before. Agencies recognize that the Congress might use strategic plans and performance reports to make premature program decreases or to even eliminate entire programs. Managers recognize that they have much less control over outcomes than outputs. In the substance abuse example cited above, managers can use various strategies to influence arrests, but they cannot change many of the social and economic conditions that contribute to substance abuse.

Implications For Offices of Inspector General

The preceding discussion has significant implications for the Inspector General community. What is the OIG role in assessing GPRA compliance and when is an appropriate time to schedule a review? In some cases, agencies will fail to link strategic planning and budget processes or report

performance accurately, and in other cases agencies will simply ignore the GPRA requirements. Without OIG "encouragement," GPRA may be inadequately implemented by many agencies.

The OIG must also consider implications for its own internal operations and funding requests. OIG strategic plans, like their agency counterparts, must clearly describe how resources will be used to support agency benefits to taxpayers. This requirement will be especially difficult for audit and investigative functions to implement. Will the OIG successfully establish performance measures based on outcomes to supplement their legislatively mandated requirement to report outputs to the Congress? Will the Congress continue to fund large OIG budgets if return-on-investment cannot be demonstrated? Serious consideration must be given to these questions lest OIG organizations suffer reductions similar to those recently imposed on the U.S. General Accounting Office.

The following suggestions, if implemented, will contribute to improved management and accountability processes and practices:

1. Develop Relevant Strategic Plans.
   a. Conduct a rigorous assessment of every agency program and determine how that program can be changed to provide maximum benefit at least cost to U.S. taxpayers.
   b. Use the assessment to develop clear, measurable goals and objectives for each major program. Ensure that the goals focus on specific future accomplishments for the programs, such as a 30 percent reduction in illiteracy, a 12 percent increase in small business survival rate, etc. Without clear goals, it is difficult to measure progress and success and, as noted by Behn (1993), it is "difficult to accomplish much."
   c. Establish near-term, mid-term, and long-term strategies to achieve program goals and objectives. This technique will more closely link strategies and tactics and make goal/objective success seem less formidable.
   d. Define performance measures and targets that can be used to assess progress in achieving the goals and objectives. Complement traditional performance measures with output-based performance measures and targets.
2. Link Planning and Budgeting Processes.

   Develop a financial strategy consistent with the near-term, mid-term, and long-term strategies described in the strategic plan and use the financial strategy as the basis for budget formulation and review. Price-Waterhouse observed that "the measurement system needs to directly impact the infrastructure of an organization — budgeting, personnel appraisal, etc. — or risk being ignored by managers and employees and inevitably 'die' of neglect."
3. Develop and Review Performance Reports.

   Require program managers to develop and present quarterly and annual performance reports which use performance measures and targets to describe program and financial progress in achieving goals and objectives. Use performance reports to adjust program strategies and funding emphasis.

Conclusion

Osborne and Gaebler (1992) suggested that the central problem of Governments today is "not what they do, but how they operate." Fundamentally, Government does not have to work towards a "bottom line." Yet the GPRA is designed to move agencies in that direction. It expects clear goals that demonstrate taxpayer return on investment.

If Government's goals are to seek productivity increases consistent with U.S. macro-economic goals (2-4 percent productivity increase per year), maintain low taxes and fees, and deliver excellent public services, it must manage using three basic business principles: long-range planning, performance budgeting, and performance auditing/program evaluations (Chan, 1994). These revised management processes, if successfully implemented, will contribute significantly to the public perception that the Federal Government is effective, efficient, and well-managed.

References

Behn, Robert (1993). Bottom-line government. The Governors Center at Duke University, Durham, N.C. Internet: http://192.156.133.18/Alliance/clusters/op/bookrevw.6a.html

Chan, Amy (1994). Managing a government like a business: The Sunnyvale system. Government Finance Review, Chicago, Illinois: Government Finance Officers Association, April.

Osborne, D., and Gaebler T. (1992). Reinventing Government, Addison-Wesley Publishing Company, Inc.

Price-Waterhouse (1993). Performance measurement: The key to accelerating organizational improvement. Contact Price-Watehouse at 202-822-8507.

Southern Growth Policies Board (1995). Public sector accountability literature review: measure-by-measure: benchmarking and performance measurement in the South. PO Box 12293, Research Triangle Park, NC, 27709, 919-941-5145. ❑

Congressional Oversight: The Ten "Do's" for Inspectors General

by Lorraine Pratte Lewis[1]

Lorraine Pratte Lewis, General Counsel, U.S. Office of Personnel Management

In the life of every Inspector General (IG) there will come a time when he or she is invited to testify before a congressional committee or subcommittee as part of an oversight hearing. Typically, the IG will present findings, conclusions and recommendations based on the Office's audit or investigative work. In many cases, the work will have been ongoing for years. The IG's testimony will likely precede the testimony of the agency's designated representative and may be accompanied by testimony from a representative of the General Accounting Office (GAO).

In my experience working for a Committee Chairman who frequently sought out IGs as witnesses for oversight hearings, there are a number of steps an IG can take to make the congressional testimony experience a positive one. I call these the ten "Do's."

(1) Lay the Proper Groundwork. Preparation for oversight testimony should take place long before an IG is actually called to testify on a particular matter. The IG should appoint a Congressional Liaison Officer for the Office of Inspector General (OIG). This person will be the office's eyes and ears on the Hill and will be readily available and known to Hill staff. In large Inspector General offices, this should be a main job responsibility.

(2) Do Courtesy Calls in Advance. Equally important to becoming acquainted with the Hill players, and becoming known to them, the IG should pay courtesy calls on key Members and staffs of applicable authorizing, appropriations, and Governmental Affairs/Government Reform Committees. This includes both the Senate and House, Majority and Minority, full committee and subcommittee. These visits should occur soon after the IG's appointment. Of course, some IGs will be able to accomplish this during the Senate confirmation process.

(3) Know What the Hearing is About. At the time the IG is first contacted, his or her Congressional Liaison Officer should sit down with Committee staff to learn as much as possible about the nature and scope of the hearing being planned, before the testimony is written. Some hearings are called because the Member is truly interested, others are staff driven. Talking to the staff about specifics will clarify this. In addition, many letters of invitation are vague or broadly worded. It is always a good idea to try and determine whether the Members and staffs have specific expectations regarding the IG's testimony. If those expectations are misguided, the IG needs to know and correct that right away in order to avoid later misunderstandings. The IG should provide the committee staff with those key background documents that are relevant to the testimony. If it is clear that there are significant disagreements with management, it is useful to provide a summary of management's point of view as well.

(4) Treat Majority and Minority Alike. The IG should always make sure the Majority and Minority have the same information throughout the preparation for the hearing. Although "Majority rules" on the Hill, and the focus of any oversight hearing is likely to reflect mainly the concerns of the Majority Members and staffs, you should never neglect providing the Minority with the same information. The Minority can be the source of helpful questions at the hearing, and as recent history shows, the Minority can become the Majority.

(continued on page 18)

[1] General Counsel, Office of Personnel Management. Formerly General Counsel, Senate Committee on Governmental Affairs. The views expressed in this article are the author's own, and do not represent those of the Office of Personnel Management, the Committee on Governmental Affairs, or any other Federal agency.

(5) Like the Boy Scouts, Be Prepared. This is the most crucial step of all. The IG should ensure the most current and accurate information is available about the particular matter which is the subject of the hearing. For example, management may have acted on some recommendations since an IG report was issued months ago. The IG must be aware of this and acknowledge it in testimony. The IG must also practice the testimony before members of his staff to get ready. Dress rehearsal, moot court, murder board -- whatever you call it -- there is no substitute. Nothing kills good material quicker than bad preparation.

(6) Take It to the Top. Most of the preparatory work will occur with the committee staff. However, if for any reason the IG believes something must be discussed with or brought to the attention of a Member before the hearing, the IG should not hesitate to call or schedule a meeting with the Member directly. If the IG is not able to talk to the Member, be sure to set forth the concerns in writing and deliver this document to the Committee.

(7) Agency Heads Up. It is often a good idea for the IG to give the agency's Office of Congressional Relations a courtesy "heads up" that the IG has been invited to testify, subject to the caveat that this should only be done if it does not compromise the IG's preparation for the hearing. The IG is not required to clear testimony with the agency. A courtesy copy should be given to the agency's Office of Congressional Relations at the time the Committee receives it. Both the "heads up" and the courtesy copy help to ensure against the possibility that the IG's and agency representative's testimony will be like two ships passing in the night.

(8) Write Long, Deliver Short. Write a long, detailed version of the testimony for the record. Deliver a second, much shorter version. At the hearing, Members want to get to their questions. The IG can work the necessary details into answers during the question and answer periods. Be sure to offer any and all relevant documents, like IG reports, for the hearing record. The presiding Member invariably admits it all. Bring extra copies of those documents to the hearing for press, members of the audience, and staff and Members.

(9) Correct the Record. After the hearing, always review and edit the transcript for accuracy. Otherwise, you will usually end up sounding less articulate than you meant to be. If it turns out that you were just plain mistaken during an answer, offer a written correction and request that it be inserted in the record at that point.

(10) Back at the Agency. Whether the hearing produces consensus, or highlights continuing disagreements between the IG and management, it is a good idea for the OIG to offer to meet with agency representatives immediately following a public hearing. After the bright lights go out, it shows that the IG is ready to continue working on the business at hand.

In the end, I can't guarantee that even if you follow these ten IG "Do's," every oversight hearing will go smoothly, but they should help you avoid some of the most common pitfalls. ❑

The Truth About Cats and Dogs: The Auditors and the Investigators

by David C. Williams

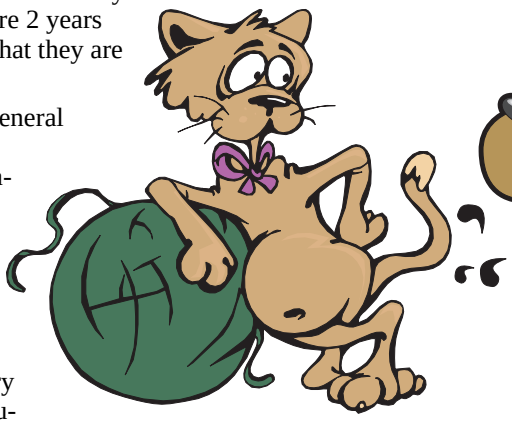
David C. Williams,
Inspector General,
Social Security Administration

See if you can pick out the audit report title from the investigative report title, keeping in mind that the inquiries looked into the same event.

"Budget Officer Nabbed In Massive Embezzlement."

"Department Fiscal Controls Are Substantial, But Must Be Improved."

Very good! Do you know how you did it? Why do program managers brood passively at the news of being audited, and yet throw up a coin they swallowed when they were 2 years old, upon being advised that they are under investigation?



To new Inspectors General (IGs), the mission of the auditors and the investigators may appear deceptively similar and inexplicably different. Both conduct inquiries into Government problems and failures. Their field work can appear very similar — collecting documents, conducting interviews, analyzing findings and delivering their findings in summary reports. The manner in which these vital, but different resources are deployed will in many ways define the character of the office an IG develops and the manner in which the IG relates to the Department.

Why are these fact-finders so different? Let's do word contrasting associations next. See if you agree with these word contrast associations with auditors and investigators.

- Congressional requesters like investigations; program managers prefer audits.
- Auditors report on the donut; investigators report on the hole.
- Auditors are bomber pilots; investigators are fighter pilots.
- Auditors deliver artillery barrages; investigators engage in hand-to-hand combat.

The beginning of the differences between auditors and investigators might be in what they are expecting to find in their inquiries. The professions seem to embrace widely divergent world views. In antiquity there were two views of sin. The Greeks, like auditors, viewed sin as evidence of incompleteness. The Romans, like investigators, viewed sin as evil. The auditors are looking for processes to make whole. The investigators are looking for evidence of intentional wrongdoing to assure proper handling by criminal courts.

Audits are broad comprehensive reviews that leave behind neatly plowed plots of land. Investigations are often narrow little trails that furrow through any number of programs or processes. The risk for auditors in their approach is that they sometimes find it irresistible to ignore leads that run off their defined game boards. The risk for the investigators is that in the narrowness of their pursuit, they can miss the context in which their evidence is discovered. Contract provisions are a notorious area in which investigators believe they have clear evidence of theft only to discover that the money was taken in compliance with a provision of the contract that the investigator failed to study and understand.

Audits are inquiries concerning programs and processes. Investigations are examinations about people and events. Audits focus on system failures and regulatory oversights that defeat controls. Investigations concern willful acts that are directed at defeating controls.

Investigators just love surprises. It is sometimes their only chance of gathering evidence of actions that are cloaked in falsehoods. To disclose the direction of their questioning is to compromise their effort to penetrate the cloak. Auditors hate surprise. For them it mostly means delay, because their interviewees have come unprepared

(continued on page 20)

to cover an unannounced topic. They are looking for the fully prepared witness. Department officials being questioned resent surprise and trickery too. When the interview technique is used inappropriately, hard feelings result and may last forever.

Auditors have a bias toward using documents as evidence. Investigators have a bias for witnesses. Auditors' final products are reports to which documents can be easily appended. Investigators are preparing for trial with live witnesses. Any documents gathered by investigators have to be introduced and interpreted by a witness that must be determined and readied. Documents are an extra inconvenience. Investigators are often skeptical of documents. They are very common instruments for constructing false alibis and nonexistent authorities for actions otherwise illegal. Auditors have a different view of documents. Auditors favor documents over witnesses. Documents are often well thought out and logically structured. Documents speak for themselves. Witness statements are illogical streams of consciousness and wholly at the mercy of the witness' memory at that moment. Witnesses recant and documents are nearly indisputable stubborn little things.

Audits make recommendations that flow from conclusions. The recommendations are intended to make incomplete sinners whole. Investigations avoid even reaching judgments and do not make recommendations. That job is for the courts and for jurors. Their task is to present clean evidence upon which conclusions can be drawn by others.

Audit reports are exactly the sum of their parts, and as a result, are rather easy to review for standard compliance and can be easily indexed and referenced. Investigative reports often conclude that the matter under investigation is greater than the sum of its visible parts. These conclusions often cannot be scientifically determined and are matters for judges and juries to conclude, not with absolute certainty, but only beyond a reasonable doubt. Inspections of investigations and the use of indexing and referencing while sometimes helpful is ultimately limited for investigations.

Big Finish!

Audit reports can be disappointing to customers outraged by the activity under investigation. These customers often include Congress, victims and public interest groups. Alternatively, investigations can be frustrating for a customer seeking the root cause of a failure or charged with using the report to fix broken programs. Obviously program managers and the Department heads often find audits more useful and less volatile.

The biases associated with audits ultimately result in risks and blind spots. Investigative biases have exactly the same result. There is a fairly sharp contrast between poor investigators and poor auditors. Excellent investigators and excellent auditors are much more like one another. They have overcome their biases and mastered skills that are unfamiliar and engaged the new skills to strengthen their effectiveness. They have reduced the risks that come from tunnel vision and borrowed the best skills from one another's professions. Like any other diverse group, Offices of Inspector General can be very powerful resources if you can keep the auditors and investigators focused on the dynamics of interchange instead of confrontation and petty jealousy.

Decisions by IGs on how to staff sensitive work will ultimately define the results the IGs achieve and define their relationships to their agencies. Responding to congressional requests and charges of agency scandal with audits will generally please the Department and disappoint the congressional requester. A criminal investigation of agency scandal will predictably respond well to congressional customers, while terrifying agency officials and limiting their choices as to how to fix the problem. For an entity with dual reporting responsibilities, this choice is daunting. In searching for an objective beacon for making such decisions, IGs should probably focus on what solution is needed to resolve the question. It is also helpful to remember the limits of the two disciplines — audits do not catch bad guys, investigations do not fix broken systems.

I am pleased to have both auditors and investigators in our Offices of Inspector General. It would be very awkward to have only one of the two disciplines in conducting our mission. Although decisions for staffing sensitive work require thought, the answer usually becomes apparent upon reflection. Although I do not believe the disciplines should ever be merged, I believe that auditors and investigators have much to learn from one another. Auditors should strengthen their interview skills and be comfortable with confrontation. Investigators should strengthen their ability to analyze documents and study the missions for the program areas of their departments. The best of the professionals will do just that and make the Offices of Inspector General uniquely strong entities.❑

Professional Note:
Constructing Compliance Agreements

by John C. Martin

John C. Martin, former Inspector General, Environmental Protection Agency

This article discusses two different approaches to compliance programs; one is proactive and the other is reactive. When business entities violate the law, they usually attempt to settle at one time all the criminal, civil and administrative actions that could be brought against them. This is known as a global settlement and is the reactive approach. An important part of this global settlement is the compliance agreement which pledges the company to actions that seek to prevent violations from happening again.

The Environmental Protection Agency (EPA) has used compliance agreements for many years as part of its efforts to ensure honesty and fair dealing in its contract process. One such agreement with a major Government contractor which was part of a global settlement involved the following provisions which are typical of the issues EPA has emphasized:

Training – The contractor's employees were to receive detailed training in time charging practices which were acceptable to the Government. To ensure consistency in the training, a videotape was prepared as the main teaching device. Every employee had to certify that he or she attended the training and was fully aware of the time charging policy.

Business Ethics Review Committee – In addition to standard ethics oversight responsibility, this Committee was obliged to issue semiannual announcements "reinforcing the firm's Government contracts compliance program and reminding employees of the jeopardy for noncompliance for themselves and the firm." The Committee also undertook responsibility for monitoring the company's hotline program.

Ethics Hotline – The company formalized a toll-free worldwide hotline for its employees to make inquiries regarding ethics matters and to report noncompliance. The employees could remain anonymous when they called or were ensured confidentiality and safeguarded from retaliation. Posters announcing the hotline were to be prominently displayed in all company locations.

President's Memo – The company president was obligated to send memoranda to each employee at least annually emphasizing the company's expectations of honest business practices.

Personnel – Certain company employees were reassigned to non-government business activities pending the completion of the Government investigation. Employees who were subsequently suspended, debarred, indicted or convicted of wrongdoing were to face appropriate disciplinary action by the company.

Audits – The company agreed to EPA reviews of its compliance with this agreement and pledged access to its facilities, personnel and records. The company also agreed to reimburse the costs of such reviews up to a pre-determined amount.

It is obvious from the detailed and sometimes rigid nature of agreements like this that the contractor has made serious commitments to the Government and even suffered substantial intrusion into its business operations. As a means to taking control of their own destiny and getting ahead of the situation created by ethics violations, many companies are establishing proactive ethics programs before problems develop.

These more aggressive programs were spurred on by the actions taken by Congress beginning in 1984 to alter Federal sentencing practices in criminal matters. In that year Congress passed the Compliance Crime Control Act which included a plan to bring uniformity to sentences imposed on convicted offenders and eliminate what was seen as widespread disparity in sentencing, which bred contempt for the law. To implement this change, Congress created the U.S. Sentencing Commission. The Commission first issued sentencing guidelines for individual defendants in 1987 and corporate defendants in 1991.

According to these guidelines, a base fine is either reduced or multiplied according to a fairly objective set of factors. When all is said and done, the fine can swing over an 80:1 ratio thus offering a very strong incentive for defendants to accentuate those elements that reduce a fine and to eliminate those elements that increase a fine. The initial fine range, before any multipliers or reducers are added, is $5,000 to $72,500,00, and is the greater of the loss suffered by the victim, the gain received by the defendant or a penalty taken from the offense level fine table.

Once the base fine is established, it is increased or decreased by calculating a defendant's culpability score.

(continued on page 22)

The fine will be increased (by maximum multiplier of 400 percent) by considering the size of the organization, involvement of its top officials in the crime, prior violations and any obstruction of justice. The fine will be decreased (by a minimum multiplier of .05 percent) by considering the "4C's" - Comply, Contact, Cooperate, and be Contrite. Varying levels of fine reduction are applied for different combinations of these elements. The first element "Comply", will be discussed after a brief review of the other elements.

Contact means that a corporation will self-report wrongdoing after conducting a thorough review of the matter at issue. **Cooperative** corporations work with the law enforcement organization investigating the matter and a **Contrite** entity accepts responsibility for the wrongdoing and expresses remorse for it.

Of the 4C's, **Comply** is the one that allows corporations to be proactive by setting up an effective compliance program in advance of any indication of wrongdoing in order to prevent violations from occurring. It is this element that has had a dramatic effect on raising the awareness of corporate ethics issues throughout the business community that deals with the Federal Government. That is because an effective program starts at the top of an organization with the CEO and Board of Directors and touches all of its employees.

The sentencing guidelines outline seven elements which a compliance program must have. The first is a set of compliance standards that employees must follow and procedures that help the company live up to those standards. These standards and procedures need to be tailored to the particular company and industry so that all potential risk areas can be covered. The second involves oversight responsibilities. Specific high-level individuals within the organization must be assigned overall responsibility to oversee compliance with the standards and procedures.

Third, the organization must use due care not to delegate "substantial discretionary authority" to anyone with a "propensity to engage in illegal activity." This requires that prospective employees and independent contractors must be carefully screened.

Fourth, the company must have taken steps to effectively communicate its standards and procedure to all its employees and "agents" such as by requiring participation in training programs or by distributing publications that explain in a practical way what is required of them.

Fifth, the organization must use monitoring and auditing systems which are designed to ferret out criminal conduct by its employees and independent contractors. A system should be provided to make it easy for these persons to report misconduct without fear of retribution.

Sixth, the organization's standards must be consistently enforced through appropriate disciplinary action against those who commit or fail to detect an offense.

Seventh, after an offense has been detected, the organization must respond appropriately and take any additional measures necessary to prevent future similar violations.

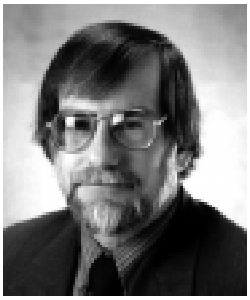
While these seven elements are required in any effective compliance program, there is a great advantage to companies to set up their programs in advance and use their own good judgment about a program's details. The alternative is to be placed in the situation of negotiating with the Federal Government over the same plan after a problem surfaces and perhaps being forced to accept detailed procedures that go well beyond what would have otherwise been required. There is also the very great advantage of keeping the company's reputation intact, without the damage suffered from criminal conviction.
As one executive said, " the cost of being indicted and the related fallout is beyond measure..."

Compliance programs of the type just described can clearly be a powerful tool to promote high ethical standards. If they are developed proactively they have the added advantage of preventing problems before they develop and help ensure honesty and fair dealing in Federal contract programs. ❑

The Urge to Merge - OIG Semiannual Report/ Agency Accountability Report

by Pamela J. Gardiner and Steven L. Schaeffer

Pamela J. Gardiner,
Assistant Inspector General for Audit,
Office of the Inspector General,
Social Security Administration



Steven L. Schaeffer,
Director of the Office of
Financial Policy and System Design,
Social Security Administration

The Social Security Administration (SSA) and its Office of the Inspector General (OIG) did something that no other Federal agency has ever done before -- it issued a joint, streamlined, accountability report covering Fiscal Year 1996. The *Social Security Accountability Report For Fiscal Year 1996* was published on November 22, 1996, less than 7 weeks following the close of the fiscal year, and 5 days ahead of the Agency's own scheduled completion date. In addition to the Agency's financial statements and performance measures for Fiscal Year 1996, it also included the Inspector General's report on SSA's financial statements, plus the equivalent of two Semiannual Reports.

In these times of downsizing and reduced budgets, the Congress and Government managers now, more than ever, are seeking timely information on Agency performance that is useful for decision making. For SSA in particular, several congressional committees need information for funding decisions about Agency programs. The public is also seeking a candid appraisal of the manner in which their taxes are spent. Integrating OIG and Agency results provides a balanced, comprehensive presentation of this information. Also, by producing a single report, SSA's and the OIG's messages are not lost among the multitude of reports delivered daily to both Congress and management officials.

This joint effort between SSA and the OIG was possible for a number of reasons. First, SSA is one of eight pilot agencies authorized by the Office of Management and Budget (OMB) to streamline and consolidate the statutory reporting requirements of the Chief Financial Officers Act, Government Performance and Results Act, Prompt Payment Act, Debt Collection Act, and the Federal Managers' Financial Integrity Act into a single accountability report. The Government Management and Reform Act of 1994 (GMRA) encouraged experimentation in reporting such as SSA's accountability report. Second, OMB with support from the Congress approved the OIG's proposal to expand the scope of the Semiannual Report to include an overview of OIG results for the entire fiscal year. Third, the initiative succeeded because it was well-planned, the individuals assigned were dedicated and experienced, and the Agency and the OIG cooperated with each other and supported the initiative.

Obtaining Approval

SSA was the first of six pilot agencies to issue an accountability report for FY 1995 and the first of eight to issue its FY 1996 report. Over the past 6 years, SSA accelerated the issue date of its annual accountability report to the President and Congress from March 31, 1992 (SSA's first Annual Financial Statement for FY 1991) to November 22, 1996 (SSA's Accountability Report for FY 1996) — more than 4 months earlier. One of the main reasons for accelerating the report was to assist the Congress as it appropriates funds to finance the Agency's programs.

SSA's Inspector General (IG), David Williams, and the Chief Financial Officer (CFO) expressed interest in merging the Office of the Inspector General's Semiannual Report to the Congress with SSA's Accountability Report. To go from idea to action, the OIG staff first solicited OMB's top officials' interest and support for a merged report. Many issues had to be resolved such as ensuring the independence of the OIG's reporting. After receiving positive feedback from OMB's Chief, Management Integrity Branch, Wendy Zenker, staff from the CFO and OIG developed an implementation plan to produce a merged report and meet the November 27, 1996, publication deadline. With the implementation plan in place, SSA's Acting CFO, Dale Sopper, and IG, David Williams, wrote John Koskinen, OMB's Deputy Director for Management, in March 1996 and officially received OMB's support to pilot a merged report.

(continued on page 24)

SSA's Timeline for Fiscal Year 1996 Accountability Report

Activity	Component	Target Dates
1. Develop and obtain approval for FY 1996 Accountability Report timeline.	CFO	March 8, 1996
2. Request all data needed to complete FY 1996 Accountability Report.	CFO	June 3, 1996
3. Formally transmit financial statements and footnotes to OIG for audit.	CFO	October 25, 1996
4. Provide draft Report on Internal Controls and Compliance with Laws and Regulations and Annual Inspector General Report (known as Semiannual Report) to SSA for comments.	OIG	November 1, 1996
5. Distribute draft FY 1996 Accountability Report for review and comments to appropriate SSA executives and OIG.	CFO	November 12, 1996
6. Receive and incorporate senior staff comments into Accountability Report.	CFO	November 15, 1996
7. Provide OIG with management representation letter and legal liability letters; provide CFO with Report on SSA's Financial Statements (Opinion on Financial Statements) and Annual Inspector General Report.	CFO/OIG	November 27, 1996
8. Release Accountability Report to President, President of the Senate, Speaker of the House, OMB and congressional Appropriations Committees.	CFO	December 2, 1996
9. Distribute Accountability Report to other congressional committees.	CFO	December 6, 1996

The next step was to secure congressional support for the joint venture. Responsibility for contacting the various congressional staffs was shared by OMB and SSA's OIG, Office of Budget, and Office of Congressional and Legislative Affairs. Staff from these offices met with specific committees to discuss how the proposal would benefit them. All of the Committees were receptive and supportive.

Coordination, Cooperation, and Timeliness

Instead of seeing the timely preparation of SSA's Accountability Report as an insurmountable task with many complex variables, we regarded it as a systematic series of distinct and achievable tasks. Cooperation, coordination, and adhering to timeliness provided the keys to success.

Planning was critical to expediting publication of the Accountability Report. This was accomplished by building on the prior year's experiences and developing and adhering strictly to a viable timeline with key milestones and target dates for both the CFO and OIG staff. Some of the key milestones are shown in the table.

Another key factor was the mutual support of the initiative by SSA's CFO and OIG staff. Annually, SSA meets with Office of the Inspector General staff to critique the year that just ended and to help each other overcome impediments to doing the job better the following year. Concurrence by the OIG with SSA's accelerated timeline was paramount to expediting the publication date of the Accountability Report.

Requests for financial and program data were sent to SSA components in early summer to allow time to incorporate the requests into their work plans. Messages to be included in the Accountability Report from the Commissioner, CFO, and Deputy CFO as well as draft transmittal letters and distribution lists of congressional committees, SSA senior staff, and other Agencies who receive the report were approved by SSA executives in advance.

Drawing on our auditors' vast experience with performing audits of SSA's financial statements also increased our chances for success. They were able to plan the audit

within the Agency's ambitious timeline. Each team member was assigned audit steps with specific due dates ensuring complete audit coverage. The audit team understood that the dates were fixed and had to be met regardless of the extra hours of work involved.

In addition, we used lessons learned from past experience performing these annual audits. For example, the audit team members issued memorandums requesting information to SSA managers without going through the normal formal correspondence writing and review process. Also, SSA officials understood the importance of our deadlines and were very cooperative in providing needed information promptly. For example, SSA provided its response to the draft audit report on Internal Controls and Compliance with Laws and Regulations in just 7 days. Finally, we analyzed our audit work from prior years to determine how we could further improve our annual audit. Our analysis identified duplication of effort between our benefits' cycle and our cash cycle, and inefficiencies in our financial reporting cycle, which we were able to avoid in the most recent audit.

As we were approaching completion in October, we found it necessary to further "divide and conquer." The OIG's plan was to have one OIG product that incorporated a message from the Inspector General, the results of the OIG audit of SSA's financial statements, and an annual report to the Congress. We had hoped the annual report to the Congress would be very short, preferably 20 pages, and rather than including all of the required tables, we would make them available upon request. We learned in October that the requirements of the Inspector General Act of 1978, as amended, were still in place and we could not discontinue publishing the required tables. The narrative sections of the annual report could provide information on accomplishments for the entire year, but we had to include tables showing 6-month accomplishments.

Within the Office of the Inspector General it was very important to have two teams working on the Accountability Report. While one group compiled the OIGs Accomplishments for the annual report, the audit team was working to complete the audit of the financial statements.

The draft Accountability Report was crafted and distributed to appropriate SSA executives and the IG for comment. Once finalized, SSA's financial management staff coordinated approvals from the Office of the General Counsel and the Office of Hearings and Appeals for legal liability letters to the IG. The last step was to obtain the Commissioner's signature on final transmittal letters and management's representation letter to the IG. On November 22, 1996, 5 days ahead of schedule, it was ready for release to the President, President of the Senate, Speaker of the House, OMB, and Appropriations Committees.

(continued on page 26)

Fiscal Year 1995 Accountability Reports

Six agencies participated in the Chief Financial Officers Council's Accountability Report pilot project in Fiscal Year (FY) 1995. Copies of the reports can be obtained by contacting the individuals listed below. Reports are also posted on the Internet.

Agency	Pub. Date	Contact	Phone	Internet
Social Security Admin.	12/95	Steven L. Schaeffer	410/965-3927	http://www.ssa.gov/finance/finance_intro.html
General Services Admin.	12/95	Claudia Bogard	202/501-0332	http://www.finance.gsa.gov/cfopage/95finstm/index.htm
National Aeronautics and Space Admin.	3/96	Lew Lauria	202/358-2495	http://hq.nasa.gov/office/codeb/welcome.html
Nuclear Regulatory Commission	4/96	Sharon Connelly	301/415-5646	http://www.nrc.gov/NRC/news.html
Dept. of Veterans Affairs	4/96	Jack Gartner	202/273-5528	http://www.va.gov/corpdata/publications/ar/index.htm
Dept. of the Treasury	9/96	Jack Blair	202/622-1450	http://www.cais.com/treasury-p+g/annrep.htm

The CFO Council conducted an evaluation of the FY 1995 Accountability Reports. The document, which was issued in November 1996, can be found on the Internet at the following address:

http://www.financenet.gov/financenet/fed/cfo/streamln/streamln.htm

Conclusion

We hope to further improve the process through the Office of Management and Budget's permanent approval to issue just one annual report to Congress rather than two semiannual reports. We would also prefer not to include the tables required by the Inspector General Act in the report, but rather have them available upon request.

We believe that issuing a consolidated Accountability Report with both the Agency's and OIG's accomplishments and perspectives is a simpler and more expeditious way to provide a comprehensive assessment of SSA programs and operations. Old news is of no value to management or to Congress as it appropriates funds to finance the Agency's programs. Timely and full disclosure of performance gives not only credibility but also the ability to discuss the implications of alternative funding levels.❑

The Art of the Referral: Presenting Cases to United States Attorneys

by Kelly A. Sisario, Bruce Sackman, and Jerry A. Lawson

Kelly A. Sisario, Inspector General, National Archives and Records Administration

Bruce Sackman, Special Agent in Charge, Northeast Field Office, Office of Inspector General Department of Veterans Affairs

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

Two nearly identical audits or investigations may result in opposite decisions by the Assistant United States Attorney (AUSA). In many cases, the difference is that one auditor or investigator understood how to present a case to the AUSA, and the other did not. This article emphasizes techniques to use when you believe you have a strong case that deserves to be prosecuted by indictment or civil recovery action. Let's set the stage for successful referrals by taking a few minutes to consider things from an AUSA's perspective.

The AUSA's Perspective

There are 96 Federal judicial districts in the United States. Each district has a U.S. District Court, and a United States Attorney. Each U.S. Attorney employs AUSAs who handle most of the day-to-day work. For our purposes, the most important thing these AUSAs have in common is that they are busy. They see more meritorious cases than they can possibly prosecute.

AUSAs decide whether a judicial action should proceed based not just on their assessment, but on policies of the Department of Justice and their local U.S. Attorney. Although few AUSAs are political appointees, they can be exposed to politically-motivated criticism.

The quality of case presentation to AUSAs is uneven. Many Office of Inspector General (OIG) employees are ill-prepared for presenting cases. Some do not fully understand how the government programs they investigate actually work. Written reports are frequently poor. Some reports include no information as to how the AUSA can contact other individuals in the case such as expert witnesses or auditors. A few agents even fail to include any information on how the AUSA could contact them for follow-up questions.

Practical Consequences

The high volume of cases means that AUSAs can be, in fact, must be, highly selective. Understanding that this is a "buyer's market," a wise auditor or investigator who wants the AUSA to proceed with his or her case will make it as attractive as possible. Your cases compete for the attention of the AUSA against many other matters. If you are presenting a case where judicial action is desirable, it is your responsibility to show the AUSA why your case will be a good place to invest time and energy.

Try to learn professional preferences of the AUSAs you are going to work with. For example, some prefer to see only a case file, and don't want to meet with investigators or auditors in every case. They figure they can read a well-written summary faster than you could explain it, and they can call you if they have any questions.

Other AUSAs are offended by merely receiving a file in the mail, and scornfully refer to this as the "Crime in a Box" approach to presenting a case. They feel that if the case is important enough to be prosecuted, it's important enough that someone should bring it in and explain it. Especially if you will be having repeated dealings with a particular AUSA, find out what he or she prefers, and handle the case his or her way.

Your presentation to the AUSA is in one sense a trial run or audition of the case:

(continued on page 28)

- If your case seems poorly organized to the AUSA, then imagine how it will strike a judge who hears it.
- If your case seems confusing to the AUSA, then imagine how hard it will be for a jury to make sense of it.

Finally, when presenting a case, remember that the AUSA is evaluating not just your paperwork and the objective strength of your case, they are evaluating you. What kind of impression would you make on a judge or jury if you have to be called as a witness?

Initial Contact

The preferred timing for the initial contact will vary from case to case, from district to district and from AUSA to AUSA. In general, if there's any doubt, it's better to contact the AUSA earlier rather than later. Get an informal take on a case, especially before investing a great deal of time on it. Finding out early what the AUSA views as potential stumbling blocks may help you focus your energies where they will do the most good.

You must decide whether to contact the Department of Justice (most often the Public Integrity section) or one of the U.S. Attorney offices. If you are contacting the latter, find out if there is a designated AUSA for case intake, or even one assigned to handle cases from your particular agency.

The initial contact can usually be by telephone. Identify yourself and your agency, briefly summarize the case and explain why it is important. When the case is far enough along, request a meeting in person to talk about the referral if you think the case merits it.

Report Writing

Write your reports so that anyone can understand them quickly and easily:

- Include a brief overview of the case to orient someone reviewing the file. Consider the use of proof charts, as explained below.
- Avoid unexplained acronyms. Everyone in your agency may know what VARO, DCSAR and NAVSEA are, but don't assume the AUSA does.
- Include the full name and identity of all agents, witnesses, auditors, experts, etc., and contact information.
- Include a full criminal history of the targets, and civil record checks, if relevant, such as Dun & Bradstreet reports. It's self defeating to find out after you have presented a case and possibly received a declination that a target had a significant criminal record that would have been relevant.

List any relevant statutes that you are aware of. Most AUSAs normally have about 15 to 20 statutes that they deal with frequently and feel comfortable with. The closer your case is to one of these laws the happier the prosecutor is likely to be. If you have a choice of statutes, try to stay with the common ones like mail fraud that are most likely to be familiar to the AUSA (not to mention the judge and jury, if the case goes that far). However, you should also include any special criminal statutes relevant to your Agency that are usually not known to most AUSAs, such as Department of Veterans Affairs (VA) pension fraud, 38 U.S.C. 3501. Coordinate with your IG counsel.

While it is not required that you do so, consider attaching a copy of a complaint, indictment or arrest warrant that was used successfully in a similar investigation. Even better, provide the same material on computer diskette for easy editing by the AUSA.

In a complex case, instead of including just the standard diary-like chronological recitation of what the auditor or investigator on the case did, consider including a reconstructed chronology of the alleged wrongdoing. This will be more useful in helping the AUSA make sense of the matter.

At least one AUSA prefers files that have pictures of the key people, places and things involved in the case. "This is suspect Jones." "This is the warehouse where the stolen merchandise was stored." "This is the seized contraband." He believes that well selected photos make the issues seem less abstract, and help persuade him so he will be able to convince a jury or judge.

Proof Charts: A Case Organizing Tool

For an important case, using "proof charts" is an option. A proof chart looks like a very simple spreadsheet. Attorneys are frequently taught to construct these in law school, so there is a good chance yours will look familiar to the AUSA. You could make up a proof chart for each crime in the file that you think should be prosecuted, or for each civil claim that you think should be brought.

In complex cases, doing "proof charts" can be a valuable tool for use inside an Inspector General's office. They can help keep auditors and investigators focused on the critical issues, instead of avoid wasting time on irrelevancies.

Speaking with the AUSA

Remember that you are "auditioning" for the role of witness in a Federal court proceeding. Dress and behave professionally.

Peter Vigeland, a former Deputy Chief of the Criminal Division of the U.S. Attorney's Office for the Southern District of New York, used to advise agents presenting cases to be "Certain in their Certainty and Certain in their Uncertainty." He felt strongly that agents should never state something as a fact unless they knew it to be correct. They should never guess at an answer. Once an AUSA determines that an agent's information is unreliable, they will not be eager to continue working with that agent.

Tom Dworschak, formerly a Special AUSA for the Eastern District of Virginia, suggests that it's a good idea to

A Sample Proof Chart

Bribery: 18 U.S.C. 201 (b): Whoever ... directly or indirectly, corruptly gives, offers or promises anything of value to any public official ... to influence any official act [shall be guilty of bribery].

Summary of this case: On June 21, 1999, John Smith offered to pay Tom Jones, a clerk at the Office of Personnel Management, $5,000 for a copy of the personnel file of George Thomas, who was a candidate for political office.

Element	Facts	Evidence	Evidence Location
directly or indirectly, corruptly gives, offers or promises anything of value	At the Tiffany Tavern on June 21, Suspect (John Smith) conditionally promised to pay Jones $5000	Statement of Jones	Tab A
to any public official	Jones is a clerk at OPM	Statements of Jones and his supervisor, Bill Johnson	Tabs A and E
to influence any official act	Smith told Jones he would be paid only on receipt of Thomas's personnel file	Statement of Jones	Tab A

approach cases "backwards." In other words, figure out early on what is the realistic expected sentence if you get a conviction. He believes everyone presenting cases to AUSAs needs to have a working knowledge of the sentencing guidelines, as it usually makes little sense to ask the AUSA to spend months on a case where little punishment is likely even if you are successful.

Agreeing to proceed with a case resulting from your audit or investigation can mean a time commitment of weeks, months or even years from the AUSA. No prosecutor wants to work with someone who is poorly organized or hard to deal with. Use this opportunity to show the AUSA that you are on top of things and they will be that much more willing to proceed on your cases.

It's also a good idea to let the prosecutor know that the case is important to you and your Agency and that even if it drags on for months or years, you will continue to provide the support that will be necessary to bring the case to a successful conclusion.

Why, Why, Why?

Regardless of whether you are putting a case file together or meeting the AUSA in person, if you don't think a case should proceed, tell the AUSA up front, and tell them why. For example, "Jones is our main witness, and he's not credible. We'll probably lose this case if it goes to trial."

On the other hand, if you are working on a case you think deserves prosecution, you should do whatever you can to highlight the reasons why. Make it very easy for the AUSA to see why your case should be prosecuted. For example:

- Will prosecution produce a good deterrent effect?
- Was a significant amount of money involved?
- Was this offense particularly egregious?
- Did the offense create unusual obstacles to the effective operation of your agency?
- Is there a history of corruption at the particular Government facility or in the program involved?
- Are there few or no disputed evidentiary issues that could prevent a conviction if the case goes to trial?

Frauds that affect more than one agency are attractive to prosecutors. Particularly in a benefit fraud case, check with your counterparts in other agencies to see if the target has defrauded others as well. Some AUSAs will be more likely to prosecute someone who has defrauded several Government agencies, even if the total dollar amount is small. Another red flag is the existence of a good confession from the target. This is usually the strongest possible sort of proof, and makes a case that much more attractive from the prosecutor's point of view.

(continued on page 30)

A 1989 President's Council on Integrity and Efficiency (PCIE) study found that the cited reason in 9 percent of declinations was "lack of criminal intent." Many perpetrators of sophisticated white collar fraud are clever, articulate and have no prior criminal convictions. After hearing the evidence against them, they can frequently come up with a cover story that convinces a jury it was all an innocent mistake. For this reason, you should be alert for what one former AUSA referred to as the "big fat dirty filthy stinking rotten lie." He uses this joking expression to make a serious point. It is a major help to a prosecutor in white collar cases if the file has proof of some untrue statement made by a suspect that proves his conduct was not merely an honest business error. Such a statement makes a case more attractive not just because it shows the suspect deserves criminal punishment, but because it makes it easier to convince a jury of guilt, especially if the untruth was memorialized in writing. The prosecutor can tell the jury, "The defendant lied to you, just like he lied previously."

If you have reason to believe that politicians or high-ranking officials of your agency would be interested in a case, let the AUSA know so that factor can be weighed. While presenting an important case on behalf of a large State agency, one of the authors even arranged for the Agency head to attend a meeting with the prosecutor. It's hard to imagine a more effective way of showing the prosecutor, "This case is significant."

Often auditors or investigators are acutely aware of factors like these or others that should influence the prosecution decision, but we fail to highlight them. Sometimes we never tell the AUSA about them at all. You could talk about factors like this in a cover letter, in a phone call, or in a face-to-face conference with the AUSA. Just make sure that whatever method you choose, the AUSA does know about them.

A good auditor or investigator should not automatically refuse to present a case to the U.S. Attorney because it falls outside prosecutorial policies. These policies are usually just guidelines. If there is a compelling reason, don't be afraid to ask for an exception to the policy.

One of the authors investigated a case involving the theft of about $8,000 in Government funds from a VA Medical Center. The Federal Bureau of Investigation (FBI) was not interested in the case because the local U.S. Attorney's office had a threshold of $10,000. When the author presented the case to the AUSA, he explained that the particular facility had a history of numerous frauds and thefts, that employees there felt they could commit crimes with impunity and that arresting the targets could help develop information on other unsolved crimes at the facility. Much to the surprise of the local FBI office, the AUSA accepted the case.

Sometimes you can make several cases that individually would be poor candidates for action more attractive by presenting them to the AUSA as a package. One fraud case of $5,000 may not be enough, but three or more such cases grouped together often will.

Is There Life After Declination?

Suppose that the AUSA declines to proceed on a case you have presented. Is that the end of the matter? In many cases administrative sanctions, or even no action at all are more in society's interest than a criminal prosecution. However, if you have a good reason to believe that a judicial action is appropriate, you can try again.

Don't re-present a case without substantial justification. This is not something to do on a whim, or out of pique. However, if you have a strong reason, don't be afraid to try it. The AUSA does not want to see a miscarriage of justice any more than you do.

Even if you have mounds of justification, you should be careful about how you re-present a case. Don't antagonize the AUSA, by, for example, trying to find some other AUSA and re-presenting the case as if it had never been rejected previously. Occasionally it might be appropriate to try going over the head of the AUSA by talking to the supervisor, but you should not do this without considering the possible adverse consequences.

Your best opportunity will usually be re-presenting the case to the first AUSA. Diplomacy is in order. Try to find some relevant facts that were omitted or underemphasized during the initial presentation. When you re-present the case, preface it with an explanation of the missing information, and why giving it proper consideration should result in a different decision. This way, you give the AUSA a way of reversing the previous decision without losing face.

Whose Job Is It, Anyway?

A few auditors and investigators will probably react negatively to some of the suggestions in this article, such as the notion that they should prepare proof charts, or offer the AUSA copies of successful old complaints, and so on:

"But this would be a lot of work. Why should I do the AUSA's job?"

Partly, it's a question of efficiency. It may only take an auditor or investigator who has lived with a case for weeks or months a short time to prepare a case summary. The auditor's or investigator's investment may save days or even weeks of time to an AUSA who would otherwise be starting at ground zero.

Partly, it's a question of seeking justice. Is the case important to you? Do you want to see it prosecuted? If so, then you should be happy to do whatever it takes to help it along. The conclusion of an audit or an investigation is not the end of the auditor's or investigator's role in helping see that justice is done in a particular matter.

Investing the time and effort that is needed to win a court case by preparing charts, tables, and anything else that will make your case easier for the AUSA to understand and prepare for prosecution can reap better rewards in the long term. Ideally, your commitment to justice will come to the attention of other AUSAs, who will then be more inclined to accept your other cases.

Conclusion

Misunderstandings and communications failures can cause less-than-optimal relationships between prosecutors and Inspector General personnel.

Auditors and investigators are sometimes dissatisfied with the time it takes AUSAs to reach decisions. They seldom realize that in many cases, their own poor presentation of a case contributes to the delay.

Declinations are another source of friction. Some cases with strong substantive merit are declined because very real reasons to proceed were obscured by an auditor's or investigator's poor organization. It is not enough to mail the AUSA a file with hundreds or thousands of confusing documents and expect him or her to sort it out.

OIG personnel sometimes perceive AUSAs as arrogant because they refuse to take cases that are significant from the OIG perspective. In many cases, the perceived arrogant attitude is caused by inadequate explanation of why a case is significant. The auditor or investigator handling the case should make it easy for the AUSA to understand why a case is important.

OIG personnel can and should help AUSAs identify those cases which are most deserving of prosecution by indictment or civil action. By improving the way in which you present cases to the U.S. Attorney's office, you may improve not just the speed with which decisions are made, but your satisfaction with the substance of those decisions.❑

The Near Horizon: Evaluation of Emerging Issues

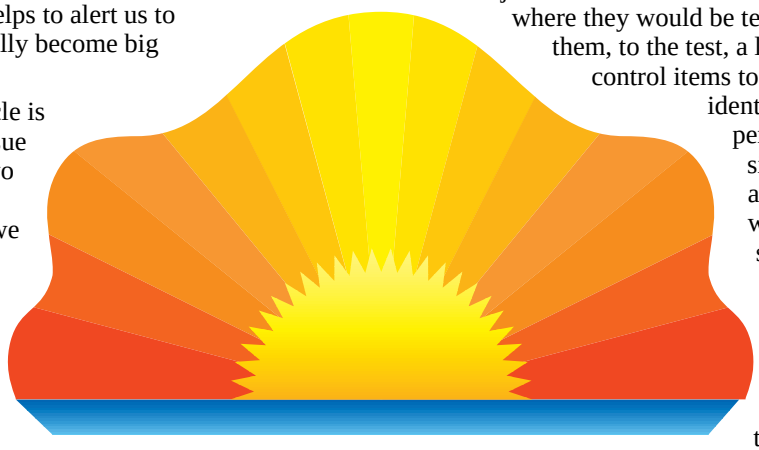
by William C. Moran

William C. Moran, Regional Inspector General, Office of Evaluations and Inspections, Department of Health and Human Services

Introduction

The Air Force uses AWACS to track airspace for hostile movement; the Navy relies on sonar to warn its ships about foreign vessels; and the Army utilizes reconnaissance forces to probe enemy lines. At the Department of Health and Human Services, the Office of Inspector General (OIG) has its own early warning device. This device, called "emerging issue reviews," helps to alert us to situations that could potentially become big problems down the road.

The purpose of this article is to tell you what emerging issue reviews are by explaining two such studies. These two examples will tell you how we identified the topic, how we conducted the review, and what the outcome was. Basically, these reviews are forward-looking, anticipating problems before they occur. They look for causes behind symptoms and for incentives that encourage unwanted behavior. The scope is the broader system, not the individual provider.



Public Cholesterol Screening

In the mid-to-late 1980s, there was a flurry of activity around cholesterol testing. Not only was the American Medical Association encouraging people to be tested by their personal physicians, but the U.S. Public Health Service was advising the public to "know your cholesterol number" by being tested.

This led to some creative marketing practices on the part of hospitals, drug stores, health clubs, shopping malls and independent entrepreneurs. Ads began to appear that invited people to show up for "public health fairs" at hospitals and "testing days" at drug stores, health clubs and in shopping malls where, for free or a low price, you could learn what your cholesterol number was.

Having completed an OIG study on physician office laboratories in early 1989, we asked ourselves some questions about cholesterol screening in more public settings. Who was performing the tests? What kind of equipment was used? What quality control measures were in place? What educational information was there to inform the person of the significance of the cholesterol number? Were referrals being made?

In order to get a better handle on this emerging issue, we decided, in the spring of 1989, to ask OIG staff in 10 major cities to seek out five to ten public screening sites where they would be tested. Staff would carry with them, to the test, a list of 13 specific quality control items to check on. They would not identify themselves as OIG personnel at the site, but would simply go through the process and observe the 13 items which they would record shortly after completing the procedure.

The results from the tests were informative. In roughly half of the cases, the persons performing the tests either did not wear gloves or did not change gloves with each new screenee. This was at a time when the HIV/AIDS epidemic was growing rapidly. Other rules of infection control, sample collection techniques, and counseling were not being observed.

In addition to the on-site testing, we telephoned every State to determine if they had any State regulation of this type of testing. We found that only 16 States regulated public cholesterol screening, with the type and extent of regulation varying widely. Federal regulation of this type of screening did not exist at the time of our review; however, there was a 1988 law that was to go into effect in 1990 that could possibly cover this type of screening, but many knowledgeable observers felt that it probably would be exempt from the law.

(continued on page 34)

Armed with these findings, we provided our results to the U.S. Public Health Service in the fall of 1989. We told them that in our probe sample across the country we found numerous shortcomings that compromised the safety and effectiveness of public screenings. We pointed out that screening staff may be placing themselves, as well as screenees, at risk due to marginal observation of the basic rules of hygiene and infection control procedures.

We recommended that the Department of Health and Human Services should discourage public cholesterol screenings that are unregulated and lack strong education, counseling, and referral components. We also recommended that this type of testing be covered by the 1988 law. By 1990, both of our recommendations had been implemented.

As a result of some good environmental scanning, we were able to nip in the bud the inappropriate growth of an industry around inferior testing for cholesterol. This not only helped prevent the spread of unclean and probably inaccurate testing, but also prevented the unnecessary expenditure of public and private health care funds.

Rural Health Clinics

While conducting field work on a home health agency study, OIG staff noted that a for-profit home health provider was buying up rural health clinics across the State. Since rural health clinics (RHC) had been in existence since the late 1970s, why would a profit-making company be interested in them now? Were there enough of them to make a difference in profits? Was this phenomenon occurring in other States?

During the summer and fall of 1995, OIG staff attempted to get an answer to these questions. We started by looking at a year-by-year listing of the number of RHCs in each State. It was quite obvious from looking at the listing that RHCs were growing, but the growth was very uneven across the States.

Not only were they growing, but when we looked at the number of applications that were in the pipeline, it appeared that the growth could be exponential over the next few years. We also noticed clusters in some States that were hard to understand in terms of rural areas.

We decided that we should visit three States that had experienced rapid growth and that had clusters of RHCs in parts of their State. We ended up visiting 27 RHCs in these three States.

We found that in addition to wanting to increase access to care, there were three other interrelated factors that appeared to be driving the growth of RHCs: reimbursement policies, the certification process and managed care pressures.

RHCs receive reimbursement from a variety of sources, but two of the major sources are Medicare and Medicaid. In 1995, RHCs were paid, conservatively, $500 million from these two sources alone. They were paid an “enhanced rate” on a cost-reimbursement basis for every encounter that they had with a patient. There is little incentive for efficiency and there are opportunities for inflated and inappropriate payments. It is a system that requires close oversight.

How difficult is it to become an RHC? Not very. If you provide health care in an area that has less than 50,000 people, there is a good chance you can become an RHC. Each State has Federally designated areas that qualify as RHC territory. In addition, a Governor can designate an area.

If you are in the designated area and meet some minimal criteria, such as employing mid-level practitioners (nurse practitioners, physician assistants, and certified nurse midwives), you can become an RHC, regardless of how many other RHCs may be located in your area. Even hospitals can be designated RHCs. Once you are designated as an RHC, you will always receive enhanced reimbursement, regardless of the changing population.

So, if I can receive an enhanced rate for services, which could be double the regular rate, and if the payment mechanism is provided on a cost reimbursement basis, won’t I be better off in a managed care environment by getting certified as an RHC? Of course. Thus, it is not hard to understand why a for-profit company was buying up RHCs in that State.

In late 1995, we presented these findings to the Health Care Financing Administration, which is responsible for the certification of RHCs, and to the Health Resource Services Administration, which is responsible for designating the geographic areas.

We recommended that they modify the certification process to ensure more strategic placement of rural health clinics. We also recommended that they take steps to improve the oversight and functioning of the current cost system, with the long term goal of implementing a different payment method. They agreed with our basic findings and recommendations.

By conducting an emerging issue review when we did, we were able to catch the proliferation early on and better understand the reasons behind the growth. We were then able to provide the program policymakers with the information they needed to take action.

Summary

These two emerging issue reviews provide insights into the characteristics of these type of studies. They are forward looking, anticipating problems before they occur. They look for causes behind symptoms and for incentives that encourage unwanted behavior. The scope is the broader system, not the individual provider.

The outcome and impact of our use of emerging issue reviews has convinced us that they are a much needed and indispensable tool in our arsenal of OIG weapons.❑

Multidisciplinary Approach to Teamwork

by Paul J. Coleman

Paul J. Coleman,
Special Agent in Charge,
Investigations Section,
Office of the Inspector General,
National Science Foundation

With the growing complexity of today's technology, Federal agents often need innovative approaches to resolve complex issues arising during fraud investigations. Agents may find that their training and expertise in the gathering of documentary and testimonial evidence are not sufficient to accomplish the analysis of evidence involving scientific or technological issues. The National Science Foundation (NSF) Office of the Inspector General (OIG) developed multidisciplinary teams of agents, scientists, and attorneys that led to the successful resolution of complex cases involving Federally-funded scientific research projects. This article discusses NSF OIG's experience with the multidisciplinary teams.

Several years ago, the NSF's OIG identified the Small Business Innovation Research (SBIR) program as a program that was vulnerable to fraud. The SBIR program is designed to stimulate technological innovation in the private sector, strengthen the role of small businesses in meeting Federal research and development needs, and increase the commercial application of the results of Federally-supported research. Eleven Federal agencies, including NSF, provide funds to SBIR companies. To receive funding, a qualified small business must submit a highly technical, scientific proposal to a SBIR program office at one of the funding agencies. The proposal describes the research that the company will conduct to develop an innovative product that the company could eventually commercialize. In the proposal, the company must certify whether the company has submitted, or received an award for, the same or similar proposal from another agency. The proposals are peer-reviewed by scientific experts to determine which proposals will be funded.

Since 1995, the Department of Justice has resolved three of the cases we investigated involving companies that applied for and received duplicate funding for similar research from multiple agencies by submitting false statements that concealed the original SBIR award. These investigations have resulted in two felony pleas, three civil settlements with total monetary recoveries of $4.1 million, the termination of $2.5 million in SBIR grants and contracts, and the debarment of three companies and five individuals. In addition, these investigations have produced Governmentwide changes in the SBIR program that will limit and prevent fraud in this program. The successful resolution of these cases and the important changes in the SBIR program were the result of teamwork, the cooperative efforts of Federal special agents, scientists, and attorneys who used their expertise to resolve the evidentiary, legal, and scientific issues that arose in analyzing and prosecuting these cases involving Federally-funded science programs.

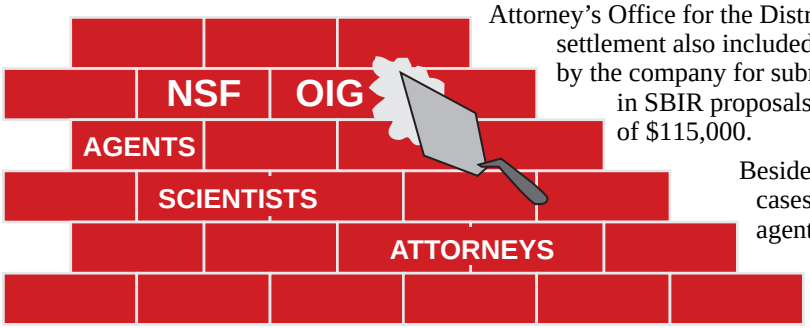
The investigative teams initially consisted of special agents from NSF's OIG; the National Aeronautics and Space Administration's (NASA) OIG; and the Department of Defense (DoD), which included agents from the Defense Criminal Investigative Service, the Air Force's Office of Special Investigations, the Army's Criminal Investigation Division, and the Naval Criminal Investigative Service. As these cases progressed, we received assistance from the U.S. Marshals Service, the U.S. Customs Service, and the U.S. Immigration and Naturalization Service. Initially, teams of agents gathered and analyzed the documentary evidence needed to support criminal and civil actions. This included finding and sifting through hundreds of SBIR research proposals, grant and contract documents, and final research reports that the SBIR companies had submitted to Federal agencies.

Early in this process, we determined that, while agents have the training and expertise to gather evidence and testimony, they lack the technical expertise to distinguish legitimate scientific differences in the SBIR research proposals and final reports from cosmetic differences that are meant to conceal duplicate proposals and previously conducted research. To compensate for this lack of technical expertise, we recruited Government scientists to work with agents to scrutinize the documentary evidence. The addition of scientists to the investigative teams was invaluable. They identified the legitimate scientific differences in proposals and allowed the agents to focus on the documentary evidence that established intentional efforts to receive duplicate SBIR awards from multiple agencies. By working directly with the scientists, the agents gained an

(continued on page 36)

understanding of the technical material. This was later used successfully to interview witnesses and obtain admissions of guilt from the subjects of the investigations.

In one case, the owner of two small companies admitted to agents that his companies submitted "some identical proposals and final reports," but he "submitted these proposals and final reports, with the intention of extending the research findings and [that] SBIR award money was invested in the company to grow the business." However, continued investigation found that the companies performed little, and in most cases none, of the research detailed in their SBIR final reports. We determined that the research reported by the companies was conducted by postdoctoral researchers and graduate students at two universities. Teams of agents as well as NSF and DoD scientists traced the research results and graphs in the companies' SBIR reports to specific experiments conducted at the universities. They did this by reviewing and analyzing laboratory notebooks; research results; drafts of research publications; and dissertations that had been subpoenaed from the universities and their former researchers. We found that virtually all of the substantive research that was reported by the two companies had been conducted at the universities as much as two years before the companies' reports were submitted to the Federal agencies, and the research had been previously submitted for publication as research articles and dissertations by the graduate students. Assistant U.S. Attorneys from the Eastern District of Virginia used this evidence during negotiations with defense attorneys, and the evidence was key to the quick settlement of this case.



On several occasions during this case, teams of attorneys, agents, and scientists worked together to analyze and discuss the relevance of the evidence. This included one meeting at a DoD research laboratory where scientists demonstrated the technology and equipment pertinent in the case. The scientists provided explanations of the technical material and how it related to specific documentary evidence that was understandable to the agents and attorneys. The attorneys used this information to rebut technical arguments raised by the defense counsel. This lead to settlement of the case, which included a guilty plea to a felony charge of mail fraud, criminal and civil restitution and fines totaling $3.47 million, and the termination of $908,556 in government contracts.

NSF OIG and Department of Justice attorneys routinely assisted the investigative teams by drafting subpoenas, reviewing reports, and negotiating administrative settlements with the defense counsel. NSF OIG attorneys added to the teams by providing detailed legal analysis and expertise in the interpretation of science program rules and the peer review process which NSF and other agencies use to evaluate scientific proposals. Most NSF OIG attorneys have doctorate degrees in scientific fields and therefore are uniquely qualified to assist in these investigations. In a case prosecuted by the U.S. Attorney's Office for the Central District of California, NSF OIG attorneys and agents assisted with drafting and filing a $4.2 million complaint and motion to freeze the defendants' assets under the Federal Debt Collection Procedures Act of 1990. In one of the first of such actions brought under the Act, the U.S. District Court found that the complaint demonstrated that the defendants were attempting to sell their properties and transfer their money overseas, and the Court ordered the Federal seizure of the defendants' property and bank accounts. The seized assets were later transferred to the Government as part of a civil settlement.

In another SBIR case, attorneys from the NSF and NASA OIGs drafted an administrative agreement in which the company and its owner accepted a 3-year exclusion from the SBIR program but allowed the owner, who is a scientist, to work on a limited basis on Federally funded research. This complex administrative agreement was part of a global settlement negotiated by the U.S. Attorney's Office for the District of Columbia. The settlement also included a felony guilty plea by the company for submitting false statements in SBIR proposals and a civil settlement of $115,000.

Besides resolving specific cases, our attorneys and agents collaborated to recommend systemic changes to the SBIR program. Vice President Gore's National Performance Review recommended that Inspectors General use the results of investigations to "help improve systems to prevent waste, fraud and abuse, and ensure efficient and effective service." Based on the National Performance Review, the President's Council on Integrity and Efficiency urged all Inspectors General to "enhance the effectiveness of an investigation in facilitating positive change" and "examine the underlying causes of fraud ... and recommend ways that program vulnerabilities can be reduced." Consistent with that advice, our attorneys and agents analyzed systemic issues that arose as a result of our investigations involving the SBIR program. We made a number of systemic recommendations that were designed to reduce the potential for fraud and abuse of this program. Many of our recommendations focused on the concealment of duplicative proposals submitted to various agencies and the acceptance of funding from different agencies for the same or overlapping research.

After we issued our recommendations, the General Accounting Office (GAO) reviewed the SBIR program. In its 1995 report, *Interim Report on the Small Business Innovation Research Program*, GAO adopted our recommendation that the Small Business Administration create a SBIR program-wide database to reduce the potential that

different agencies could fund duplicate proposals. GAO also agreed that duplicate funding is a problem and recommended that the Small Business Administration consider revising the SBIR proposal certification form and develop substantive definitions and guidelines for agencies and companies regarding "duplicate research." These recommendations have been accepted, and the changes will limit fraud and abuse of the SBIR program.

We continue to build on the team concept that developed during these investigations. In a recent case in which the owner of a SBIR company was indicted for wire fraud and submitting false statements under a NSF SBIR grant, we added auditors to our team of agents, scientists, and attorneys. We have identified two other companies that have received duplicate funding from multiple agencies for the same proposed research. Our investigative teams are working with the Department of Justice to resolve these new cases. We anticipate that these and future cases will be investigated and resolved quicker because we are building on our team experiences. The initial SBIR cases were successfully investigated and resolved quickly because of the cooperative efforts of Federal agents, scientists, and attorneys who used their expertise to resolve the evidentiary, legal and scientific issues that arose, and the creativity that comes from teamwork.❑

Cyber-Crackers: Computer Fraud and Vulnerabilities

by Alan Boulanger

Alan Boulanger, Global Security Analysis Laboratory, T.J. Watson Research Center, International Business Machines Corporation

"Threats?!? What Threats?"- Anonymous IS Manager

In 1994 the Computer Emergency Response Term, or CERT as it's known within the computer security community, reported over 40,000 intrusions into network computer systems. CERT's 1995 figures show an increase in "cracker"/"hacker" activity. In 1995, the Federal Bureau of Investigation (FBI) disclosed the results of their computer security survey that showed 40% of the surveyed sites had experienced at least one unauthorized access.

As organizations become increasingly dependent on computer network technology, they are also becoming increasingly vulnerable to losses, both financial and reputation, resulting from security breaches within their computer and communications infrastructure. The media had reported many recent attacks on high-profile sites:

Dec 1996 - U.S. Air Force home-page defaced and replaced with pornography.

Sep 1996 - Denial of service attack on panix.com; effectively shut them down.

Sep 1996 - Central Intelligence Agency (CIA) home-page defaced and replaced with pornography and graffiti

Aug 1996 - U.S. Dept. of Justice (DOJ) home-page defaced with pornography and graffiti.

1995 - Russian accountant hacks Citibank computers for $10 million.

1995 - MGM/UA Movie "Hackers" home-page altered with graffiti.

1994 - British teen penetrates ROME labs computer systems.

These successful attacks represent a small percentage of the actual attacks that have occurred. The "computer-underground" is very active and is wreaking havoc on computer systems around the world. The majority of successful attacks go unnoticed. The intruders will attack a system, gain entry, install backdoors, and remove all of their traces from the systems logs and accounting files long before anyone notices they have been attacked. Once the back doors have been installed, the intruders can then return at their leisure. By activating the backdoor, the intruders will have unlogged administrative access to the entire system. Even if the intruders fail to remove evidence of their presence and activity from the systems logs, there is an excellent chance that their activities will go completely unnoticed. When a system has been compromised it is difficult to tell from a user's viewpoint that the system has been violated. Most systems administrators are surprised when they learn that their systems have been broken into.

During the penetration tests that we have conducted at the request of our clients, on systems ranging from small home-pages to large enterprise-wide systems, our activities have been detected on less that 1 percent of the total number of systems we have attacked. We are usually able to breach the system security, leave a calling card, and cover our tracks, completely undetected by any of the system's users and administrators. These scenarios are played out daily in the computer underground and by the legitimate "tiger-teams"[1] tasked with testing the security of a network. Our tiger-team experience confirms what the intruders have known for years; most systems are vulnerable and only a few systems are being watched.

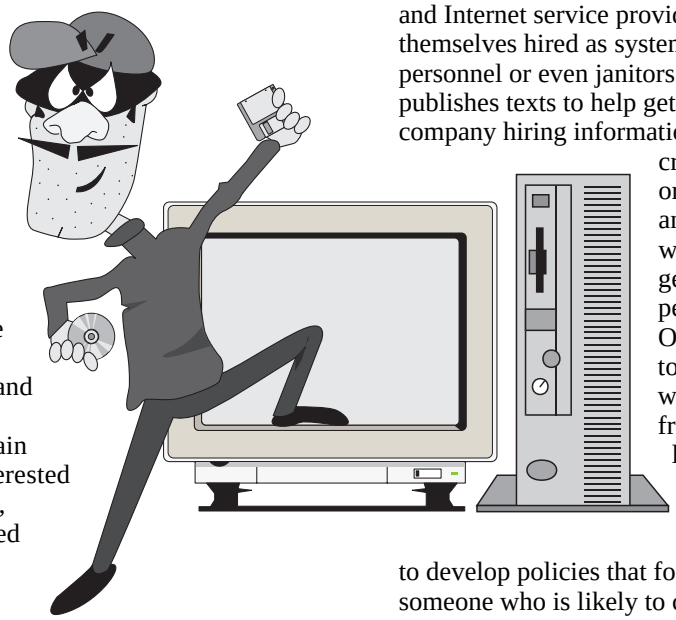
It should not be surprising then that the number of security-related incidents have been steadily growing. As more people flock to the Internet, and other on-line services, a certain percentage of them will become interested in "cracking" and seek to obtain the technical skills required to breach the security of many computer systems. By searching the Internet and underground bulletin board systems (or BBS's as they are known) any person can obtain enough information about computer networks and telephone systems to become an effective cracker. Much of this can be attributed to the fact that, while more vulnerabilities are surfacing and being corrected, many sites are still vulnerable to old, well-known, bugs and configuration errors. In short, the old techniques can still be effectively applied.

(continued on page 40)

[1] These are groups of individuals from reputable firms that attempt to violate a firm's automated security system to determine the strength of the system. This activity is authorized by the company to test their security system.

Along with information about old vulnerabilities, the underground hacker community offers a rich source of sophisticated tool-kits that are designed to penetrate into computer networks. Most of the operators of these tool-kits will lack the technical background to fully understand what functions the tools are performing. However, many of the tools are so well-written that any user with a minimum technical understanding will be able to effectively wield them.

Like the street gangs of our urban landscape, "cyber-gangs" are emerging on our networks. A cyber-gang consists of a group of people that share expertise and resources within the group. They are known to each other by their nickname, or handle, and their capabilities and interests. Often the members of these groups have not ever met in person and only communicate with other members through the telephone, voice-bridge, or chat-services. A growing number of these groups are becoming involved in computer-terrorism, vandalism and fraud. The groups responsible for the CIA and DOJ home-page attacks are clearly seen as vandals. Their main goal is to make the news and gain notoriety. Other, more dangerous groups strive to remain invisible. These groups are interested in making money through bank, credit card, and telephone related fraud. The groups interested in credit card fraud will use a computer to steal, or generate, credit card numbers and either use them to make cash advances and purchases or wholesale them to others.



Telephone related fraud consists of acquiring telephone calling card numbers and cellular telephone ESN/MIN[2] pairs. The calling cards can then either be sold in the street or used to call long distance.

The ESN/MIN pairs can also be wholesaled on the street and then used to "clone" cellular phones (calls made on the "cloned" phone will be charged to the subscriber assigned the ESN/MIN pair). Cracking into computer systems has become a very profitable endeavor.

Threat Analysis - What are the threats to network security:

The threats to our computer systems come from a variety of sources. These can be broken down into the following categories: Inside/outside, physical, administrative and technical.

Inside/Outside Threats:

The traditional, and most feared, scenario of a computer intrusion consists of an outside attack. An outside attack is an attack perpetrated by a person having no previous association with the organization and no legitimate access to the system. While there are many intrusions from outside sources, the majority of the successful, and profitable attacks are conducted by someone on the inside. A person on the inside, especially one with technical skills, has an excellent chance of being able to break into the organization's computer systems and then covering up their activities. Serious crackers know this and attempt to become hired by the companies they wish to attack. The most notable targets are the various telephone companies and Internet service providers where crackers attempt to get themselves hired as system administrators, technical support personnel or even janitors. The computer underground publishes texts to help get them hired and they trade company hiring information amongst themselves. Some crackers will even attack an organization's computer system, and then contact the organization with the results of the attack and get hired on, as consultants, to perform more security testing. Occasionally a cracker will manage to get themselves hired at a level where they can then hire their friends on as consultants. Several large companies have experienced this and some are still working at containing the damage. The best way to address this threat is to develop policies that focus on reducing the risk of hiring someone who is likely to compromise your systems.

Physical Threats:

The physical threat is closely related to the inside/outside threat. If an organization has a sensitive system, it needs to take steps in physically securing their systems. A competent systems administrator will be able to gain administrative privileges on most computer systems very easily if he or she is given physical access.

If a cracker is hired as a cleaning person and has physical access to the facility and to the system, he or she can reboot the system in "single-user" mode granting him or her administrator privileges. He or she can also boot the system from a floppy disk or tape smuggled in. Another possibility is where the cracker smuggles in a computer and "clips-on" to the organizations' networks and records the network traffic. This traffic will provide the cracker valid user accounts and passwords to other systems connected to the network. Should the above methods fail, the cracker could easily swap the mass storage device and boot his or her own system; thus allowing the cracker access to the sensitive information residing on the original device.

These few simple techniques, available to anyone with a minimal amount of technical expertise, can be deployed

[2] ESN/MIN—Electronic Serial Number and Mobile Identification Number. These codes are needed to use cellular phones.

and bypass all the firewalls and other security countermeasures used to protect the systems. One defense against the physical threat is to develop and implement an effective physical security policy.

Administrative Threats:

Administrative threats are defined as the threats resulting from the use and policies of the computer network's users and administrators. The largest single administrative threat results in a systems vulnerability to password-based attacks. A password attack consists of a successful intrusion as the result of a password failure. The failure can be attributed to accounts that are protected by well-known default passwords, blank passwords and weak passwords. Many computer systems are shipped with a set of default accounts. The accounts are used by the administrator to set up and configure the system; however, many systems administrators forget to either remove the accounts or change the password. The cracker community maintains a list of all the computer vendors and what default passwords are shipped with their systems. Some vendors ship systems that contain default accounts without passwords. A cracker, again using the list, can probe the system and check to see if any of the unprotected accounts exist. If the cracker is unable to compromise a system using the default passwords or unprotected accounts, he or she can then attempt to gain entry using weak passwords. If the intruder is able to obtain a password file from the targeted systems, using any one of a variety of techniques, the next step is to attempt to obtain a valid username/password pair by "cracking" the password file. To help minimize the vulnerability to password attacks, the site should develop and implement a password policy that will prevent users from selecting weak passwords and administrators from permitting default passwords on their systems.

Many administrators and users have lax security views because they think, "Who would want to break in here? We don't have anything!" A good cracker will find a use for every site he or she gains entry to. The compromised system can be used to stage attacks on other systems (running password crackers, monitoring the network traffic, storing tool-kits, etc.). Recently, during a successful tiger-team penetration test, we discovered the systems administrator had been using the company's computers to crack password files from other sites. Many system crackers will maintain a list of the sites they have compromised and will use those systems to leapfrog into other systems. Crackers know the system can be configured to monitor and record user and network activity. As a result, it is now common practice to launch attacks through a series of compromised systems making it more difficult to trace the origin of the attack.

Technical Threats:

Technical threats are the security exposures directly related to the computer systems themselves. These vulnerabilities are due to problems in system configurations as well as mistakes, or bugs, contained within the software of the computer systems. A security threat caused by an improperly configured system can allow an intruder access to the system without an existing account. The configuration error could also allow a regular user the ability to become a privileged user. A privileged user is able to access and modify any file on the system and to monitor network traffic from other systems. A security exposure attributed to a software bug will enable an intruder access to the systems without first having a legitimate account on the targeted system.

During our penetration testing, we have discovered that if we are able to obtain access to the system as a regular user, we will, the majority of the time, be able to promote ourselves to the level of administrator using either configuration errors or software bugs. System logs recovered from sites that have been attacked also confirmed that once an intruder has a toehold into a network, they can rapidly obtain administrator privileges and therefore control the entire system.

Much of the technical information on system vulnerabilities is publicly available. As computer vendors learn of new software vulnerabilities, they respond by issuing an alert that contains a description of the problem and the steps to take to correct it. It is important for the system administrators to keep abreast of the latest alerts and promptly apply the vendor patches to help ensure their systems security.

Information Warfare Implications:

Cracking into computer and telephone systems is no longer just a game for teenagers. There is an increasing number of reports of attacks targeting specific types of computer networks. The attacks are not conducted by teenagers roaming through a random computer network for fun. These attacks are conducted by professionals against targets that have been selected for the valuable information they are believed to possess. This information can be obtained and used for industrial espionage, Government espionage or even gaining tactical advantage in a time of war. Defense contractors can be targeted by groups seeking information on classified Government information and weapons systems. Regular businesses can be targeted for industrial espionage by domestic and foreign concerns seeking economic advantage. It is known that these systems are vulnerable and the chances are good an intruder will be able to breach the organization's security measures.

Some of the "cyber-gangs" are hackers-for-hire and offer their services to the highest bidder. They will break into the target's systems and report their findings to their clients. Professional crackers could also launch denial-of-service attacks against the targeted systems, effectively shutting them down, while their competitor works to draw the targets now disgruntled customers. An example of this occurred recently in New Jersey when a service-provider had an employee shut down a competitor's system, and then directed the competitor's clientele to their "more stable" system.

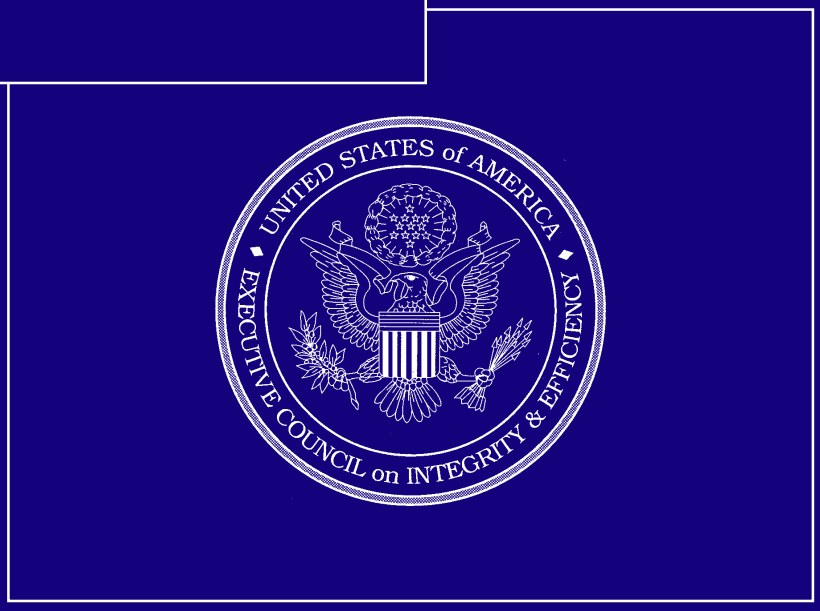
(continued on page 42)

Another recent example occurred in Connecticut when the owner of a plumbing business had the telephone calls of a competitor forwarded to his own business phones.

While the above examples involve civilian systems, the same techniques can be applied towards military objectives. An attack on a telephone switching system through the computer network could be used to disrupt an adversary's command, control and communication systems and be just as effective as an air strike. Cracking into a nation's C3I system could be just as, if not more, effective than deploying a network of field agents in gaining reliable intelligence. Cracking into a nation's financial institutions could possibly destabilize that country's economy though the modification or destruction of vital transaction records. In short, the ability to break into computer systems, has become a very valuable weapon in today's military arsenals.

It is very important to address the issues of electronic and computer security. Previously, most organizations would build a system and, if it worked, would install security precautions as an afterthought. Security concerns need to be taken seriously and addressed throughout the development and maintenance phases of each project. The need for this is evident in *Information Week's* annual survey results, published in October 1996, where, of the organizations responding to the survey; 78 percent had reported financial losses resulting from security breaches. If we fail to adequately address these security issues today, then our national and economic security will be placed in jeopardy tomorrow.❑


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


UNITED STATES of AMERICA
EXECUTIVE COUNCIL on INTEGRITY & EFFICIENCY