

HEARING regarding  
Legislative Proposals and Issues  
Relevant to the Operations of the Inspectors General

Wednesday, July 19, 2000  
10:00 a.m.  
SD-342 Dirksen Senate Office Building

WITNESS LIST

**THE HONORABLE JOSHUA GOTBAUM**  
Executive Associate Director and Controller  
United States Office of Management and Budget

**THE HONORABLE GASTON L. GIANNI, JR.**  
Inspector General, Federal Deposit Insurance Corporation  
Vice Chair of the President's Council on Integrity and Efficiency

Accompanied by:

**THE HONORABLE PATRICK E. MCFARLAND**  
Inspector General  
United States Office of Personnel Management

**THE HONORABLE KENNETH M. MEAD**  
Inspector General  
United States Department of Transportation

**MR. NICHOLAS M. GESS**  
Associate Deputy Attorney General  
United States Department of Justice



S. Hrg. 106-350  
The Inspectors General Report on the Export-Control  
Process for Dual-Use and Munitions List Commodities

HEARING BEFORE  
THE COMMITTEE ON GOVERNMENTAL AFFAIRS  
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS FIRST SESSION

JUNE 23, 1999

COMMITTEE ON GOVERNMENTAL AFFAIRS  
FRED THOMPSON, Tennessee, Chairman

WILLIAM V. ROTH, Jr., Delaware  
TED STEVENS, Alaska  
SUSAN M. COLLINS, Maine  
GEORGE V. VOINOVICH, Ohio  
PETE V. DOMENICI, New Mexico  
THAD COCHRAN, Mississippi  
ARLEN SPECTER, Pennsylvania  
JUDD GREGG, New Hampshire

JOSEPH I. LIEBERMAN, Connecticut  
CARL LEVIN, Michigan  
DANIEL K. AKAKA, Hawaii  
RICHARD J. DURBIN, Illinois  
ROBERT G. TORRICELLI, New Jersey  
MAX CLELAND, Georgia  
JOHN EDWARDS, North Carolina

Hannah S. Sistare, Staff Director and Counsel  
Christopher A. Ford, Chief Investigative Counsel  
Curtis M. Silvers, Professional Staff Member  
Joyce A. Rechtschaffen, Minority Staff Director and Counsel  
Laurie Rubenstein, Minority Chief Counsel  
Darla D. Cassell, Administrative Clerk

Witnesses

Donald Mancuso, Acting Inspector General, Department of Defense.  
Johnnie E. Frazier, Acting Inspector General, Department of Commerce  
John C. Payne, Deputy Inspector General, Department of State  
Gregory H. Friedman, Inspector General, Department of Energy  
Lawrence W. Rogers, Acting Inspector General, Department of Treasury  
L. Britt Snider, Inspector General, Central Intelligence Agency



Fraud and Waste in  
Federal Government Programs

February 10, 1999

House Committee on Government Reform  
Dan Burton, Chairman

PANEL I

The Honorable Roger Viadero  
Inspector General  
Department of Agriculture

The Honorable Susan Gaffney  
Inspector General  
Department of Housing and Urban Development

The Honorable June Gibbs Brown  
Inspector General  
Department of Health and Human Services

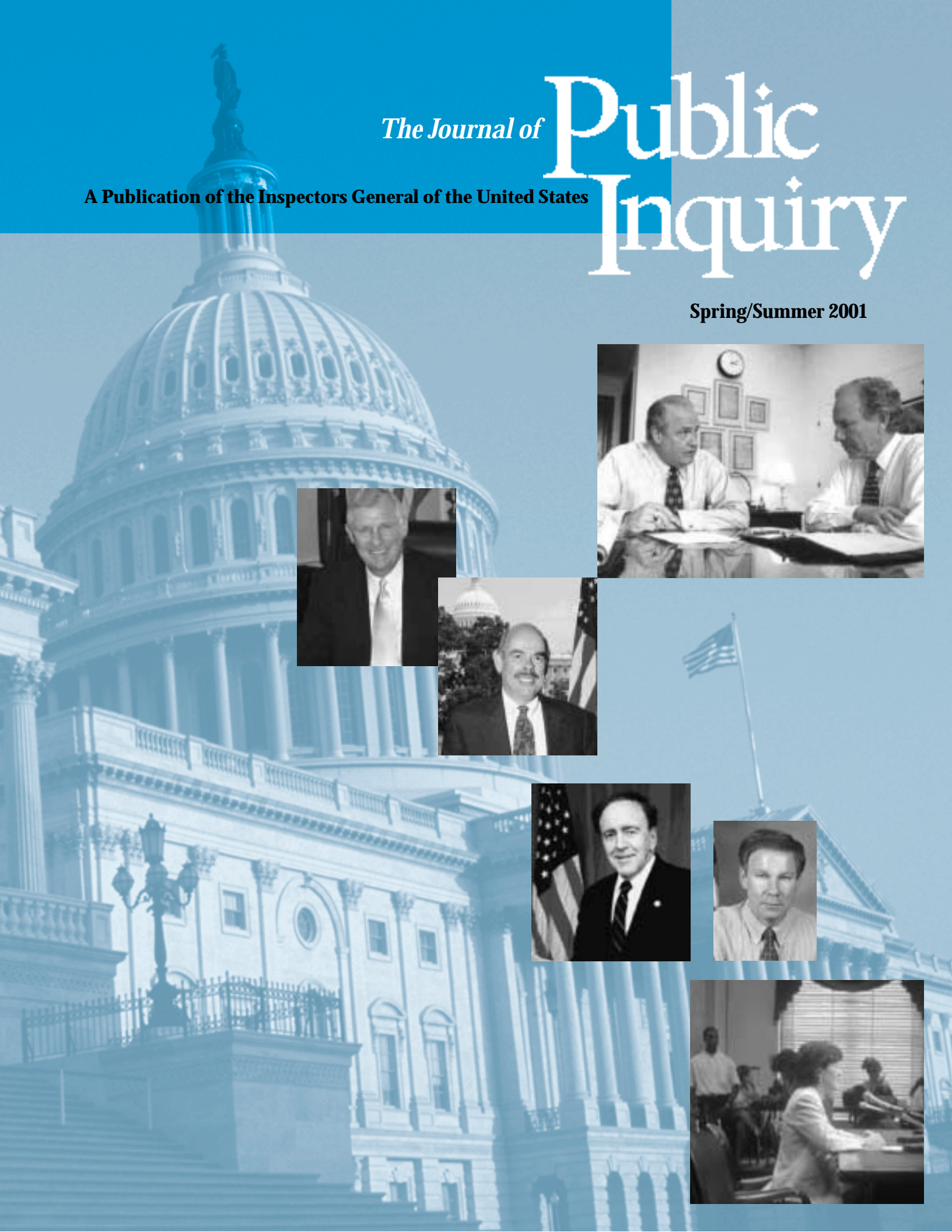
PANEL II

The Honorable David Walker  
Comptroller General  
U.S. General Accounting Office

*The Journal of* **Public Inquiry**

**A Publication of the Inspectors General of the United States**

**Spring/Summer 2001**



## EDITORIAL BOARD

**Aletha L. Brown**, Equal Employment Opportunity Commission, OIG

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

**Maryann Grodin**, Nuclear Regulatory Commission, OIG

**James E. Henderson**, General Services Administration, OIG

**Elaine Kaplan**, Office of Special Counsel

**Russell A. Rau**, National Aeronautics and Space Administration, OIG

**Karen M. Shaffer**, Office of Management and Budget

**Joseph R. Willever**, Office of Personnel Management, OIG

**David C. Williams**, Treasury Inspector General for Tax Administration

## STAFF

### *Editor-in-Chief*

**David C. Williams**, Treasury Inspector General for Tax Administration

### *Editor*

**Agapi Doulaveris**, Treasury Inspector General for Tax Administration

### *Editorial Services*

**Karen Hainer**, Treasury Inspector General for Tax Administration

### *Printing*

**Department of Defense OIG**

**Treasury Inspector General for Tax Administration**

### *Design & Layout*

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

## INVITATION TO CONTRIBUTE ARTICLES

*The Journal of Public Inquiry* is a publication of the Inspectors General of the United States. We are soliciting articles from participating professionals and scholars on topics important to the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. Articles should be approximately 3–5 pages, single-spaced, and should be submitted to Agapi Doulaveris, Treasury Inspector General for Tax Administration, Department of Treasury, 1125 15th Street, N.W., 700 (Ste. A), Washington, DC 20005.

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

## NOTICE

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

---

JO ANN L. BECKER

Chief, Forensic Science Laboratory, Treasury Inspector General for Tax Administration

# Science Non-Fiction

## *The Forensic Lab*



Paul L. Kirk, father of modern criminology, best defines forensic science's role, *"This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are, it is factual evidence, physical evidence cannot be wrong, it cannot perjure itself. . . only its interpretation can err."*

**W**ith the technological advances at a criminal's disposal, white-collar crimes have become increasingly difficult to investigate. Their mere complexity necessitates the need for specially trained experts who can interpret physical evidence, identify its relevance and eliminate premature case theories that waste valuable investigative resources. In this respect, the forensic scientist can be an investigator's greatest asset.

Forensic science is the application of science to matters of law. It embodies principles of biology, chemistry, and physics and applies them to physical evidence to resolve legal disputes. Technology gleans clues essential to the criminal investigator—a suspect's identity, an item's authenticity or a chain of events—and answers questions pertaining to the who, what, where, when and how of a crime. Suspect motive, the why, is beyond the realm of forensic science.

### **The Need for an Inspector General Forensic Lab**

Of the thousands of investigations conducted by the 2,900 criminal investigators in the IG community, many involve elements of fraud that can be established through scientific analysis, e.g., identifying the author of handwriting or the source of latent fingerprints, demonstrating signatures to be forgeries, or detecting altered documents. Scientists can pinpoint clues from evidence and help investigators prove fraud or formulate realistic theories from impartial, scientific data.

To assess the OIG community's critical need for forensic lab support, a survey was sent to members of the PCIE and ECIE to solicit agency input. A majority of respondents (84%) indicated their offices lacked access to a principal lab provider and either did without lab services altogether, requested federal, state or local lab assistance, or paid private sector contractors. Assistance from federal, state or local labs is often not responsive because these operations face 5–9 month work backlogs. In fact, many labs currently refuse outside case-work unless the evidence is part of a joint agency investigation. Therefore, the IG community is left with little leverage to find priority lab support for its investigations.

---

G. MICHAEL BAIRD

*Office of the Treasury Inspector General for Tax Administration*

# Integrity U



G. Michael Baird

Integrity is a learned behavior or trait. Webster's dictionary defines integrity as "firm adherence to a code or standard of values". The Inspector General Criminal Investigator Academy constantly reinforces this adherence in every aspect of its training programs. This constant brings to mind that this Academy is "Integrity U."

The Academy continues to be co-located at the Federal Law Enforcement Training Center in Glynco, Georgia. This partnership provides the Academy with distinct advantages in the availability of training resources and facilities. The staff of the FLETC is very supportive of the mission of the Academy and of the students and staff.

With the enactment of Public Law 106-422, the Academy is positioned to further realize the potential of becoming the IG community's principal source in meeting their specific training needs. Just some of the benefits to the OIG community are: 1) a dedicated staff of professional instructors; 2) consistent, relevant and cost-effective training; 3) IG-specific course development to meet the changing needs of the community; 4) a reduction in the amount of training responsibilities necessary within individual OIGs; 5) an economy of scale (number); and 6) access to the training needed and required to fulfill the OIGs mission.



The staff has completely remodeled the priority program, the Inspector General Investigator Training Program (IGITP). The IGITP is now a training program that is relevant, comprehensive, and challenging. After having successfully completed this program the students will be returning to their respective agencies not only with a sense of accomplishment, but also with more confidence in their abilities and authority.

The Academy will continue to eliminate redundancies in basic criminal investigator training and increase the quality and quantity of IG-specific courses. Also fundamental to the positive change that the Academy is making in its programs is to insert, wherever pos-

# All the President's Men and Women



Senator Fred Thompson

I ndependence is the lifeblood of the Inspector General. Whenever that independence is threatened, it is the duty of Congress to investigate and protect it. Because it has jurisdiction over the Inspector General Act, the Governmental Affairs Committee has taken the lead, particularly in recent years, in ensuring that IGs are free to operate at a sufficient arm's length. When allegations arose, for example, that the Inspector General at the Department of Housing and Urban Development was being harassed by the Secretary, our Committee asked the Office of Special Investigations at the General Accounting Office (GAO) to review the situation and publicly issue a report.

That congressional responsibility is increased when the IG serves a Designated Federal Entity (DFE). DFE IGs are not appointed by the president, but by the agency head who retains the authority to fire them without cause. As a result of this arrangement, DFE IGs stand a greater risk of retaliation from an angry or offended agency head simply because retaliation is easy - the only restriction on this authority is that the agency head must notify Congress of the removal along with his reasons. What follows is a description of an investigation that the Governmental Affairs Committee conducted regarding problems experienced by one DFE IG, the legislative action taken by Congress to prevent further problems, and a description of some of the options considered by Congress to permanently protect the independence of DFE IGs. I believe this particular incident can serve as a case study to help us address how to better protect the independence of DFE IGs in the future.

On May 26, 1999 Congress received a seven-day letter from the Tennessee Valley Authority (TVA) IG George Prosser pursuant to §5(d) of the Inspector General Act. In that letter, the IG alleged that Craven Crowell, Chairman of the TVA Board of Directors, had "harassed him" and attempted to impede the independence of his office. The letter was accompanied by allegations against the IG by Chairman Crowell. After receiving the letter, the Governmental Affairs Committee asked GAO to review the allegations and determine whether the independence of the IG had, in fact, been threatened. In response, GAO conducted a thorough investigation and published a report.<sup>1</sup>

---

<sup>1</sup>GAO Report, *Facts Surrounding Allegations Raised Against The Chairman And The IG*, 106<sup>th</sup> Cong. (Sept. 15, 1999).

---

HOWARD W. COX

*Director, Computer Intrusion, Office of Inspector General, U.S. Postal Service*

# Will the Circle be Unbroken?

## *Meeting the Challenges of the Expanding Role of the Inspector General Community in Federal Computer Security<sup>1</sup>*



Howard W. Cox

With the passage of the Government Information Security Reform Act (GISRA), 44 USC § 3531 *et seq.*, the inspector general community is now charged with conducting annual reviews of agency computer security. This statutory mission provides the IG community with a unique opportunity to become a major participant in the areas of computer security and infrastructure protection.

For the last three years, increasing attention has been given to the need for federal agencies to improve their efforts to protect critical government infrastructures in general, and computer security in particular. For example, in 1998, President Clinton signed Presidential Decision Directive 63 (PDD 63). Among the requirements of PDD 63 was a requirement that each federal agency must identify critical assets that support the nation's infrastructure, and develop a plan to protect these assets from harm.

As part of this initiative, increasing attention has been paid to the role of computer security in ensuring the continuity of critical federal operations. While secure computer operations have long been a concern to federal agencies with a national defense mission, all federal agencies have been affected. For example, United States Postal Service Inspector General Karla Corcoran has initiated a comprehensive audit and investigative program to examine the operation and security of the Postal Service's massive computer network. This network is essential to support the nation's mail operations.

Furthermore, recent presidential and legislative initiatives have expanded the importance of secure computer operations to all federal agencies:

- In 1994, Congress passed the Federal Acquisition and Streamlining Act that encouraged the federal government to engage in electronic contracting. As a result, many federal agencies have chosen to move to a computer based "paperless" contracting environment.

---

<sup>1</sup>The views expressed in this article are the views of the author and do not necessarily reflect the position of either the United States Postal Service or the Office of Inspector General.

---

JAMES J. FLYZIK

*Deputy Assistant Secretary for Information Systems and Chief Financial Officer,  
Department of Treasury*

# Net Escape

## *Policy for Personal Use of Internet Access by Federal Workers*

*How do we balance the need to conserve government resources against the need to compete in the marketplace for talent that sees unlimited Internet access as an innate right?*

In general, this is a reprise of an older question that has ebbed and waned in the government—the issue of regulating the personal use of government resources. Not that long ago, a mother who called her child’s doctor or school from her desk, on her lunch hour, technically would be subject to disciplinary action. While we have given our managers more leeway to deal with such situations, much of the old language remains. As we have worked to provide the American people more services in an increasingly timely fashion, we have introduced a wide range of new technologies into the workplace. These technologies not only aid the citizen; they also provide new opportunities for employees to live their lives more efficiently. A mother who is able to reassure herself by seeing a Web Cam of her child in daycare is more likely to be a productive and effective employee. These new opportunities are considered only in the context that the American taxpayers still receive the maximum benefit for their tax dollars. In order to provide our managers with better written guidance and also to help with the introduction of other new technologies in to the federal workplace, the Federal Chief Information Officers (CIO) Council has provided a model policy for “LIMITED PERSONAL USE” OF GOVERNMENT OFFICE EQUIPMENT. (The cover memo, and access to an electronic copy of the model policy, may be found at <http://cio.gov/docs/perusememo.htm>) This is a recommended policy for assisting agencies or departments in defining acceptable use conditions for executive branch employee personal use of Government office equipment including information technology. The Treasury CIO Office supported the development of this policy and has used it as the basis for its new policy, currently being circulated in draft.

The substance of this policy is that it defines a privilege that:

*“allows employees to use government office equipment for non-government purposes (Personal Use) when such use involves minimal additional expense to the government, is performed on the employee’s non-work time, does not interfere with*



---

JACK TALBERT, *Auditor*, MARSHALL GRAY, *Computer Specialist*, AND SHARON TUSHIN, *Writer/Editor*,  
*Office of Audits, Office of Inspector General, Federal Deposit Insurance Corporation*

# Online on Our Time

## ***OIG Reviews Employee Internet Use***

### **The Federal Deposit Insurance Corporation**

*The Congress created the Federal Deposit Insurance Corporation (FDIC) through the Banking Act of 1933 to provide protection for bank depositors and to foster sound banking practices. The FDIC insures deposits at more than 10,100 of the nation's banks and savings associations. In cooperation with other federal and state regulatory agencies, the FDIC promotes the safety and soundness of these institutions and the U.S. financial system by identifying, monitoring, and addressing risks to which the deposit funds are exposed.*

*Consider the following: It took 46 years for electricity to reach one quarter of American households. It took 35 years for the telephone to reach one quarter of American households. As for the world wide web—it was integrated into one quarter of American households in a mere 7 years!*

Not surprisingly, the growth of the information technology sector and the Internet, in particular, has been phenomenal throughout the federal government. We can hardly imagine accomplishing our various missions without the use of computers and the Internet resources they provide us. At the Federal Deposit Insurance Corporation (FDIC), the Internet provides access to a variety of communication and information resources that can aid employees in doing their jobs. For the FDIC, the Internet is a highly effective means of improving communication and delivering products and services to its financial industry clients as well as to the public. FDIC employees also use the Internet as an efficient tool to research and obtain financial-related information.

Despite the advantages of the Internet and e-mail, these new technological tools create certain risks that must be considered. Such risks to an agency can include public embarrassment, negative publicity, legal liabilities, and employee misuse that leads to lost productivity and network inefficiencies. To explore the overall environment of Internet use at the FDIC, the IG conducted a review of Employee Use of the Internet. The team used a number of different review techniques when attempting to address the following questions: How does management control employee use of the Internet? What are the risks and threats to the agency when employees use the Internet? Are managers using the FDIC's existing Internet policy? How do other federal agencies control employee use of the Internet? What policies and practices exist elsewhere in the government and private sector that the FDIC can learn from? The audit team ultimately presented its results to the FDIC Operating Committee, a committee comprised of FDIC Chairman Donna Tanoue and her deputies, the FDIC member of the Board of Directors, and all division and office directors.

---

DAN DEVLIN

*Office of the Treasury Inspector General for Tax Administration*

# The World in Your Lap



Dan Devlin

*“The portal is the first killer implementation of the knowledge management philosophy.”*

Carl Frappaolo, Co-founder of the Boston Delphi Group

## Introduction

Telecommuting, the practice of working away from the office, seems to be an idea whose time has come. Its popularity draws from its appeal to both employers and employees. Employers, particularly in the private sector, are finding that the quality of their customer service is enhanced when employees are situated closer to their clients and that employee productivity increases when workers are left alone to concentrate exclusively on their work<sup>1</sup>. Employees are attracted to working away from the distractions of the hectic office and the too often annoying commutes over traffic-clogged roads. Telecommuting, which began as a private sector management innovation, is being adopted increasingly in the federal government. The practice will likely increase over the next four to five years as federal agencies move to implement a new legislative requirement (PL 106-346) to offer telecommuting to twenty-five percent of eligible employees each year until the year 2005 when all eligible employees will be entitled to telecommute.

Migrating from a traditional office environment to a mobile workforce will bear directly on the business processes of OIGs. One process that will be influenced by telecommuting directly is knowledge management—that is, the process for capturing and disseminating critical information. Knowledge management is vital to inspectors general due to the primacy of information to their mission. Audits, investigations, and evaluations are fundamentally exercises in collecting, analyzing, and reporting information. To continue these functions at existing levels of production and quality under telecommuting, IGs will need to safeguard their information management processes from disruptions resulting from the shift to a mobilized work environment. Still, to fully realize the benefits of telecommuting, IGs will need to look for opportunities to advance their information management functions in creative and dynamic ways.

---

JOSEPH I. HUNGATE

*Assistant Inspector General for Information Technology, Treasury Inspector General for Tax Administration*

## A Map of PARIS, DC!



Joseph I. Hungate

Ever find yourself traveling down the management information path searching for employee information, performance information, time spent on particular investigations or status on projects, and not knowing which turn to take?

Upon its creation in January 1999, the Treasury Inspector General for Tax Administration (TIGTA) found itself in just such a place. TIGTA was traveling down a management information maze of multiple legacy information systems which contained duplicate data that often required redundant entry efforts but resulted in different information about the same subject. This inconsistent reporting was the norm. Compounding the problem of inaccuracies, these systems were not Y2K compliant and used unsupported database systems. While these systems did provide a basic level of management support to some of TIGTA's functions, other functions had no management information systems at all.

The high-level requirements were clear. A comprehensive management information system was needed that would report mission performance, update TIGTA's obsolete information systems, and provide external stakeholders with detailed, accurate information. All organizations require easy access to current and accurate data to be able to execute their strategic plans and achieve their mission objectives. TIGTA was no exception.

TIGTA's predecessor organization expended significant effort planning for system replacement, including searching for a commercial off-the-shelf system to meet agency needs. Unfortunately, the initial and subsequent searches did not yield a product that would satisfy a sufficient number of TIGTA's requirements. The decision was made to create an in-house management information system based on commercial software and tools. Thus, the road to PARIS was paved—DC that is!

### What is PARIS?

The Performance and Results Information System (PARIS) is an organization-wide management information solution for TIGTA. It uses state-of-the-art, web-based information technologies to manage critical data.

---

# Inspector General Concept

**T**he dynamic development of the Inspector General concept and the Inspector General community over the past twenty years has been profound.

From an innovative concept in the congressional mind's eye with a handful of pioneers, the Inspector General community has grown to over 60 presidentially-appointed and designated federal entity Inspectors General, thousands of staff, and presidential coordinating councils.

The following three articles link this process. Messrs. Messner and Greenstone discuss the very early pioneers of the IG world. Messrs. Ink and Jasper provide a picture of the development and current status of the IGs and their relationship with agency heads. Finally, Inspector General Kenneth Mead provides us with a snapshot of legislation affecting the IGs - past, present and future. These three essays combined will provide you with an insight about the IG concept, its traditions, and beyond.

---

## DWIGHT INK

*Chair of the National Academy of Public Administration's Presidential Transition Project panel. He held policy positions under seven Presidents, including Assistant Director for Management in the Budget Bureau and OMB. He is President Emeritus of the Institute of Public Administration.*

## HERB JASPER

*Project Director of the Academy's Presidential Transition Project panel. He served as a senior staff person in the Budget Bureau, GAO, the Congressional Research Service, and as committee and personal staff in the US Senate.*

# Talking Heads

## *Inspectors General and Their Relationships with Agency Heads*

One of the features of government that new department and agency heads without prior federal experience find to be most unusual is the fact that they have an inspector general who also reports directly to Congress. Difficult relationships with this office can easily fester into serious problems before attention is focused on how to develop an effective working arrangement. This article suggests ways in which both the agency head and the IG can develop a positive relationship that will help the agency carry out its mission effectively.

In cooperation with a number of inspectors general, the National Academy of Public Administration (NAPA) conducted a workshop on October 19, 2000. Nine Inspectors General attended, as did three Academy fellows representing the standing panel on executive organization and management. Bill Shields from the NAPA staff, who made arrangements for the workshop, recorded the proceedings, and took notes on the discussion. In addition to the workshop, we also discussed this subject with two agency heads and the former head of two independent agencies.

The purpose of the workshop and subsequent interviews was to gather ideas from inspectors general regarding IG practices that can help their offices and incoming political leadership work together in a constructive way. The following report reflects the views of its authors, not necessarily those of the persons interviewed. We took account of a number of the suggestions made during the workshop and during interviews with agency heads as well as interviews with two current or former IGs outside the workshop.

### Background

The IG positions were created by the Inspector General Act of 1978 (5 USC Appendix) during the Carter Administration. This legislation consolidated federal audit and criminal investigation functions under a statutory IG. The concept derived from the position of Inspector General in the military departments and in many of their commands.

Each executive department (as well as some of the larger independent agencies) has an IG who is appointed by the president with the "advice and consent" of the senate.

---

KENNETH M. MEAD

*Inspector General, U.S. Department of Transportation<sup>1</sup>*

# A Non-Random Act of Kindness

## *Congress and the Inspectors General*

### Evolution of the Inspector General Role

**W**hen the Inspector General Act (IGA) was first proposed in the late 1970's, skeptics abounded. The novel concept—of having an independent, non-partisan voice within an agency reporting to both its head and to Congress—would never work. It would infringe on traditional presidential prerogatives, undermine the authority of cabinet secretaries, and balkanize criminal investigations. Further, we were told, it would be impossible for an inspector general to be responsive to 535 different members of congress. Fortunately, experience has proven otherwise.

As we enter the third decade following passage of the IGA (Public Law No. 95-452), inspectors general have become an integral component in efforts to improve government efficiency and integrity. We are no longer best identified by the moniker of a certain Danny Kaye movie. With a new administration and Congress settling in, we are in a good position to make high impact contributions by focusing attention on federal management challenges and recommending constructive solutions. By virtue of our independent and nonpartisan status, we provide a measure of continuity and offer a wealth of institutional knowledge and expertise. We note that key members of Congress urged President Bush to recognize this vital role by adhering to established practice in retaining the services of presidentially-appointed inspectors general at the start of his administration. We appreciate knowing their trust and support, as well as that of the President.

The fruits of our work will not blossom, however, unless we, as a community, actively reach out to help new officials understand how we may assist them in confronting the management problems landing on their desks. Indeed, there are some 3,000 political appointment slots to fill in the executive branch, and many of these offi-

---

<sup>1</sup>Brian A. Dettelbach, Senior Counsel for Legislative and External Affairs and Paul M. Feeney, Legislative Counsel, contributed greatly to the writing of and research for this article. Disclaimer: The views of the authors are their own. They do not reflect the views of the PCIE or its Legislation Committee.

---

BETH SEREPCA

*Audit Manager, Office of Inspector General, Nuclear Regulatory Commission*

# Why Knowledge Management?

*Short answer: To make the organization more productive, more effective, and more successful. Other than that, it's not needed!*

## What is Knowledge Management?

**W**hat is knowledge, where can I find it, how can it be managed, and how would organizations benefit from managing it? Knowledge management (KM) is a concept that has emerged explosively in the business community over the last few years. KM is the explicit and systematic management of vital knowledge. It is a set of tools, practices, interventions and infrastructure, aimed at improving a firm's ability to leverage its knowledge sources to achieve business objectives. This article discusses several of these techniques, but cultural change, best practices, benchmarking, learning organization, business intelligence, competitive intelligence, data mining, workflow, communities of practice, collaborative filtering, and document management are only a sampling of the tools, practices, and infrastructure-based approaches that firms have embraced in an effort to better leverage knowledge and information. And who doesn't want to achieve business objectives? Increasingly, corporate strategists view KM as an organization's only long-term sustainable competitive advantage.

Knowledge is not data and it is not information. Knowledge is part of a continuum that KM practitioners usually depict as a pyramid. Data, the largest component, forms the base, information is the middle level and knowledge is at the top. To distinguish among the three, think of data as raw numbers and text gathered from many sources. Information is data that has been ordered and put into context, such as an accounting spreadsheet. Knowledge adds even more value, containing the expressly human contributions of experience. It is information that has been interpreted.

Studies have shown that managers get two-thirds of their information and knowledge from people, such as in face-to-face meetings or phone conversations, while only one-third comes from documents. While people automatically employ KM as part of their everyday lives, in the workplace, KM requires turning personal knowledge into corporate

knowledge that can be shared and applied organization wide.

KM divides knowledge into two main categories, tacit and explicit. Tacit, or informal, knowledge is the personal knowledge resident within the mind, behavior and perceptions of individuals. It is typically shared through discussion, stories, insight, and judgment. The other category is explicit knowledge, which exists in documents or databases. Explicit, or formal, knowledge can be articulated in language and transmitted among individuals. In business organizations, tacit knowledge is often viewed as the real key to getting things done and creating value for the organization. People transform data and information into either tacit or explicit knowledge.

Effective KM requires a structure and climate that enables and encourages the sharing of knowledge between those who have it and those who need it. For a KM initiative to succeed, several things must happen. First, an executive sponsor—a champion who understands knowledge management—must lead the effort to communicate and promote the program. Second, it must have senior management buy-in. Finally, the KM program needs to support the agency's overall mission.

## The Government's Need for KM—Fact or Fiction?

*"We are drowning in information, but starved for knowledge"*

John Nesbit, *Megatrends*.

One of the nation's largest KM implementers is the United States government. In fact, the KM programs in place in many government installations are equivalent in scope to those in business enterprises. The U.S. Navy, for example, has spent \$30 billion to transform itself into a knowledge-sharing organization.<sup>1</sup> The Federal Communications Commission is developing a knowledge strategy to map its future, and the National Aeronautics and Space Administration is undertaking an Intelligent Synthesis Environment initiative designed to change the agency's culture to a more collaborative workplace for scientists and engineers.

The government has no single, overarching KM strategy. Agencies are learning by experimenting. As in the private sector, the government's most serious obstacle to knowledge sharing is the culture. If you ask staff to change their behavior, you must provide appropriate rewards and incentives to induce the required cultural change. The General Services Administration (GSA) is developing monetary awards to recognize staff for sharing best practices. One of

the pilot programs planned for this year is a best practices sharing pilot in GSA's Public Building Service.<sup>2</sup>

Another incentive to change is provided when employees experience benefits from sharing knowledge. For example, when the Social Security Administration first offered a storytelling feature to articulate a particular experience, it was indifferently received because the users saw no reason to share knowledge. However, after several respected project managers participated, the concept caught on and employees vied to get their stories and pictures displayed on the web site. They started with three stories and now have over 100. Staff wanted to share their experiences with a particular software process methodology and how it helped them go home on time and made their lives easier.

It is essential that federal agencies capture critical employee information. In many organizations there is only one person who is trained for a specific job, and when that person leaves, so does the expertise. The loss of expertise can create deficiencies in a department's effectiveness. Furthermore, the impending retirement of millions of baby boomers adds a sense of urgency for the federal government to capture explicit knowledge.

## What Knowledge is Relevant for My Organization? Start With a Knowledge Map of the Organization

To determine what knowledge is relevant and useful, it is advisable to capture the agency's knowledge with a knowledge map. Knowledge mapping is a KM technique that captures and shares explicit knowledge and serves as a visual pointer to the holders of implicit knowledge. It creates a "yellow pages" for employees to quickly identify relevant information and sources of expertise to help with decision-making and problem solving. A map can answer questions such as:

- What information exists and where is it located?
- What expertise resides in my organization?
- What are the best sources of relevant internal information?

Maps help an organization capture and leverage what people know. Items in the map can be text, graphics, models or numbers. The information must be organized so that employees can easily search and retrieve the information or contact the individual who possesses the specific tacit knowledge.

## Organizational Culture is a Critical Success Factor for KM

We know that people have a natural instinct to hoard and to protect their territory. In this concern, knowledge is part of

<sup>1</sup>Mary Eisenhart, "Washington's Need to Know," *Knowledge Management Magazine*, January 2001.

<sup>2</sup>Dorothy Yu and Curtis Hartman, "Washington's Knowledge Management Pioneer," *Knowledge Management Review*, March/April 2000.



that “territory.” Individuals hoard knowledge to justify their indispensability. Research has shown culture to be the principal determinant influencing the success or failure of a KM initiative. Yet, it is also the most neglected aspect. Organizational culture has been defined as “the combination of shared history, expectations, unwritten rules, and social mores that affects behavior throughout the organization.”<sup>3</sup>

The biggest challenge reported by practitioners is shifting the prevailing view that “knowledge is power” to an understanding that “knowledge sharing is power.” The willingness of employees to share and contribute what they know and to leverage explicit content from inside and outside the organization is critical to KM’s success. Implementing an effective KM program usually requires significant or organizational changes. Changing behavior demands leadership. The senior management must understand the cultural barriers that impede sharing and look for ways to remove the impediments.<sup>4</sup> People who are asked to change need clear, recognizable signals from their highest-ranking colleagues indicating their acceptance of the change. Employees also need to understand the logic behind the change policies and the consequences of failing to follow them.

People, rather than technology, can be the biggest impediments to the success of a KM program. The process and technology can be effective, but, if people refuse to participate, there is no knowledge to share. While instilling a KM culture is a critical success factor for KM, implementing cultural change is the most demanding, yet least understood, work effort. According to a study conducted by the GartnerGroup, cultural changes require 50 to 70 percent of the overall KM implementation effort. Failure to change culture accounts for at least 50 percent of the KM failures.<sup>5</sup>

Enterprises have traditionally operated within a cultural framework that encourages and rewards competition and individual achievement. Employees often perceive that they can advance their careers by keeping their knowledge to themselves for their own benefit, rather than sharing it with others. However, for KM to be successful, the culture must shift so that collaboration, knowledge sharing and team achievement are valued equally with competition and

individual achievement.<sup>6</sup> In a study of 431 US and European organizations in 1997, changing people’s behavior was the most frequently identified difficulty in managing knowledge.<sup>7</sup>

For management, the golden rule must be to promote knowledge sharing and transfer. To shift the behavior to knowledge sharing, it is necessary to promote an enterprise-wide belief that 1) knowledge sharing is the source of employee power, 2) reliance on knowledge content can return value to those who use it, and 3) collaboration and shared development will be rewarded.<sup>8</sup>

People tend to share knowledge for three main reasons: reciprocity, repute, and altruisms. Reciprocity means that people share knowledge with one another in the belief that when they need to gather knowledge in the future, others will share their knowledge with them. This is the most fundamental reason for sharing. Employees will give up something of value if they expect to get something in return. If this relationship does not exist, the organizational culture must try to develop that relationship across the entire organization. Repute encourages the sharing of knowledge because of the belief that it will enhance the sharer’s reputation and standing within the community. Experts are sought after for their knowledge and to participate in projects of importance to the organization. In the present downsizing environment, the importance of repute as an inducement to share knowledge is increasing. Altruism is the sharing of knowledge with no direct thought of compensation. Under this motivation scenario, people may share knowledge if they believe it will enhance the overall performance of the organization in a way that directly affects them.

Socialization aspects of knowledge sharing are very important. People are more likely to share knowledge with people they know. People who are linked by e-mail, web pages, ideas, and common interests will share more readily. Conversely, research by the British Psychology Society found that those who feel mistreated at work, unhappy or don’t trust their employer are the ones most likely to hoard knowledge.

Information is often shared through dialogue. Socialization can help promote a more cohesive organization, while at the same time, it further embeds the knowledge-sharing system into the cultural bedrock of the organization. It also fosters personal relationships among a greater number of employees, regardless of their geographical proximity to one another.

<sup>3</sup>“Creating a Knowledge-Sharing Culture,” Consortium Benchmarking study Best-Practice Report, American Productivity and Quality Center, Houston, TX, 1999.

<sup>4</sup>Chuck Seeley and Bill Dietrick, “Crafting a Knowledge Management Strategy,” *Knowledge Management Review*, Issue 11, November/December 1999.

<sup>5</sup>K. Harris, “The GartnerGroup Cultural Framework for KM,” Research Note, Decision Framework, December 1, 1998.

<sup>6</sup>K. Harris, M. Fleming, R. Hunter, B. Rosser, A. Cushman, “The Knowledge Management Scenario: Trends and Directions for 1998-2003,” Strategic Analysis Report, GartnerGroup, March 18, 1999.

<sup>7</sup>Alex Poole, “The View From the Floor-What KM Looks Like Through the Employee Lens,” *Knowledge Management Review*, March/April 2000.

<sup>8</sup>R. Casonto, K. Harris, “Can an enterprise Really Capture “Tacit Knowledge?” Research Note, select Q&A, GartnerGroup, March 16, 1999.

## How Do We Become a Knowledge-Sharing Organization?

We must maximize the positive reasons for sharing, while recognizing and minimizing barriers. The single most important yet most difficult, step is to develop a culture that supports the knowledge sharing throughout the entire organization. Generally, this venture is best started as a pilot effort within a small part of the organization, usually where the organization has identified an area of less-than-desired performance.

Promoting the positive aspects of sharing include monetary incentives, such as rewards for sharing knowledge, designation of employees as “knowledge experts” in specific areas, and having the recognition of peers. The reward system needs to incorporate both monetary and non-monetary elements.

Senior managers can take two actions to increase the likelihood that changes in knowledge sharing behavior become rooted in organizational culture. The first is ensuring that their own knowledge-sharing behaviors are consistent with the behaviors they are encouraging in their employees, e.g., they should “walk the talk.” Second, they can provide positive reinforcement of employee knowledge

sharing by keeping staff informed on how the approach is contributing to improved organizational performance.<sup>9</sup>

## Conclusion

An unwillingness to share knowledge dooms us to repeat the mistakes of the past and miss opportunities for the future. Development of a knowledge map facilitates the identification of needed expertise and knowledge. However, without knowledge sharing, the map has no value. The ability to link experts to concentrate on one issue has little chance of success if the culture discourages the active flow of knowledge.

Our organizational culture is not averse to sharing, but it does not strongly support and reward sharing. Unless we recognize this fact and take steps to evolve our culture into a more sharing one, a knowledge management effort will not survive. Thus, it is important to embed knowledge sharing practices into the everyday work routine. 📖

---

<sup>9</sup>John P. Kotter, “Leading Change: Why Transformation Efforts Fail,” *Harvard Business Review on Change*, Harvard Business School Press, pp.18-19.

cially may be unfamiliar with the statutory duties of an Inspector General. Moreover, those members of Congress instrumental in passing the IGA and overseeing its implementation, such as John Glenn, Bill Roth, Jack Brooks, Frank Horton, and Bill Clinger, have left its hallowed halls. Out of the 535 members of the 107th Congress, over one-third of *each body* has been in office less than five years. These new members may have had only infrequent or inconsequential dealings with inspectors general.

## The IG Act in Real Life

There is an inherent tension embodied in the Act due to its dual reporting responsibilities. The inspector general must keep the agency head and congress “fully and currently” informed about program or operational deficiencies, make recommendations to promote the “economy, efficiency, and effectiveness in the administration” of such activities, and to “prevent and detect fraud and abuse in, such programs and operations.” Consequently, inspectors general have one foot in the administration, one in Congress, yet are not wholly part of either branch. Admittedly, there is a fine line to walk in balancing the needs and requests of a cabinet secretary, on one hand, and a committee chairman, on the other. But that is precisely the beauty of the Act itself, and why it has served Congress, the administration, and the public so well.

The Act also provides that an inspector general is under the “general supervision” of the agency head and deputy but, significantly, does not define those parameters. It does make clear, however, that an agency head cannot prevent an IG from “initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena during the course of any audit or investigation.” Further, the Act authorizes the inspector general to immediately report “particularly serious or flagrant problems, abuses, or deficiencies” to the agency head, who then must transmit the report and any comments to Congress within seven days, the “7-day letter” provision. Finally, inspectors general have a statutory right to “review and comment on existing and proposed legislation and regulations,” a duty that should be exercised vigilantly and robustly.

Given these elements, the foundation for success depends more upon the relationships we forge between the parties than on the plain words of the Act itself. It certainly helps to have a mutual understanding of the role played by an inspector general, with a commitment to always be fair, but firm, in speaking “truth to power,” as Paul C. Light is wont to say. While there are bound to be occasional disagreements, they will be handled professionally and respectfully, not personally. Indeed, inspectors general know that credibility is derived from the accuracy and objectivity of their reports.

## IG Contributions and Authority

*“The greatest reward for doing is the opportunity to do more”.*

Jonas Salk

As inspectors general have become established fixtures within the federal government, it is significant to note that our mission can no longer be defined solely by the Act itself. Rather, Congress has sought to expand and enhance the duties of inspectors general by assigning us new responsibilities through general management laws. Congress has also provided individual inspectors general with additional authority through agency-specific statutes. Moreover, for a number of other high visibility issues, Congress has often asked inspectors general to perform comprehensive assessments, such as the “Top 10 Management Challenges” series. This years’ reports were utilized extensively by agency transition teams, have already been the subject of Congressional oversight hearings, and were covered extensively in the media.

### ***Amendments to the IGA and other General Management Laws***

*1988 Inspector General Act Amendments*—In 1988, Congress made the first substantial modification to the IGA by passing the Inspector General Act Amendments (Public Law No. 100-504). It created OIGs within the Departments of Justice and Treasury as well as the Office of Personnel Management, the Federal Emergency Management Agency and the Nuclear Regulatory Commission (the only agencies then without statutorily established, presidentially-appointed inspectors general). Additionally, the 1988 amendments established OIGs within “Designated Federal Entities” (DFEs), primarily federal regulatory bodies or agencies receiving over \$100 million annually in federal funds. The head of each DFE would appoint the inspector general and notify Congress upon removal of the inspector general. Finally, the amendments also required each agency head to report to Congress on the implementation of management decisions on OIG audit findings and recommendations.

*Chief Financial Officers Act*—To improve federal financial management, Congress passed the Chief Financial Officers (CFO) Act of 1990 (Public Law No. 101-576) which, in part, required over 20 agencies to produce financial statements. Under the CFO Act, these annual agency financial statements are audited by inspectors general. At first, only revolving, trust fund, or substantially commercial accounts were covered, though a pilot program was established for certain agencies to prepare financial statements for all accounts. The Government Management Reform Act (GMRA) of 1994 (Public Law No. 103-356) extended the requirement for audited financial statements covering all

accounts to include all 24 CFO agencies. It also required the preparation of a governmentwide consolidated financial statement.

**Federal Financial Improvement Act**—The Federal Financial Improvement Act (FFMIA) of 1996 (Public Law No. 104-134) mandated that the CFO Act agencies implement and maintain financial management systems that substantially comply with applicable federal requirements and accounting standards. If agency financial management systems or components thereof are not in compliance, the agency head and the Director of OMB must establish a three-year corrective action plan. FFMIA also requires inspectors general to report to Congress when agency remediation plan target dates are not met, including items such as the nature, extent, and reasons for noncompliance, and actions necessary to achieve compliance.

**Government Information Security Reform Act**—On October 30, 2000, the Government Information Security Reform Act was signed into law as part of the FY 2001 Defense Authorization Act (Public Law No. 106-398). Designed to enhance the effectiveness of federal agency information security systems, the law, in part, provides for inspectors general to conduct an annual evaluation of the agency's security program and practices. This includes testing the effectiveness of security controls for agency information systems and making an assessment of their compliance with applicable policies, procedures, and guidelines. Under the Act, agencies must establish procedures for detecting, reporting, and responding to security incidents. In recognition of the vital role Inspectors General will play in this framework, guidance issued by the Office of Management and Budget (OMB) specifically highlights the need for IGs to be included as an "integral part" of the agency's reporting process for security incidents.

#### **Types of Projects Initiated by the IG Community**

In addition to new duties authorized by law, Inspectors General also initiate their own reviews of specific management issues facing a number of agencies governmentwide. Some of these crosscutting audits are in response to requests from Congress, particularly our oversight committees, and inspectors general provide them with individual reports. Other audits may be requested by the administration, and such reviews often are conducted under the auspices of the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE). Established by Executive Order, these Councils:

*"continually identify, review, and discuss areas of weakness and vulnerability in federal programs and operations to fraud, waste, and abuse, and . . . develop plans for coordinated, Governmentwide*

*activities that address these problems and promote economy and efficiency in federal programs and operations."*

The PCIE consists of presidentially-appointed inspectors general, along with representatives from the Offices of Management and Budget, Personnel Management, Government Ethics, Special Counsel, and the Federal Bureau of Investigation. The ECIE is comprised of Inspectors General at DFE agencies appointed by their agency head. Both Councils are chaired by the OMB Deputy Director for Management, with an inspector general selected from each Council to serve as the vice chair. Following are examples of some recent PCIE/ECIE and OIG initiatives.

**Screening of Federal Grant Applicants**—Under the direction of the Inspections and Evaluations Committee, OIGs examined successful agency "best" practices to better screen applicants seeking government funds (discretionary grants, loans, loan guarantees, and cooperative agreements) so that potential problems can be identified before new or additional financial assistance is awarded.

**Federal Non-Tax Delinquent Debt**—Led by the Treasury OIG, the PCIE/ECIE conducted a review on non-tax delinquent debt and agency implementation of the Debt Collection Improvement Act of 1996. That law was intended to address the estimated \$50 billion in non-tax delinquent debt owed to the federal government by maximizing collections through new systems and tools, and reducing losses incurred from inadequate debt management activities.

**Top 10 Agency Management Challenges**—At the request of Congress, IGs have been preparing annual reports of the Top 10 agency management challenges. Congress and the administration have found this to be an extremely useful report that spotlights attention on critical, systemic issues in government requiring sustained commitment by senior leaders. Because Congress has come to rely on these reports in conducting their legislative oversight, they were incorporated for agencies having Accountability Reports as part of the Reports Consolidation Act of 2000.

**Agency Implementation of the Results Act**—Pursuant to requests from Congress, the 24 CFO Act IGs have been evaluating agency implementation of the Government Performance and Results Act (GPRA). Much of this work has centered on verifying data and validating underlying performance measurement reporting systems for accuracy and reliability. In addition, Congress has asked inspectors general to assess agency Performance Reports and Plans to determine whether: (a) they sufficiently address the IG's Top 10 priority management challenges; and, (b) the department is making appropriate progress in these issue areas.

### **Multi Agency Efforts to Improve Program Integrity**

The work performed by every inspector general varies since it is based largely on the programs, operations, and priorities of each agency. However, it can be generally grouped into four different themes: Disbursement of Federal Funds; Financial Management and Information Technology; Public Health, Safety, and the Environment; and, Employee Misconduct and Program Integrity. Moreover, particularly in the investigative realm, inspectors general serve on many federal interagency law enforcement task forces to combat fraud and crime. A few examples suffice.

*Child Support Enforcement*—HHS OIG is part of a federal and state team that, with the assistance of local law enforcement agencies, tracks down and prosecutes chronic delinquent parents owing large sums of child support.

*Operation “Safe Home”*—In conjunction with other federal, state, and local authorities, HUD OIG launched “Operation Safe Home” to identify and combat violent crime and drug trafficking in public and assisted housing, fraud in the administration of public housing authorities, and equity skimming by owners and managers of FHA-insured multi-family housing.

*Food Stamp Felons*—The USDA OIG has spearheaded “Operation Talon”, in conjunction with other federal and state authorities, to identify, locate, and apprehend dangerous and violent felons who may also be illegally receiving benefits through the Food Stamp program.

*Highway and Airport Construction Fraud*—DOT OIG has designated a national contract and grant fraud coordinator to help direct fraud prevention, detection, and investigation efforts within DOT. The coordinator also works closely with state Departments of Transportation and grantees managing billions of dollars in highway, airport, and transit projects. Last year, OIG sponsored a major conference on construction fraud attended by federal and state auditors, criminal investigators, and state highway agencies and inspectors general offices nationwide.

### **Agency-Specific Priorities**

Finally, in addition to the IGA and other general management laws, there is another source by which some Inspectors General may exercise their authority. That is, through legislation such as an authorization or an appropriation measure specific to the agency itself. For instance:

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established a national program whereby the HHS OIG, the Secretary of HHS, and the Attorney General coordinate federal, state and local law enforcement activities with respect to health care fraud and abuse. This effort provides

authority to fight fraud committed against all health plans, private and public, such as Medicare and Medicaid.

- To address the threat posed to the traveling public by motor carriers and their drivers who falsify log books to circumvent federal regulations governing the number of hours they can be on the road without rest, Congress passed the Motor Carrier Safety Improvement Act of 1999. That law, in part, recognized the efforts of the DOT OIG and clarified its authority, working with other federal, state, and local officials, to conduct investigations for violations of federal criminal law and help keep unsafe and fatigued drivers off the road.

## **Recent Legislation and Outlook**

### **The 106th Congress**

There were some significant congressional activities involving the inspector general community during the last session of Congress.

*Elevation of TVA OIG, Criminal Investigator Academy and Forensics Lab*—Legislation (Public Law No. 106-422) was enacted to elevate the Office of Inspector General at the Tennessee Valley Authority from a DFE position to one appointed by the President and confirmed by the Senate. As part of that law, Congress also authorized the Inspector General Criminal Investigator Academy, which provides training and development for OIG special agents, and the Inspector General Forensic Laboratory, to perform forensic services for the community.

*Oversight Hearing on Law Enforcement Authority and IG Act Amendments*—The Senate Committee on Governmental Affairs held an oversight hearing on issues facing inspectors general, focusing primarily on the question of statutory law enforcement authority and the provisions of S. 870, the Inspector General Act Amendments, introduced by Senator Collins. That bill would have required management reviews of OIG operations, changed current reporting requirements, and mandated a study by the General Accounting Office of options for potential consolidation of DFE Offices of Inspector General.

*Fraud Recovery Audit Legislation*—The OIG community provided extensive input during House consideration and passage of the Government Waste Corrections Act of 2000, sponsored by Representative Dan Burton, Chairman of the House Committee on Government Reform. This legislation would have required federal agencies to conduct audits on major program activities to recover any erroneous payments made to contractors.

### **Legislative Issues Affecting Inspectors General**

Although it is hard to predict exactly what types of inspector general issues may come before Congress during the 107<sup>th</sup> Session, our experience over the years shows that they would generally fall into one of several broad categories: organization, mission; authority; accountability; and independence. Indeed, if the past is prologue, we can identify some possibilities.

*Fixed Terms of Office*—Some members believe that inspectors general should have a fixed statutory term of office, as have several other nonpartisan offices such as the FBI Director and the Comptroller General. The rationale is to provide continuity and enhanced security for inspectors general, especially during changes in Administration. The tenure of office for inspectors general has ranged from just a few months to over 13 years, with an average of 4.2 years. Proponents see fixed terms as a means to increase that tenure and provide greater stability within the IG community through longer tenure. Others, however, have expressed concerns over whether fixed terms could result in IGs being ignored as “lame ducks” at the end of their terms. Or conversely, whether IGs would be tempted to compromise their aggressiveness in hopes of securing possible reappointment.

A corollary issue pertains to the removal of inspectors general by the president. Inspectors general serve, in effect, at the “pleasure” of the president and can be removed at will, like other political appointees, with one very notable proviso. Under the IGA, a president must inform Congress as to the reasons for an IG’s removal. One option discussed in the debate over terms of office is whether to couple it with a removal “for cause” provision, such as malfeasance in office, as is traditional with most other term appointments.

*External Management Reviews*—Members of congress, such as Senator Collins, have proposed that there be periodic, independent reviews of OIG management and operations, especially in the areas of contracts, appropriated funds, and personnel actions. Any such new requirements must be done carefully with the aim to complement, not duplicate, the scrutiny IGs are now under. This would include the current three-year Peer Reviews, performed in accordance with applicable Government Auditing Standards, and agency-wide reviews such as personnel practices by OPM, ethics requirements by OGE, and travel voucher audits performed by agency CFOs that already scrutinize OIG operations.

*Revising the Frequency and Content of SemiAnnual Reports*—One concern often raised by members and staff of Congress is the usefulness of IG Semi-Annual Reports (SARs). A recent GAO study found that, while most Hill readers appreciated receiving them, the current form, con-

tent, and statistical emphasis of the SAR was of limited value in assessing both an IG’s performance and that of the agency.

This may be due to the statutorily-mandated categories of information we must provide. It also is a question of timeliness. The SAR is retrospective, covering activities concluded in the prior six months, and for many readers, that may well be “old” news. One approach would be to include a prospective summary of work planned or in progress in each SAR.

Congress has also considered streamlining the current SAR reporting categories and converting it to an annual report. Most IGs would support such an effort, providing there is flexibility for submitting similar reports on a more frequent basis. Indeed, several IGs believe it imperative to establish more regular and periodic lines of communication with the Hill, not less.

*Creation of an Independent IG Oversight Council*—Prior Congresses have considered creating an entity to review IG activities, including allegations of misconduct. As envisioned, such a Council might include members of Congress or their appointees, as well as representatives from the IG community. This concept resulted, in part, from Congressional concerns about the manner in which complaints against OIGs were once handled. The PCIE Integrity Committee has subsequently addressed those concerns and revised its process to ensure that all allegations are promptly and thoroughly investigated.

*Consolidating or Restructuring DFE OIGs.* There have been proposals to transfer the functions of certain smaller IGs to an office headed by a presidentially-appointed IG in an agency with related duties. Another option discussed is whether to combine the functions of some, or all, DFE OIGs into one consolidated Office under an IG who would be appointed by the president. Advocates contend this would make smaller DFE Offices more cost-efficient and enhance their independence. Should Congress consider this issue, it must determine the importance of having an IG presence (both physical and office location) in the agency’s building. It also will have to closely examine the criteria and standards used for any consolidations.

*Inspector General Pay and Compensation.* Some members want to codify guidance issued by the Clinton administration that requested PAS IGs, drawn from the ranks of the Senior Executive Service, to voluntarily waive their right to receive cash awards and bonuses from their agency head. Proponents believe any possibility that an IG could receive a cash award from an agency head poses an inherent conflict of interest. In return for foregoing such incentive awards, the salary of PAS IGs would be raised from Executive Level IV to Executive Level III.

The IG community strongly supports efforts to avoid even the appearance of a conflict of interest. However,

should Congress deliberate this issue, it must do so with some caution and some equity. We must continue to attract a high caliber of personnel to our career senior ranks, not only to carry on the mission, but also to serve as a pool of qualified candidates for future inspector general vacancies.

**Statutory Budget and Personnel Authority**—Some members of Congress have sought to enhance the independence of inspectors general by clarifying their authority over budget and personnel management matters. One budgetary option is to include the level of funding originally requested by the OIG and the amount proposed by the agency in its submission to OMB as part of the President's annual budget request to Congress. Still others have urged that IGs be given authority to submit their budget requests directly to Congress. The underlying rationale is that since inspectors general report directly to Congress, in addition to the agency head, Congress should have access to such information as it determines an appropriate level of funding commensurate with the performance of an inspector general.

The IGA provides that inspectors general serve under the general supervision of the agency head and deputy. By tradition and practice, OIGs make their own decisions with respect to personnel matters. In response, some have proposed to clarify by law that Inspectors General, with respect to all personnel actions, do not fall under the "general supervision" of the agency head.

### **Legislative Items of Interest to the IG Community**

While the following items do not represent an exhaustive list, they are items of interest to many members of the IG community. Any effort to amend the IGA in a comprehensive fashion should entail a discussion of these issues.

**Statutory Law Enforcement Authority**—Following a hearing last year, Senator Fred Thompson, Chairman of the Senate

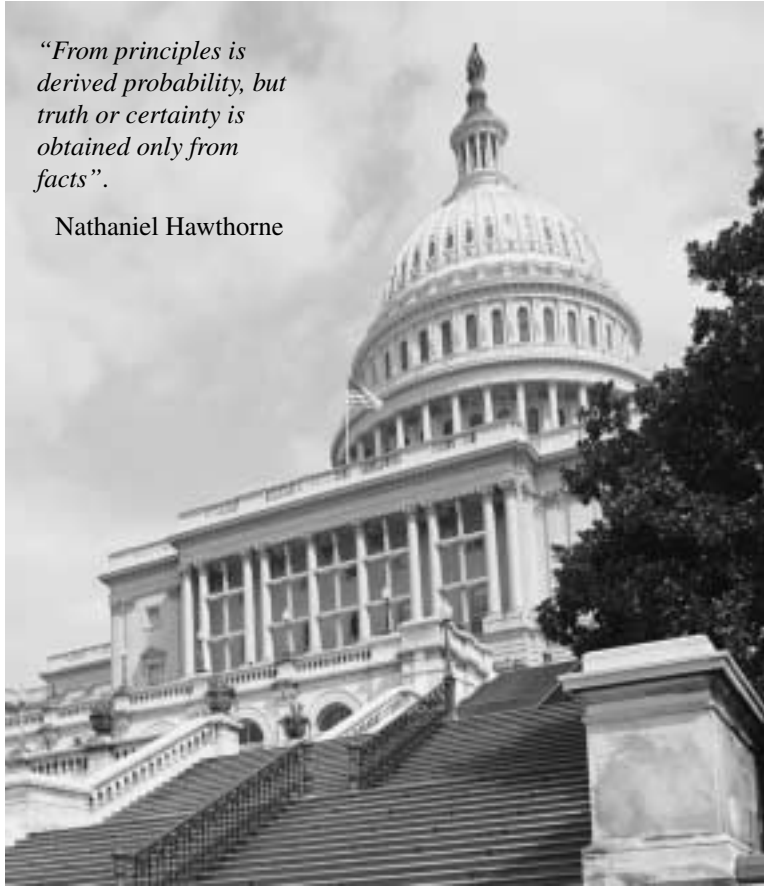
Committee on Governmental Affairs, introduced legislation to provide permanent law enforcement authority to 23 offices with presidentially-appointed, senate-confirmed Inspectors General. These offices currently exercise such powers to seek and execute search warrants, make warrantless arrests, and to carry firearms in the course of their official duties through special deputation agreements from the Department of Justice (DoJ) and the Federal Bureau of Investigation (FBI).<sup>2</sup> Significantly, the legislation had the support of both OMB and DoJ. Although it was unani-

mously reported out of Committee, the Senate did not take action prior to adjournment.

Historically, OIG criminal investigators exercised this authority for many years, originally on a case-by-case basis. As OIGs earned their stripes working closely with other federal, state, and local law enforcement agencies, and becoming active participants in interagency crime task forces, the need for such appointments became great and the volume of requests so large that the concept of "blanket" deputation for OIG agents evolved, beginning with a pilot program. That proved successful and in 1996, OIG criminal investigators began exercising law enforce-

ment authority under officewide deputations, renewable on a biennial basis.

Now over 2,500 OIG agents exercise this authority in a wide variety of law enforcement activities: health care fraud; contractor kickbacks; embezzlement of federal funds; bribery of public officials; crimes in subsidized housing; violations of motor carrier safety laws; diversion of federal grants; and many others. During FY 1999, for example, PCIE OIG investigations resulted in over 3,700 successful criminal prosecutions, 798 personnel actions, 6,660 suspensions and debarments, and \$1.7 billion in recoveries.



*"From principles is derived probability, but truth or certainty is obtained only from facts".*

Nathaniel Hawthorne

<sup>2</sup>Three OIGs—Agriculture, Defense, and Tax Administration—have law enforcement authority granted through agency-specific authorization.

OIG agents have earned the trust and respect of law enforcement colleagues in all levels of government. We certainly will do our part to support Chairman Thompson's efforts, work with other members, and the administration to make statutory law enforcement a reality.

*Clarifying the Scope of IG Authority*—The IGA provides very broad authority, imposing a duty to conduct “audits and investigations relating to the programs and operations” of agencies, and “to make such investigations and reports relating to the administration of the programs and operations . . . as are in the judgement of the IG, necessary or desirable.” Congress explicitly granted IGs the authority to issue subpoenas for the production of records and empowered IGs to take sworn testimony. Finally, Congress mandated that IGs are to expeditiously report to “the Attorney General whenever the IG has reasonable grounds to believe there has been a violation of federal criminal law.”

Despite what appears to be a rather unambiguous grant of Congressional authority, decades old Justice Department Office of Legal Counsel Opinions<sup>3</sup> and certain decisions of federal courts<sup>4</sup> construe the IGA in ways narrowing this authority. Courts are divided on the question of whether IGs can investigate false statements made to federal agencies by third parties that do not receive direct federal funds but nonetheless are subject to agency regulation.

Some courts have construed the IG Act's grant of authority to allow investigations of a regulated entity only when they are *direct* recipients of federal funds, such as contractors or grantees. Under this view, IGs may not investigate criminal conduct of regulated entities even if the subject has engaged in criminal conduct to intentionally deceive the agency. This could arise in situations where entities have received certificates or permits to operate but no direct agency funds in return for agreeing to abide by and periodically report on compliance with law and agency regulations.

At DOT, we have been challenged extensively on this particular issue. Courts are split as to whether we have authority under the IGA to conduct criminal investigations of motor carriers subject to DOT regulations and registration requirements, including the number of hours they are permitted to be on the road each day. Fortunately, with bipartisan support of Congress and the administration, Congress clarified that we had such authority as part of the Motor Carrier Safety Improvement Act of 1999.

Other inspectors general, particularly those whose agencies regulate financial institutions or engage in protect-

ing public health, safety, and the environment, have indicated an interest in having Congress clarify this discrepancy. We note that the Senate Committee on Governmental Affairs favorably reported such legislation several years ago. If the community believes it is time to revisit this matter in earnest, we must first work to lay a sound foundation with specific case examples.

*Paperwork Reduction Act Requirement and OIG Audits*—Many IGs believe that being subject to the review process requirements of the Paperwork Reduction Act (PRA) conflicts with their statutory mission to be independent and nonpartisan. They assert that these requirements affect our ability to carry out audits and evaluations required by members of Congress, through law or by requests, in a timely and effective manner.

While agency heads may generally supervise inspectors general, they are not to “prevent or prohibit the IG from initiating, carrying out, or completing any audit or investigation.” Yet the PRA requires that information collections, such as OIG surveys, be subject to approval from a “senior official” of the agency and then from OMB. While the 1995 PRA Amendments specifically exempted independent regulatory agencies from these requirements, and continues to exempt GAO, they were silent on the question of application to inspectors general.

We recognize OMB's wealth of knowledge in the formulation and conduct of surveys. Indeed, our community may wish to informally seek its advice in the areas of survey formats, techniques, and methodologies. However, application of the PRA to OIGs has both process and substance implications.

Congress increasingly requires IGs, through law or by formal request, to conduct specific audits of agency programs in a very short time. Part of the audit process may involve gathering information or other data from surveys of agency contractors, grantees, those entities subject to agency regulation, or the public. Subjecting such surveys to the review and approval process could impact our ability to provide an accurate and professional produce under the tight deadlines required by Congress.

The substantive issue is whether Congress intended that either departmental officials or OMB have authority over OIG information collection efforts that are key to the performance of a successful audit. Questions will arise should an agency head or OMB withhold approval of, or order modifications to, a proposed OIG survey. Again, it will be up to the community to present its case for clarification of this potential conflict between the IGA and the PRA.

*Codification of Integrity and Efficiency Councils*—Congress may also wish to consider whether PCIE and ECIE should be put on a par with our affinity Councils, the Chief Financial Officers (CFO) and Chief Information Officers (CIO),

<sup>3</sup>The so-called *Kmiec* and *Barr* Opinions. March 9, 1998 opinion of Douglas Kmiec, Deputy Attorney General, 13 U.S.Op. O.L.C. 54; July 17, 1990 opinion of William P. Barr, Acting Deputy Attorney General.

<sup>4</sup>Notably the Fifth Circuit's decision in *Burlington Northern Railroad Co. v. Office of Inspector General, Railroad Retirement Board*, 983 F.2d 631 (5th Cir. 1993).



through statutory codification. The mission of the PCIE/ECIE Councils is to promote collaboration on integrity and efficiency issues that transcend individual governmental agencies and to increase the professionalism and effectiveness of IG personnel throughout government.

The IG community appreciates the support given by the Deputy Director of OMB for Management, as chair of each council, and OMB staff assistance in recent years. However, codification would provide the Councils with a permanent, institutional footing—one that allows the councils to reach their full potential and better serve the needs of the administration and Congress.

Congress could, for example, require the councils by law to produce annual reports summarizing the major crosscutting issues identified in the Top 10 series, including recommendations on how best to address them and progress made to date. Besides specifying the types of governmentwide issues where IGs can play a key role, codification also would serve as a mechanism to assign the councils responsibility for professional development opportunities, such as establishing a first rate, multidisciplinary

training program for both auditors and investigators. Finally, to help carry out these statutorily-enhanced responsibilities, codification could allow us access to limited federal funds, through rebates from the use of government credit cards, a source which our fellow CFO and CIO councils already can draw from.

## Epilogue

*“From principles is derived probability, but truth or certainty is obtained only from facts”*

Nathaniel Hawthorne

The inspector general community can rightly be proud of our contributions in service to the nation and its taxpayers. Our very mission is a public trust. That is, to provide independent, nonpartisan, and objective advice to Congress and the administration. We stand ready to work with Congress, OMB, and the administration on legislative matters affecting the IG community. 🏛️

Appointments, removals and authorities of IGs differ from those of other presidentially appointed, Senate confirmed (PAS) positions in several ways:

- They have a dual reporting responsibility to their agency heads and the Congress.
- They are to be appointed “without regard to political affiliation” and “solely on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration and investigations.”
- Pursuant to the Constitution, they serve at the pleasure of the President but if he terminates them, he must send a letter of explanation to the Congress.

The IG Act also provides for appointment of IGs by the agency heads in “Designated Federal Entities.” They are subject to the same provisions listed above, except that it is the agency head who must send a letter of explanation to the Congress in the event of termination.

The role of the IGs is unique in the government. Because of their dual reporting responsibility to the agency head and to Congress, they have a substantial degree of independence. They vigorously protect this independence, as their statutory responsibilities require. Unless new agency heads have previously served in the federal government or in the armed forces, they are unlikely to be familiar with the IG position and concept. They may, however, remember a few cases where an agency head and the IG have had major disputes that were extensively covered by the media.

To some extent, one can expect such disputes to arise from time to time. Both the Congress and the media are very interested in and receptive to reports about fraud or mismanagement in the agencies. And agency heads may not readily recognize that these senior officials can not, in some respects, perform like other members of the leadership team in their agency. Therefore, serious issues may arise between agency leadership and IGs, no matter how well intentioned they both are. Considering that reality, let us outline practices that have proved to be conducive to developing a cooperative relationship between agency heads and IGs, as well as to identify practices that are not as helpful.

### Importance of Initial Impressions

The initial impression of a new agency head concerning the IG appears to be very important. Problems have sometimes developed even before the new agency head had the time or information to fully understand the IG concept or to observe one’s performance. In a number of instances, the incoming agency head has had prior government experience and is likely to want to meet early with the IG, thereby providing an opportunity to establish a constructive working relationship. More often, however, incoming agency

heads have received only “textbook” information about IGs. Often, they are briefed by senior career officials, some of who may have an interest in restricting the scope, authority or influence of the IGs.

Sometimes, a new agency head is provided misleading anecdotal stories about the current or past IG upon his or her arrival. This may lead to a perception that IGs are problems whose roles are largely negative and detrimental to the operation of the agency and may jeopardize the development of good relationships between new agency heads and their IGs. Because attempts by IGs to counteract such negative perceptions are likely to be regarded as self-serving, we urge that efforts be made as a part of orienting new agency leadership to counter such perceptions.

In practice, the role of the IGs varies somewhat among the agencies, but their statutory authorities and responsibilities are extensive. They range from detecting and preventing fraud, waste and abuse, to evaluating management systems, and even advising on program design. Examples of IG contributions to improved agency performance include:

- ✓ substantial monetary savings through prevention of abuse, assessing penalties, or recovery of fraudulent charges,
- ✓ identification of system vulnerabilities, whether of a physical, financial or data security nature, often leading to correction before system failures occurred, and
- ✓ recommendations of streamlined organization or improved policies and processes.

On the other hand, cases have arisen that reflected sharp clashes between agency leadership and IGs. At least two such clashes have been widely publicized to the detriment of both the agency and the IG. Accordingly, both an agency head and an IG ought to recognize early that agency interests can best be served by the development of a cooperative relationship between the two, even though the IG must retain the independence contemplated by the law.

Agency heads will find that IGs are often the “institutional memory” of their agencies and thus can help an incoming administration by providing history about what has succeeded or failed. IGs can be counted on to provide the facts, whether good or bad, thus helping the agency head avoid the risks inherent in the tendency of well-meaning subordinates to over-emphasize the positive.

### Transition Orientations

A fundamental dynamic in framing the relationship is whether the new administration views the IG role as positive, or as weak, troublesome or even irrelevant to the agencies’ missions. It is very difficult to overcome negative perceptions encountered during a presidential transition before an IG and a new agency head have even met. Therefore, we urge that the role of IGs and their potential value to the

incoming political leadership is covered in the orientations and workshops for top political leaders authorized by the Presidential Transition Act 2000.

In those orientations or workshops, or in initial briefings and discussions by senior career personnel, pains need to be taken to convey the nature of the IG concept, including the rationale for IGs' having certain independent authorities by statute. It should be explained how the IG office can be an asset to the agency head and the agency in advancing its mission even though some IG reports will likely include decidedly negative findings. It needs to be stressed that any such negative finding increase the opportunity for the agency to begin to take corrective action before it escalates into a problem needing congressional attention.

## Responsibilities of the IG

Clearly, the effectiveness of an IG depends heavily on how his/her office can demonstrate its value to the agency by the exercise of independence and objectivity.

*Prevention*—By detecting emerging problems, IGs can provide early warnings before they become costly or develop into scandals. It is to the advantage of both the political and career leadership to have the opportunity to initiate corrective action before problems become public issues and the subject of congressional investigations.

Pre-audits of the design of administrative and program procedures before they become operational can help ensure that they provide adequate internal controls. In some instances, a limited audit shortly after funds begin to flow has been found to be useful in determining whether the processes are functioning as intended.

Apart from their investigating role, IGs can also provide valuable advice in the development of policies and implementing regulations. While avoiding taking policy positions, an IG can do much to alert the policy makers to operating pitfalls that make programs unnecessarily vulnerable to waste, fraud, and abuse. An IG can also help an incoming agency head by flagging "hot button" items before hearing about them from congressional sources or the media.

*Keep Agency Informed*—The IGs agreed with agency heads about the importance of keeping agency leadership informed of emerging problems as an audit proceeds, thereby facilitating early corrective action. One agency head cited the experience of often first hearing about negative IG findings from Congress or the media, a practice that most IGs try hard to avoid. The workshop revealed that such practices by IGs are increasingly uncommon.

It is established practice for IGs to share draft audit reports with agency management before they are made final. GAO has also used this approach very successfully. It

not only helps the agency, it reduces the likelihood of errors in the final IG report. Several IGs pointed out that they incorporated any agency corrective actions in their final report, a practice that appears to have become quite common. Some IGs also share draft investigative reports, when deemed appropriate and consistent with any requirements for secrecy.

Some enterprising Hill staff are adept at extracting information from IG subordinates before the facts have been thoroughly developed and checked. An IG has a responsibility to take steps to avoid this problem. Because of their dual reporting responsibilities, IGs need to try to make sure that neither the Congress nor the agency head is blindsided.

*Avoid "Gotcha" Image*—In some agencies, there is a perception that IGs are more interested in gaining attention for themselves by pointing the finger at the failures of agency personnel than in helping the agency achieve its program objectives. All the IGs stressed the importance of avoiding practices that might give rise to this perception which is counter-productive for a successful IG. Where IGs are perceived to be performing in this manner, they are not regarded as part of the agency management team and are typically excluded from most policy level meetings.

Agency heads noted that those IGs who had gained the most stature over the years eschewed such a role, recognizing that needed information might be provided to their offices in such situations reluctantly and after much delay. IGs must also be careful to avoid being "used" by individual members of congress or their staffs in order for them to make a case against a particular official or contractor.

*Agency Success*—Both IGs and agency heads agreed that IGs who were more interested in helping the agency succeed than in seeking glory for themselves were the ones who gained influence and respect within the agency. In most cases, they are also the ones who command the most respect in Congress. By participating in agency staff meetings (consistently with the need to maintain independence) and in discussions of important administrative and program issues, the IG's interaction with policy officials fosters mutual respect and trust—important attributes that cannot be provided by a statute.

IGs need to think through carefully how best to explain to an incoming agency head that the task of helping him or her succeed will at times require audit and investigative reports that are quite negative. Past examples of the costly consequences of failing to uncover agency problems at an early stage may be useful.

*Responsiveness*—Agency heads stressed how important it is for IGs to be in a position to respond to their need for a quick audit or review of a problem area. One cited several instances in which he was left exposed to congressional

criticism because of inability to quickly investigate emerging problems or having to hire his own auditors who lacked the familiarity with agency activities that the IG staff possessed. At times this problem has occurred because the IG was completely occupied with congressional requests. But one IG pointed out that, in most cases, it is easier to avoid an unreasonable burden of requests from congress than one might imagine.

The IGs regarded failure to respond to a legitimate need of the agency leadership as an unusual problem. However, there are occasions in which an agency head will ask for review of a rather inconsequential matter, requiring an IG to explain why the staff time needs to be spent on higher priority issues. There have also been instances when an agency head asked for an investigation that amounted to a fishing expedition in which the primary objective was to find something that would provide an excuse for firing an individual. Those at the workshop said they took pride in being able to respond quickly to problems of concern to the agency leadership, that is, both the agency head and the other senior officials. It is important, however, that an agency head realize that once an investigation is begun, it cannot be stopped by the agency and the “chips will have to fall where they may.”

*Professionalism of IG Staff*—It is reassuring to an agency head to learn that the IG staff are experienced and well trained. In addition, the IG can supplement the IG staff by contracts or detailees when there is need to look into an area involving specialized activities for which the IG cannot afford to maintain permanent staff.

A high level of professionalism needs to be demonstrated in the work of the IG staff. One weak report or audit containing substantial mistakes or gaps can severely damage an IG’s reputation, though an effort to achieve total perfection may result in a timid report or one that is stale by the time it is issued. It was stated that IGs should promptly admit mistakes when they occur. They are considered more credible when willing to consider new evidence that might alter earlier conclusions. IG staffs should avoid giving the impression they believe they are always right and that those being audited or investigated are always wrong.

*Give Agency Credit*—Reports should give the agency credit for corrective action that has been taken, or for effective administration if an audit reveals that no corrective action was needed. When agency leadership has requested an audit or investigation, it is wise to make that fact known in the report. By keeping management informed as an audit or investigation proceeds (limited by the occasional need for secrecy in investigations), agency leadership is able to take actions that place them in the role of attacking waste and abuse rather than appearing to tolerate such problems or to be slow in addressing them. IGs should not be concerned about agencies’ receiving credit for actions in which the IG

role may not be given sufficient recognition. Whenever an IG action helps the agency look good in the eyes of Congress or the public, the Office of the Inspector General gains acceptance and support within that agency.

## Responsibility of the Agency Head

Our discussions identified several positive actions an agency head could take to help IGs be more effective in their roles:

*IGs a Part of Management*—Treating IGs as part of the top management team not only increases their knowledge base; it enhances their stature and reduces tension and suspicion. It also increases the IG’s incentive to help agencies succeed in their mission. Involving IGs in the staff meetings of the agency head, as well as meetings called to deal with developing new policies and programs, is an important step. While advising about the risks foreseen in adopting proposed policies is an appropriate role for IGs, it must be recognized that the IG act specifically enjoins an IG from being “an employee who determines policies to be pursued. . . .”

*Attitude of Agency Head*—Whether or not an agency head is known to respect and value the IG’s role has an important bearing on how agency employees view an IG and the degree of cooperation they extend.

*Giving Credit to IGs*—Just as it is wise for IGs to give agencies credit for corrective actions, it is important that agency leadership give recognition to whatever role the IG may have played in agency successes.

*Attend IG Meetings*—From time to time the agency head and/or the deputy can attend an IG staff meeting or special IG sessions convened to address particular agency problems.

*Audit Plan*—The agency head should participate in the development of the annual audit plan.

*Avoid Retaliation*—There have been occasions in which employees who cooperated fully with IGs suffered some retaliation from fellow employees or agency managers, often at the middle management level. Viewed as less common than formerly, it is nonetheless a behavior the agency leadership must take pains to avoid or correct.

## Actions That Limit or Undermine the Role or Effectiveness of IGs

*Isolating the IG*—Agency heads that are highly defensive or not open in their management style tend to sharply limit the extent to which IGs are treated as part of the management

team, thereby limiting the contribution the IG can make to their agency. Excluding IGs from staff meetings and otherwise keeping them out of important agency discussions undermines their ability to serve the agency in many ways. Ignoring the potential value of the IG is counter-productive to the objectives of the political leadership.

*Secrecy*—When agency heads make an effort to keep important matters secret and unavailable to an IG, they eventually learn that cover-up is often even more damaging than the information being withheld. Furthermore, Washington, DC is a “city without secrets.”

*Inaction*—Inaction by the agency head can weaken the ability of an IG to help the leadership and the agency as a whole. Examples are failure to pursue early warnings conveyed by the IG or to develop a serious follow-up program on audits.

*Carrying Independence Too Far*—IGs understandably try to preserve their independence. However, there have been cases where this objective seems, unnecessarily, to have compromised the pursuit of economy and efficiency goals. For example, consistent with government-wide initiatives for seeking assistance from outside of an agency, proposals have been made for IGs to hire outside auditors or to engage IG staff in other agencies under cross-servicing agreements. Because IGs have resisted such proposals, this

has sometimes caused loss of confidence in them as “team players” on the part of agency managers.

### Final Observation

Agency leaders with whom the NAPA fellows have talked emphasize the critical importance the incoming leadership of a new administration should assign to the selection and retention of IGs. Highly qualified IGs can be one of the most valuable members of the top management team. Poorly qualified IGs can do enormous damage within an agency. Therefore, when vacancies occur, it is important to give cognizance to the Inspector General Act of 1978 as amended which requires IGs to be selected solely on the basis of professional qualifications.

These leaders stressed, too, that, before taking their positions, few new agency heads have had the experience of working with an office having the independent role of the IG, particularly the provision in the statute for direct reporting to Congress. The audit function does have some similarity to private business, however, and is the area that is likely to be easiest for new leaders to understand in the beginning. The transition team needs to give special attention to the unique character of these appointees and their value to the new members of the administration. Above all, they must be recognized as occupying professional positions, not political or patronage posts. 🏠

# When the IGs were Pups

## *Reflections on the Early Years of the Inspector General Program*

**I**t has been almost twenty-five years since the Congress passed the Inspector General Act of 1978, and President Jimmy Carter assigned the implementation of this Act to the Office of Management and Budget and to the Department of Justice. The purpose of this article is to reflect on the purposes of the Act and the steps taken by the Executive Branch to implement the programs. When President Carter signed H.R. 8588, which established the Inspector General program on October 22, 1978, he said:

*“I think it is accurate to say the American people are fed up with the treatment of American tax money in a way that involves fraud and mismanagement and embarrassment to the government. I consider, and these Members of the House and Senate behind me, consider the tax money to be a matter of public trust. We have not yet completely succeeded in rooting out the embarrassing aspects of the government management or mismanagement. This bill will go a long way toward resolving that problem.”*

As senior staff in the Office of Management and Budget, the authors of this article had the responsibility for organizing the Executive Branch program to respond to President Carter’s call for a way to “root out fraud, waste and abuse from government programs”. This effort, which today involves thousands of people throughout the government and in those private sector firms who support federal and state government programs, began with a reasonable and clear agenda.

### **The Selection of the First Statutory IG’s**

The IG legislation made it clear that the persons selected for service in each of the departments and agencies included in the Act would have professional standing and knowledge of the issues to be addressed in the audit and investigation functions outlined in the Act. This required an unusual personnel screening and selection process which involved the White House personnel office, the Office of Management and Budget Management Division, the Department of Justice, and the individual federal agencies. Candidates were reviewed carefully before nominations were presented to the president and Congress. We believe that one effect of this intense process was to have different points of view brought to bear on candidate selection, which highlighted the importance of the new program in

the minds of key executive branch officials. This unique selection process brought forward very highly qualified candidates for the new political positions created by the IG Act and gave each of the participating agencies a “stake” in the performance and programs of the IG.

### The Establishment of the Executive Group to Combat Fraud and Waste in Government

A key element in establishing a government-wide fraud and waste prevention program was to find a way to bring together the leadership of the inspector general community and to have them join forces in working on the “means and methods” of conducting their programs in this area. On May 3, 1979, President Carter signed a memorandum to the Attorney General, the Director of the Office of Management and Budget and the Director of the Office of Personnel Management entitled “Improving Management and Combating Fraud and Waste in Federal Programs”. The President wrote:

*“I am establishing an Executive Group to Combat Fraud and Waste in Government to assure effective implementation of the Inspector General Act of 1978 and other efforts to combat fraud and waste in programs of the Federal Government.”*

The goal for this Executive Group was to bring together the inspectors general and other senior federal agency officials to focus on leadership, policies and operational guidance to the IG community. The content of the envisioned program was to:

- (1) promote the coordinated allocation and direction of audit and investigative resources;

- (2) study the common problems and issues relating to fraud and waste which were beyond the capacity of, or authority of, the individual executive departments or agencies; and
- (3) develop recommendations for needed legislation to reduce fraud and waste in the federal government.

The extraordinary cooperation that characterized the early efforts at coordination of the IG program was a direct result of the high quality of the first group of Inspectors General and the leadership provided by John White, the

Deputy Director of OMB; Ben Civiletti, the then Deputy Attorney General of the United States; and Judge William Webster, the Director of the FBI.



### An Early Emphasis on Training and Development of the IG Community

A key element in the minds of many of the founders of the IG program was the concern that Federal Agency officials were not paying sufficient attention to the findings of the audits and investigations performed by agency personnel prior to the IG Act. The findings of evidence of program fraud or abuse was not an end in itself but rather a call to action by agency management to make improvements. One of the key management

goals for the IG program was to create officials of very senior rank who could participate at the highest levels of executive branch and departmental management. The selection of senior professionally qualified IG candidates was an important step in the direction of elevating the functions managed in audit and investigations. There was also a need to carefully train and develop all of the members of this community in professional skills and behavior and the means to communicate their findings to agency program managers and leaders. In detailing the administration’s

efforts to implement the IG Act, President Carter highlighted the need to improve training for audit and investigative personnel in his memo of May 3, 1979. The training and development function continues to be a major focus of the IG Community to this day.

### **The IG as a Member of the Executive Branch Management Team**

Past experiences with audit and investigation findings that did not receive adequate departmental and agency attention led to the belief among the early IG community leadership that the IG should be viewed as a member of the executive branch "management team". The IG, it was hoped, would be a senior member of the departments and agencies top staff, sitting in on all key management staff meetings held by the department and agency leadership. While the independence of the IG necessary to carry out statutory responsibilities was not to be diminished by participating in management meetings in the departments and agencies, the goal was to make available at the highest levels the advice, findings, and conclusions resulting from the IG work.

There was a concern at the very outset of the IG program as to a balance between the needed independence of the IG program and integration of its program into agency operations to make it relevant to agency management. There was considerable unease between congressional and executive branch expectations that had to be resolved through negotiations and operating experience. This process was large successful over time. Another concern

was the need for a reasonable balance between audit and investigative functions. The overall weakness of the audit functions and their lack of visibility in the agencies were one of the arguments for the IG legislation. The investigative functions were very limited in most agencies with almost total reliance on Justice Department resources. Careful protocols had to be developed between the Justice Department and the agency investigative functions.

### **The Next Step in the IG Program**

President Reagan came to office shortly after the start-up of the IG program. He and his staff were vigorous supporters of the concepts and did much to strengthen the program and to make it what it is today, a valued part of the governmental process. Ed Harper (the Deputy Director of OMB) and Ed Meese (senior White House staff member) helped to shape the inspector general program into a major administration program during the Reagan years by establishing the program under an executive order issued early in the new President's term. The "Executive Group" established during President Carter's term was elevated to the status of Council by an Executive Order and was significantly enhanced with staff resources and presidential participation.

Over the past twenty four years, the inspector general program has rewarded its sponsors both legislative and executive with major savings in the resources and the federal government. In addition, it has reassured the American public that the government is well managed and well monitored. 🏠



A key characteristic of PARIS is that its design uses an “open architecture”. An *open architecture* allows the system to be connected easily to *devices* and *programs* made by different manufacturers. Open architectures use off-the-shelf components and conform to approved *standards*. This design allows PARIS to evolve with mainstream electronic initiatives, taking advantage of major technological innovations. Enhancements and new features will be introduced incrementally for each of TIGTA’s functional units (audit, investigations, counsel, management services and information technology). As a result, the system will continue to provide value at a lower cost through the right combination of standards and emerging technologies.

### PARIS Technology

The PARIS system is programmed using a three-part (generally referred to as three-tier) client/server approach. In this programming approach each computer is either a client or a server. Servers are powerful computers dedicated to managing shared services, such as printers, files or databases. Clients are personal computers or workstations on which users run applications. Clients rely on servers for resources, such as files, and even processing power.

This approach was adopted because of its versatility in addressing organizational issues, such as, responsiveness to a geographically dispersed user base, consistent performance, and data security.

The PARIS programs are divided into three well-defined and separate tiers: presentation services, business services, and data services. Each PARIS tier runs on a different computer. The presentation services tier, or user interface, runs on the user’s computer (*the client*) and uses Microsoft Internet Explorer. The business services tier and the data service tier run on different servers, referred to as the *application server* and the *database server*, respectively. Microsoft Internet Information Server (IIS) and Microsoft Transaction Server (MTS) provide the foundation for the business services tier and Microsoft SQL Server supports the data services tier.

The **presentation services tier** is responsible for

- Gathering information from the user
- Sending the information to the business services for processing
- Receiving the results of the business services processing
- Presenting those results to the user

The **business services tier** is responsible for

- Receiving input from the presentation tier
- Interacting with the data services to perform the *business operations* that the application was designed to automate (for example, creating or editing complaints or investigations)
- Validating data and security utilizing user-defined business rules
- Sending the processed results to the presentation tier

The **data services tier** is responsible for the

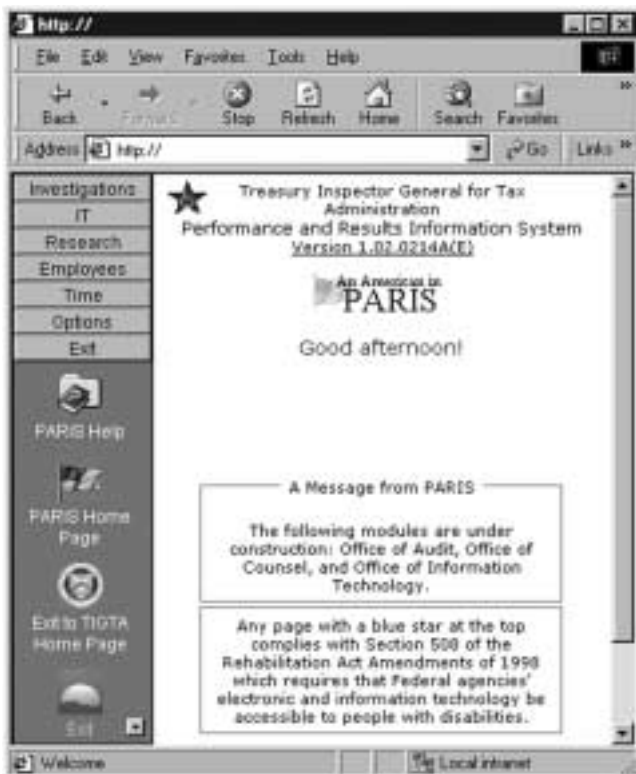
- Storage of data
- Retrieval of data
- Maintenance of data
- Integrity of data

Since PARIS is web-based, the presentation services and business services tiers talk to each other using Hyper-Text Transfer Protocol (HTTP) technology, the underlying protocol used by the world wide web. HTTP defines how messages are formatted and transmitted, and what actions the web server and the browser should take in response to various user commands.

There is no direct connection between the presentation services and data services tier—everything must go through the business services tier. This is an important security feature of PARIS.

### What Does PARIS Do?

PARIS was designed to meet the Management Information System needs of TIGTA’s five business functions. Require-



ments were gathered and those that fell across all business functions were identified as common elements. Implementation of these common elements, or modules, formed the base for the entire PARIS system. The two modules are:

- The **Time** module which has three components. The Activity component collects and reports on an employee's time spent working on activities (e.g., projects, investigations, and audits) that are defined by the system administrator. The Attendance component tracks each employee's time and attendance. The Training component tracks all training courses taken by each employee, primarily to help verify that continuing professional education requirements are met.
- The **Employee Information** module is a database with general and sensitive information about each TIGTA employee. The information is downloaded into PARIS from an external payroll system and the Treasury Integrated Management Information System (TIMIS). Access to sensitive information is controlled to prevent inappropriate disclosure. Additionally, this module contains employee position data and its relation to TIGTA's organizational structure. This allows PARIS, when needed, to direct approval requests to the correct supervisor, including delegated actors.

Once the common applications were completed, the development team began addressing the functions' individual requirements. The Investigations module was the first function to be addressed. This module is comprised of two sections:

- **Complaint Management** captures information concerning any complaint received by TIGTA. This component provides information gathering and reporting on a wide range of information such as the complainant, the subject(s), and status. The module also has a free-form remarks section, and the ability to associate electronic media to the complaint.
- **Investigation Management** captures information concerning TIGTA cases. This component provides information gathering and reporting on case tracking, case history, case assignment, master and spin-off case tracking, index-to-related cases, case remarks, and the ability to associate electronic media to the case. If an investigation is initiated from a complaint, the pertinent complaint informa-

tion is automatically populated to the new investigation. As the investigative data is updated, it is populated back to the original complaint, thus eliminating redundant data entry.

### What Impact does PARIS Have on TIGTA's Efficiency?

The PARIS management information system directly supports TIGTA's statutory mission to conduct investigations relating to the programs and operations of the Internal Revenue Service (IRS) and to inform IRS executives and the Congress of problems in the agency's programs. In performing its mission, PARIS provides the means for TIGTA to collect and analyze timely data for reports to the Department of Justice on criminal investigations, semi-annual reports to Congress, and ad-hoc report requests from stakeholders.

### Is There Springtime in PARIS?

Additional ways for PARIS to support more TIGTA functions is under development. Rather than start from ground zero, we are working with other agencies to streamline our efforts. The ability to start with an existing system to capture and validate user requirements prior to inserting new technology will allow us to get it right the first time—on time.

By listening to our clients and stakeholders we have made PARIS a 'best in class' management information system for TIGTA. Enhanced usefulness of this management tool requires us to ensure that it

- is aligned with requisite procedures and operations to support TIGTA's vision and mission
- promotes cost-effective, innovative processes and emerging technologies
- drives greater efficiency without subjugating effectiveness or quality
- captures and communicates performance measures to our stakeholders

If you would like more information about PARIS or are interested in seeing a demonstration of the system, please contact Cammie Weaver, Director, Customer Service, Office of Information Technology, at (202) 622-4842 or email [cammie.weaver@tigta.treas.gov](mailto:cammie.weaver@tigta.treas.gov). 📧

To truly improve knowledge management in a virtual environment will require both careful consideration of the unique challenges posed by telecommuting and an appreciation for the emerging technologies available to gather and distribute relevant information. One innovation that holds forth great promise to IGs is portals technology. The customized information search capability of portals technology may well serve inspectors general in overcoming the challenges inherent in managing a mobilized work force and to advance the overall knowledge management of their organizations.

### Knowledge Management in a Telecommuting Environment

IGs are highly information dependent organisms. We don't bake bread, pave roads, or tune pianos. We gather, analyze, and report information to influence positive change.

The successful conduct of these information intensive activities is influenced by the setting in which they take place. The traditional office setting of most IGs favors a productive flow of information. Concentrating the flow of information and ideas into central locations for immediate access and distribution is common to IGs. Directing the flow of information in this manner promotes creativity and innovation. IGs with high concentrations of employees in close proximity to one another are traditionally productive and efficient in their operations. Any diminution in the inflow and outflow of information, however, will threaten this life force over time.

Interestingly, the recognition that communications and the free flow of information intensify when the players are strategically located in close proximity to one another has inspired a new view of knowledge management, one that runs somewhat contrary to the presumptive appeal of telecommuting. Malcolm Gladwell, in a recent article entitled "Designs for Working" published in *The New Yorker* advances the view that offices should be designed in a way to promote desired interactive patterns. The properly designed workspace should "foster creativity and serendipity," he maintains. Malcolm points out that private companies are deconstructing their traditional office space and moving to designs that promote a desired flow of information. He cites the Ford Motor Company, which adopted a war room approach to situating its software developers at work. In introducing Ford's strategy Malcolm says:

*"In the war-room study, the company moved the client, the programmers, and a manager into a dedicated conference room, and made them stay there until the project was done. Using the war room cut the software-development time by two-thirds, in part because there was far less time wasted on formal meetings or calls outside the building: the people who ought to have been*

*bumping into each other were now sitting next to each other."*<sup>3</sup>

OIG managers should heed Malcolm's principle observation that the flow of information is affected by the proximity of its authors and users to one another. When designing protocols for information collection and distribution in the virtual work environment of telecommuting, OIGs will need to protect against the limitations imposed by employees working in locations remote from the people with whom they interact routinely.

Another implication of telecommuting on knowledge management goes beyond the effectiveness of information sharing in a closed environment to the efficiency of data collection. Malcolm alluded to this in discussing the benefits of locating team members together when he acknowledged that Ford reduced its development time by a staggering two-thirds. Information gathering is time consuming. A common industry standard has it that knowledge workers spend 30% of their time gathering and distributing information. OIGs must be positioned to protect against the risk of delaying the time it takes to collect and distribute critical information to its mobile workers.

### The Knowledge Management Challenge to Telecommuting

The challenge to managers in ensuring a free and efficient flow of information to a distributed work force of telecommuters seems clear. This challenge may be characterized as follows:

- How do you distribute information to the right people?
- How do you distribute information in a telecommuting environment without a corresponding increase in time and labor?
- How do you preserve the intimacy of the office environment so as to capture the creative opportunities forged by committed and talented professionals working together?

### Portal Technology

Like all contemporary knowledge management dilemmas, the answers to these questions can be found at only one source: technology. Managers need an automated and efficient means to distribute content-rich information to and from their telecommuters. Most companies and government agencies that have implemented telecommuting programs recognize the critical dependence on new technologies to support home based workers. Many telecommuting programs, including the pilot telecommuting program at the Treasury Inspector General for Tax Administration, provide high-speed telecommunications service to its mobile workers to facilitate the rapid transfer of large amounts of data.

Important as these investments may be to maintaining a telecommunications infrastructure though, they only constitute the means to deliver data and information. What is needed is a technology to identify and transmit meaningful, task-specific information to support the unique needs of the IG. Portals technology could be the automated solution to this need.

What is portals technology? "Portals" is the generic name for a software application that provides users with a personalized desktop that can be customized to search, navigate and view selected information. The information may originate from inside or outside an organization. The technology is produced by several companies and sold under various brand names. Unlike a static Internet or Intranet-based web page offering a fixed array of information to a user, a portal personalizes the delivery of information.

Users customize their information needs in such a way as to limit what they receive to only what interests them. Using a standard browser interface, employees establish their data and information needs.

The search and navigation applications of portals continuously search public web sites and private data sources to which the user may have access. Further, users configure the manner and frequency with which the retrieved information is viewed on their personal computers.

### Filter, Aggregate, and Push

By establishing the specific parameters of the user's information needs, portals technology limits the information it retrieves to avoid overwhelming workers with more information than they can use. The technology filters initial matches and refines them to limit the responses in accordance with the level of specificity established in the user's directory. By continuously searching all public data sources, it can integrate disparate data from multiple locations. Portals provide the added function of summarizing long documents into an abbreviated format for the ease of the user. Thus, the mundane work of searching for data is reduced, allowing added time for employees to analyze information.

Recognizing that the data needs of its users may be time sensitive, Portals employs a "push" function to transmit immediate alerts when key events occur or when data attains specified threshold levels or matches designated profiling characteristics. In pushing alerts to users, the technology is flexible enough to route information to both personal com-

puters and hand-held communications devices, regardless of the user's location or the format and structure of the data.

Thus, portals technology allows knowledge managers to step back from the task of actively seeking information of interest and rely on the filter and search capability to do it for them. Andy Warzecha, vice president, Electronic Business Strategies, characterized the business demand for this information service at a recent presentation on behalf of the META Group: "Do the surfing for me, but make it relevant!"

### Information Distribution and Collaborative Communications

With portals technology, users can predetermine the distribution of information as it is collected and rely on it to automatically distribute documents and information to interested users in an organization. Data can be stored and retrieved securely and shared throughout the organization.

Access controls over shared information may be introduced to limit the levels of review to provide security and protect confidentiality.

In addition to distributing information throughout the organization, it may also be used to conduct integrated discussions among groups located apart from each other. Users may communicate on-line and



may work cooperatively to develop products. Document development and review may be conducted either simultaneously or sequentially, thus allowing organizations to realize the creative benefit of collaboration or to maintain the order and quality assurance from successive reviews through their chain of command.

The appeal of portals as a way to create an interactive way of sharing pertinent information easily and productively was summarily characterized by Cynthia Flash in a recent article:

*"A true knowledge management portal is one that brings together various data and technology systems from within a company and makes it easier for workers to gather and share information through a corporate Intranet and online. The portal will allow workers to extract data that otherwise is hidden inside systems and oftentimes only*

*available to the information technology staff. The idea is not just to gather information, but to present it so employees can interact with it and contribute back so others can learn from it, too".<sup>4</sup>*

## Portals Technology and the Knowledge Management Challenge of Telecommuting

Portals technology offers an innovative opportunity to satisfy the information needs of telecommuters in an immediate and efficient way. By tapering the information search to only the data and text of interest to specific employees, each user is assured of receiving the critical and relevant information he or she needs to perform a job. By relying on the search and navigational tools, along with the alert function of portals, organizations may increase the availability and productivity of their workforce due to the time and labor saved from no longer searching and distributing information. Last, by distributing information of common interest and conducting on-line communications, organizations may preserve the sense of community and constructive interaction among its workers. For these reasons, portals technology very well may provide a solution to the knowledge management limitations imposed by telecommuting.

The application of portals to telecommuting was evident in an article published recently in Knowledge Management magazine. The author, Sara L. Roberts-Witt, discusses how Compaq Computer approached the task of reducing the time spent answering e-mail, locating marketing materials and coordinating transatlantic conference calls for its 2,000 member global sales force, most of whom work remotely or from their homes. She writes:

*"A successful portal must offer workers compelling reasons to change their work habits . . . According to Sarah Thomas, the Internet strategist for Compaq's marketing and communications division and the lead manager on the project, a portal was the right solution because it could centralize and simplify both communications and the distribution of materials to members of the sales force. The team found that the users wanted the portal to supply basic information they needed to do their work, such as account news, product updates and information specific to their own teams. But they did not want to have to spend as much time at the portal as the e-mail system required."<sup>5</sup>*

## Knowledge Management: Looking Beyond Telecommuting

The use of portals technology to overcome the knowledge management challenges of telecommuting is modest when

compared to its potential application to the overall business processes of OIGs. Consider the capabilities of the search and navigation features of portals and their potential use to the IG community in conducting its work. Portals technology can be used to automatically examine data and documents from disparate sources and to understand and investigate the internal, logical relationships among them. This will allow IG professionals to use internal and external information resources innovatively. Auditors, investigators and others may ask questions about the data at their disposal that are of unique concern to specific projects and assignments and may communicate the results in customized reports. Through the use of multidimensional analysis users may examine their organizations from many perspectives, including comparing them against external points of view.

This capability—equipping each user with the capability of applying business intelligence to data sources—will allow users to identify trends, relationships, patterns and vulnerabilities. It will also permit IG staff to benchmark against other organizations and to conduct comparative analysis of information. Given the specificity with which the information may be contoured and the immediacy of its delivery, this technology could influence their oversight function significantly.

The potential application of this technology to the business operation of the inspectors general was implicit in an article published in the January 9, 2001 on-line edition of Business Week. The author described the implementation of the portals software produced by the Hummingbird Company to the field of law enforcement:

*"Even police departments are getting into the act. In Detroit, 75 police agencies in four counties use Hummingbird's software to keep track of the more than 2 million crimes committed every year. Supervisors can run a query, say, of how many robberies took place by precinct, by time of day, even by whether it was rainy or clear. The hope? That by using the information they will be able to marshal personnel and resources quickly and efficiently in order to nab culprits before they strike again."<sup>6</sup>*

Through the targeted use of this technology to monitor and query data sources, inspectors general can look to improve their ability to conduct:

- Trend analysis
- Risk assessment
- Data compilation and extraction
- Audit follow up
- Early detection and intervention
- Monitoring of changes in laws, regulations, and programs

With these automated enhancements, inspectors general will be well positioned to build a strong ability to

intervene timely when circumstances warrant and to predict trends and occurrences within the agencies they oversee.

## **Conclusion**

Recent trends in employment practices in the federal government are attractive. They offer opportunities to improve the quality of life for the work force and to achieve true benefits to the taxpayers through improved service and efficiency. These trends however, introduce challenges which may not be as evident as the opportunities. One challenge inspectors general need to keep in the forefront is the need to maintain the integrity of their business operations and avoid any diminution from poorly designed telecommuting programs. One way to fortify the programs is to consider the use of emerging technologies to support the knowledge management aspects of our work. These technologies hold forth more than a means to manage work flow in a telecommuting environment—they offer broad opportunity for improved depth and efficiency in the oversight functions of inspectors general as a whole. 📧

## **References:**

1. Mary McClintock, Nortel Networks, "Implementing a Winning Teleworking Program". Washington Area Knowledge Management Conference on Telework and Telework America Day, October 24, 2000.
2. Wilson, Scott (2000). "Romancing the Tone: Powerful Possibilities for Offsite Workplaces." *Journal of Public Inquiry*: Fall/Winter 2000.
3. Hall, Jessica A. (2000). "From a Distance: Telecommuting in the Federal Workplace." *Journal of Public Inquiry*: Fall/Winter 2000.
4. Gladwell, Malcolm (2000). "Designs for Working: Why your Bosses Want to Turn Your New Office into Greenwich Village." *The New Yorker*: December 11, 2000. p. 66.
5. Flash, Cynthia (2000). "Knowledge Management Meets the Portal: Combining Knowledge Management and Corporate Portals Helps Companies and Their Employees Gather, Manage, Share, and Use Previously Disparate Information." *Earthweb.com*: November 28, 2000 p.2.
6. Roberts-Witt, Sara L. (2000). "Planning Out a Portal: Taking Advantage of This Hot Technology Requires Careful Planning and Research to Avoid Potential Pitfalls". *Knowledge Management Magazine* December 16, 2000 p.3.
7. Brown, Jeanette (2001). "Why Hummingbird Is Soaring: Data Portals". *Business Week* online: January 9, 2001 p.1.

## Focus of the IG's Work

The team determined early on that senior management at the Corporation must make the critical decisions on Internet use. Thus, a primary goal of the review was to provide corporate managers with decision factors needed to determine and implement the most effective, cost beneficial control strategy for the FDIC. These decision factors included

- FDIC line managers' ideas and opinions concerning the extent of Internet use and misuse
- Legal issues and recent legal decisions concerning privacy and Internet/email monitoring
- Best practices from other federal agencies and the private sector
- Information on advanced software blocking and monitoring tools and capabilities<sup>1</sup>
- Analysis of the FDIC's technical capabilities to implement monitoring programs.

As a starting point, the team surveyed all FDIC managers from every division to solicit their opinions and ideas. The survey was designed to determine the 135 managers' views on three key questions: (1) Were employees visiting sites considered inappropriate for the FDIC's work environment? (2) Were employees spending too much time on the Internet? (3) Did management feel that more restrictions and controls over employee Inter-

<sup>1</sup> Blocking prevents users from accessing Internet sites while monitoring may allow access to sites but will record all access, the user, and time spent.

net use were in order? We received a wide range of opinions, but on some key issues the managers' views were generally shared. Management did not believe that FDIC employees visited sites considered inappropriate for the work environment. Nor did managers feel that their employees spent too much time using the Internet at work. Managers generally did not think that a formal, corporate-wide monitoring strategy was needed. They did advocate training employees on the appropriate use of the Internet

and discouraged controls that would restrict Internet use. We believe this to be one of the most important decision factors that we provided to the FDIC's operating committee.

The primary focus of our work on the legal issues involved with employee Internet use related to privacy matters and the extent to which organizations can monitor or block Internet and e-mail use. Secondly, organizations can be sued by their employees if inappropriate material (e.g., pornographic, racial, or hateful in nature) is circulated via e-mail and Internet. However, we determined that the FDIC is protected because of an unequivocal policy that does not tolerate racial discrimination, sexual harassment, or a hostile working environment, regardless of the medium in question.

We discussed these

types of considerations with IG and FDIC counsel and shared our information and views on these issues with management as well.

Our review of other federal agencies' best practices proved to be especially valuable. The IG coordinated with National Credit Union Administration, the Federal Reserve, Department of State, Department of the Treasury, the U.S. General Accounting Office, the Federal Communications Commission, Department of Justice, and Department of Veterans Affairs to determine how these agencies dealt with



the Internet use issue. Some of the control strategies employed by these organizations included employee acknowledgement of an Internet use policy, start-up screen warning banners, email use monitoring, Internet site blocking, and Internet use monitoring. Not only did the audit staff obtain valuable information to pass along to FDIC management, they were also able to share their research with the IT managers of the other agencies. These managers were appreciative of the assistance we provided for they were well aware of the dynamic nature of Internet use and knew that our work was attempting to capture the latest legal, technical, and control issues. Some of the managers suggested a user group be formed to continue this line of discussion and assistance.

With respect to possible blocking and monitoring tools and the FDIC's capabilities in that regard, we determined that the FDIC's hardware/software environment at the time limited developing in-house corporate-wide monitoring capabilities. However we communicated to the agency that the environment was compatible with off-the-shelf software that could provide daily reports of specific users' Internet use. Such software licenses also would provide the most effective Internet blocking capabilities whereby the vendor could provide the FDIC periodic updates on new sites considered inappropriate, and managers could choose which should be blocked. Again, it was our hope that this type of information would help guide corporate decisions.

The unique nature of our review required the IG to coordinate especially closely with representatives of the FDIC's various divisions. We held discussions with representatives from the Legal Division, Division of Administration, and Division of Information Resources Management. We also organized meetings with managers from other divisions to discuss together the issues of implementing and managing an Internet monitoring program. These discussions served to strengthen the IG's partnerships with the other FDIC groups.

## Communicating Results

We shared our research and conclusions with a broad range of FDIC staff. We made PowerPoint presentations to the IT and Legal Division senior managers and then to the Operating Committee. During the presentation to the Operating Committee, we offered IG assistance for any future presentations, development of training sessions or videos, and discussions related to implementing Internet controls. We also prepared a formal presentation document that was distributed during the meetings and to FDIC managers upon request. That document contained the briefing slides, tabulated results of the survey of 135 representatives of management, information related to the control strategies used by other agencies, suggestions for an effective Internet use policy (based on Chief Information Officer Council

policy), and a listing of suggested references that contained additional information on Internet use issues.

We shared the presentation document with other OIGs from other Federal Financial Institution Examination Council member agencies (the Federal Reserve Board, Office of Thrift Supervision, Department of the Treasury, Office of the Comptroller of the Currency, and National Credit Union Administration) and again contacted the other federal agencies with whom we had spoken to provide them the overall results of our work. After briefing the Operating Committee, we also provided the document to the FDIC Audit Committee. Clearly, effective policy and practice is the responsibility of many at the FDIC.

## Suggestions Have Impact

As a result of our work we suggested a phased approach to a revision of the FDIC's employee Internet use policy. Legal and social issues call for a clearly worded, well communicated, and consistently enforced policy. As mentioned earlier, we made a number of suggestions for an effective policy that were based on the Chief Information Officers Council policy. These suggestions included addressing privacy expectations; clearly specifying what constitutes inappropriate use; outlining e-mail retention policies and procedures, considering government record retention requirements and Freedom of Information Act requests; updating descriptions of the present operating environment; and determining the corporate resources needed to support Internet and e-mail policy.

Additionally, with respect to directly communicating Internet policy to employees, one of our more important suggestions was that inappropriate Internet use be discussed in future Ethics and User Security training sessions that are conducted annually. We also suggested that on-line banners be used to remind users each time they use e-mail and the Internet that their use is not private and can be monitored.


Our work had significant impact. The FDIC sent a global e-mail detailing proper use of the Internet and e-mail, developed an on-screen banner for every initial log-on to the network, and implemented blocking devices. Additionally, the agency is now including Internet use in its corporate-wide security training and in annual ethics training, and is modifying its written Internet and e-mail use policy.

This project proved quite different from other IG audit projects and its impact went beyond strict issues of Internet use. The emerging issues related to Internet and e-mail risks required us to take a more dynamic fieldwork approach so that we could quickly provide senior managers information concerning threats to the Corporation and possible control tools and strategies. Although we did not make formal recommendations, we formulated and presented what we believed were effective control strategies based on our research. Rather than use a traditional audit report to present our results, the team chose to use alternate reporting



mechanisms—briefing documents that were tailored to different audiences. The fieldwork proved different in that it involved sharing ideas and knowledge in a concerted effort to reach the best solution for the FDIC. This two-way communication extended to our relationships with the outside agencies as well. We hope and expect to maintain these productive working relationships with all FDIC divisions

and other federal agencies as we continue to explore and revisit these challenging issues.

The FDIC IG welcomes comments or questions related to our work on Employee Internet Use. What has your organization done to address Internet use issues? We'd like to know. Please contact Jack Talbert (202) 416-2965 or Marshall Gray (202) 416-4086. 

*the mission or operations of a department or agency and does not violate the Standards of Ethical Conduct for Employees of the Executive Branch.”*

As is required with many seemingly self evident statements, the model policy provides definitions to avoid confusion or misinterpretation:

- *Privilege* means, in the context of this policy, that the executive branch of the federal government is extending the opportunity to its employees to use government property for personal use in an effort to create a more supportive work environment. However, this policy does not create a right to use government office equipment for non-government purposes. Nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes.

- *Government office equipment* (including information technology) consists of but is not limited to: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity and access to internet services, and E-mail. This list is provided to show examples of office equipment as envisioned by this policy. Executive branch managers may include additional types of office equipment.

- *Minimal additional expense* means that employee's personal use of government office equipment is limited to those situations where the government is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the govern-

ment or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include, making a few photocopies, using a computer printer to printout a few pages of material, making occasional brief personal phone calls (within agency policy and 41 CFR 101-35.201), infrequently sending personal E-mail messages, or limited use of the Internet for personal reasons.

- *Employee non-work time* means times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use government office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).

- *Personal use* means activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Executive branch employees are specifically pro-

hibited from using government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal private business also includes employees using government office equipment to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of government office equipment to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization (examples).



And again to clarify the government's intent and expectations, the model policy also provides discrete examples of prohibited activity:

1. Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, video, sound or other large file attachments can degrade the performance of the entire network.
2. Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.
3. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
4. Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but is not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
5. The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;
6. The creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc.
7. Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services).
8. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
9. Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained or uses at odds with the agencies mission or positions.
10. Any use that could generate more than minimal additional expense to the government.
11. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual

property rights (beyond fair use), proprietary data, or export controlled software or data.

The effective implementation of this policy requires trust and maturity on all sides. An unstated assumption of this policy is the support of our managers. An employee who spends time in the morning "web-surfing" is little different from the one who spends it reading the newspaper. The effectiveness of this policy will depend on managers doing their job. On the other side of this equation are our employees, who for the most part have demonstrated their professionalism and integrity in this area even without the benefit of relevant policy. It is accepted that there will be those who will attempt to abuse this privilege, as they would any other extended to them. It is important that we treat this as any other workplace performance issue and not create a new category of misconduct.

An important aspect of the effort by the CIO Council to issue a "Model" policy, is a desire to effect some uniformity across the federal government. At this time many agencies ostensibly forbid all employee use of office equipment or Internet access, yet turn their back on the reality that virtually anyone with an Internet connection is using it for some personal reasons. The model policy gives a framework for agencies to construct a realist policy that can bound the problem. It also provides a better environment to discipline the true abusers of the system who have cried foul for "selective enforcement" when they have been caught under the current situation.

Explicit within this new policy is that this limited use is a privilege not a right. As with any privilege, circumstances or misuse may result in the withdrawal of the privilege. The government extends this limited privilege with no expectation of privacy. While we may allow an employee to send a personal email from the office, he/she must understand that this activity is subject to analysis and monitoring. It would be impossible to maintain any

**Executive Branch employees should be provided with a professional supportive work environment. They should be given the tools needed to effectively carry out their assigned responsibilities. Allowing limited personal use of these tools helps enhance the quality of the workplace and helps the Government to retain highly qualified and skilled workers.**

semblance of security on our information systems if we cannot monitor and control the flow of information across the boundaries. In addition to the policy, our systems should remind users at logon that ALL activity is subject to monitoring and possible resulting disciplinary action.

Important in the understanding of this policy is that it does not support the use of any additional electronic monitoring of the employee workplace to detect misuse of government resources. One of the primary purposes of this policy is to recognize the expectation of a new generation of workers for internet access and ensure that the government is able to provide a workplace that is competitive with the civil sector. Should this policy be used as the rationale for increased or extraordinary electronic surveillance, this could produce the mistrust and paranoia that will make it even harder to find qualified workers.

Additional issues to be addressed by any agency implementing a "Personal Use" policy include sanctions for misuse and exceptions for previously negotiated labor agreements. Sanctions for misuse are generally spelled out in existing instructions and regulations. Penalties for unauthorized or improper use include: loss of use or limitations on the use of the information technology resources, disciplinary or adverse actions, termination, criminal penalties and/or the employee's being held financially liable for the cost of improper use. Agencies should involve their unions early—before adopting and completing any labor relations obligations for bargaining, where appropriate. The labor-management relations partnerships should be consulted during Agency's consideration of adopting new policy. It should be indicated, if appropriate, that the policy does not apply to union representatives when fulfilling their official capacity for the union. Agencies should consult their col-

lective bargaining agreements for the procedures and rules that apply to the union's use of equipment and technology under those conditions. However, when union representatives are not engaged in their union representation responsibilities, the new policy should apply.

The drafting of the current model brought complaints from both sides. Traditionalists who protested that this would be wasting government resources by allowing any personal use and those who felt that if employees were getting their work done that we should allow use at any time, as long as there was no significant cost to the government. Some saw the costs of incremental Internet use as a good investment against the problem of retaining our technical workforce. The current model seems to have struck a balance between the opposing interests, and as a model, can be adjusted to accommodate unique agency requirements.

The "Model" policy is but one example of the efforts of the federal CIO Council to address the issues of management, employees, and above all the citizens of our country as we attempt to exploit new technology to provide new and better services while conserving resources and tax dollars. Please feel free to provide your comments on this or any other relevant issue. (Email at [ciocouncil.support@gsa.gov](mailto:ciocouncil.support@gsa.gov))

Related Authorities for the Model Policy:

**5 CFR 2635**—Standards of Ethical Conduct for Employees of the Executive Branch

**Part 1 of Executive Order 12674**—Implementing Standards of Ethical Conduct for Employees of the Executive Branch

**5 CFR 301**—Departmental Regulations

**41 CFR 101-35. 201**—TELECOMMUNICATIONS MANAGEMENT POLICY 

- In 1998, Congress passed the Government Paperwork Elimination Act, which directed the development of paperless record keeping for many government agencies, as well as contractors, grantees and aid recipients who interact with government agencies. As a result, affected federal agencies are moving to develop paperless record keeping systems to meet the Act's October 2003 implementation date.
- In 2000, Congress passed the E-Sign Act, making electronically signed contracts and agreements legally binding.
- In 2000, Congress passed GISRA. The Act was the first comprehensive change in federal computer security since 1987. It required most federal agencies to improve computer security policies and procedures, as well as to appoint a chief information security officer. The Act also required the agency IG to perform an annual review of agency computer security.
- For the last eight years, the Clinton administration actively promoted the deployment of electronic government systems to provide the public with computer based access to government agencies, information and programs.

During this same period of time, a series of audit and investigative initiatives also focused on federal computer security issues. The General Accounting Office (GAO) commenced a series of audits on computer security at major federal agencies, such as the Department of State and National Aeronautic and Space Administration (NASA). The IG community, too, initiated a series of audits to assess agency compliance with the critical asset protection requirements of PDD 63. These GAO and IG audits have identified major security weaknesses in critical computer systems. Furthermore, in response to PDD 63, federal law enforcement directed more resources to identifying and responding to criminal attacks on the federal computer infrastructure. For example:

- Under PDD 63, the Federal Bureau of Investigation was charged with operating the National Infrastructure Protection Center (NIPC) to coordinate federal law enforcement response to computer attacks. Representatives of IG investigative organizations have been detailed to NIPC.
- Inspectors General at agencies such as NASA, the Department of Defense (DoD), the Department of Energy, the Internal Revenue Service and the Postal Service either created or greatly expanded their investigative capabilities in the area of computer crimes.
- A Computer Intrusion Working Group was formed to improve sharing of information and techniques among IG investigators.
- The DoD created a Defense Computer Forensics Laboratory to provide centralized computer forensic support for DoD law enforcement activities.

Audit and investigative activity by the IG community regarding computer security is expected to continue to grow. In a November 2000 survey performed for the President's Council on Integrity and Efficiency, the IG community identified that during the period FY 1997-2000, the 26 reporting inspectors general performed 162 system security audits. The survey also reported that, as a result of GISRA, the reporting inspectors general would need to perform 272 computer security audits during the period FY 2001-2004. However, trained staffing and funding limitations would only allow 159 such audits to be performed. This is virtually the same level of audit activity that was performed before the passage of GISRA.

### **The Need for Cost Effective Computer Security Assessment Procedures in the IG Community**

In order to meet the challenge of the statutory requirements of GISRA, there is a clear need in the IG community for greater training in the area of computer security, for a better understanding of the tools and techniques that are used by computer security professionals to detect and respond to hackers, and to assess the status of network security.

Joint training initiatives have proven to be successful. For example, since February 1999 almost 500 auditors, investigators and computer security professionals from the IG community and other participating federal agencies have attended computer intrusion training sponsored by the Postal Service OIG. By working together, on this training initiative, a significant portion of the IG audit and investigative community has obtained excellent training in a cost effective manner.

Similarly, in order to meet the required but unfunded requirements of GISRA, the IG community needs to examine ways to perform computer security audits and assessments in a more cost effective manner. One of the essential tools that can be used to assess computer security is penetration testing of agency computer systems.

#### ***What is penetration testing?***

Penetration testing is the use of sophisticated tools and techniques to assess the adequacy of a computer network's security. The primary forms of penetration testing include the use of automated commercially-available scanning programs and password crackers to examine computer networks for known weaknesses and vulnerabilities. These tests can also involve automated scans of phone systems to detect the presence of unauthorized computer modems. Sophisticated penetration tests can also involve the use of social engineering techniques – pretext contacts with agency personnel to solicit the provision of passwords and other security controls to unauthorized persons. Finally, penetration tests can also involve the exploitation of discovered vulnerabilities to actually take root or administrator privileges of tested systems.

In its assessments of federal agency computer security, the GAO has repeatedly performed penetration tests, and has urged the IG community to use such tests to assess the computer security of their respective agencies. In their response to the November 2000 PCIE survey, the reporting Inspectors General stated that during the period FY 1997-2000, 30 external penetration tests<sup>2</sup> were performed. Of this number, 22 were not performed by IG staff, but were performed by contractors for the IG. During this same period, 54 internal penetration tests<sup>3</sup> were performed, 44 of which were done by contractors. During the period FY 2001-2004, 292 penetration tests (143 external 149 internal) were planned by the IG community. This amounts to triple the volume of tests performed in the preceding three years. However, due to trained staffing and budget restraints, only 224 of these tests could be accomplished. While the survey did not identify how many of these tests would be performed using contractors, prior experience has shown that contractors perform the majority of these tests. If the average cost of a single penetration test is \$50,000, IG expenditure for 200 contractor penetration tests could exceed \$10,000,000.

Because penetration testing is an important computer security tool, and because this tool can assist both auditors and investigators in identifying hackers and network security vulnerabilities, the IG community should consider developing the in-house capability to perform these tests in a cost effective manner.

#### ***What are some of the costs in establishing an effective penetration testing program?***

The USPS OIG Computer Intrusion team has developed the in-house capability to perform penetration testing to support the audit and investigative mission of the OIG regarding computer security. The OIG staff assigned to the team has been trained in the use of commercial and freeware testing tools, as well as “social engineering” techniques. Critical postal computer systems have been identified, and an agency wide testing plan has been developed. Included in the plan are penetration tests to support IG audit activities, requests from management to perform independent security tests, and tests to assess vulnerabilities in postal e-business initiatives prior to their deployment.<sup>4</sup>

Based upon our experience, an IG office that is considering the development of an in-house penetration testing

<sup>2</sup>An external penetration test is an examination of the security of a computer system from attacks from outside of the network.

<sup>3</sup>An internal penetration test is an examination of the security of a computer system from attacks by persons who have authorized access to the network.

<sup>4</sup>Penetration tests by the OIG should not be viewed as a substitute for penetration testing by agency system administrators. Penetration testing is a well recognized computer security tool that should be performed on a regular basis by agency computer security personnel. The OIG penetration tests should be viewed as an additional independent assessment of system security.

program should be aware of the resources necessary to operate a penetration testing team. In order to perform penetration tests, an IG organization will require a number of costly resources:

- *Automated tools*—Effective penetration testing requires the acquisition of a number of sophisticated commercial scanning tools, such as Phonsweep, Cybercop, and ISS Network, Security and Internet Scanners. The site licenses for this suite of tools can be in excess of \$50,000-100,000 per year. In addition to acquiring these tools, the IG staff must be fully trained on their use to ensure effective testing without disrupting or destroying agency computer network operations. (It should be noted that freeware testing tools, such as Netmap, SATAN and Nessus, should also be part of any professional testing suite of tools.)
- *Specialized staff*—The IG staff must have a thorough background in computer security, computer operations, diverse computer operating systems (Unix, Linux, NT, Solaris), network operation protocols (TCP/IP), as well as a complete understanding of current hacker methodologies and techniques. This will normally involve the use of trained computer specialists, computer intrusion investigators or CISA auditors. While manufacturers of commercial tools usually provide training in these tools at an additional cost, the only training which is available on freeware tools is practical experience.
- *Specialized equipment*—In order to perform penetration tests on multiple computer systems, powerful laptop computers with significant operation and storage capabilities should be utilized. Furthermore, in order to remain current with rapidly developing technology, the hardware requires frequent improvements and upgrades. The average initial hardware cost for equipping a penetration testing team will be in the range of \$60,000. Furthermore, in order to provide high-speed connectivity for the team’s activities, a T-1 line should be provided. Costs for a T-1 line are approximately \$17,000/year. (Regular phone service or DSL lines can be used, but will result in a much slower testing process.)

#### **How Can a Centralized Penetration Testing Laboratory Assist the OIGs?**

While some IG offices, such as the Postal Service OIG, have made a significant investment in developing an in-house capability to conduct penetration testing, the recruitment, retention and equipping of a trained penetration testing team may be beyond the fiscal means of many inspectors general. Trained computer specialists, computer intrusion investigators and CISA auditors are in short sup-

ply, and command salaries in the GS 13-15 range. Hardware and software costs for equipping such a testing team can exceed \$250,000. Few of the current 57 OIGs can afford the “start-up” costs of such operations. Furthermore, given the current demand for trained computer security experts, the OIG community cannot afford to engage in fratricidal hiring practices.

While the IG community has contracted out much of its penetration testing to date, this method also presents a number of problems:

- ✓ Penetration testing costs average \$50,000 per test.
- ✓ Many penetration tests performed by outside contractors amount to little more than unsophisticated scanning of an agency’s network. Paying a contractor \$50,000 to run a free automated tool, such as Netmap which generates an automated report, is neither cost effective nor a meaningful assessment of the agency’s network. A properly performed penetration test should include a full suite of penetration testing techniques, such as password cracking, modem sweeps, social engineering and the non-destructive exploitation of discovered vulnerabilities. Such tests are expensive and beyond the capability of many contractors offering “penetration testing services.”
- ✓ By contracting out these services, the IG office is precluding the development of important computer security skills by its own audit and investigative staff. Computer security auditors and computer intrusion investigators require a thorough understanding of agency network topology and vulnerabilities, as well as hacker tools and techniques. In-house penetration testing provides this skill to the IG staff.

In lieu of creating a penetration testing team in each OIG, consideration should be given to creating a centralized OIG Penetration Testing Laboratory that could provide penetration testing support to those in the IG community that cannot afford to make the commitment to establish such a team. The laboratory could be centrally located under the aegis of the OIG Forensic Laboratory that was created by the Inspector General Act amendments of 2000<sup>5</sup>. Under this concept, a centralized recruitment of trained personnel, and acquisition of penetration testing tools and equipment could support penetration tests for the entire IG community.

Precedent for consolidation of computer related activities has recently been demonstrated by DoD. In 1998, in lieu of creating computer forensic laboratories for each of the four Defense Criminal Investigative Organizations, DoD chose to create the Defense Computer Forensics Laboratory, a centralized computer forensics facility to support all DoD criminal investigations.

<sup>5</sup>PL 106-422.

A centralized penetration testing team concept could work as follows:

- Each participating OIG would determine what computer network reviews would be conducted on an annual basis, as is required by GISRA;
- Each participating OIG would determine how many penetration tests would be required as part of the annual OIG review of computer security;
- Each participating OIG would then submit to the OIG Forensics Lab and annual plan for penetration tests to support each OIG’s annual review plan;
- The OIG Forensics Laboratory would establish an annual multi-agency penetration testing plan to support participating OIGs. (Sufficient flexibility should exist in the annual plan to allow for additional testing of new and/or critical systems that were not part of the original annual plan);
- Prior to the commencement of the scheduled penetration test, each participating OIG will research the topology of the network to be tested and coordinate the performance of the test with affected agency officials. (In order to ensure the validity of the tests, some tests may have minimal advanced notice to the affected agency.)
- Staff of the OIG Forensics Laboratory will perform the tests and provide the results of the test to the requesting OIG on a timely basis. (Staff of the requesting OIG could also observe the performance of the test).
- The requesting OIG will then issue the test results to affected agency management for appropriate corrective action.

In order to obtain training on the use of penetration testing tools, participating OIGs could detail staff to the OIG Forensics Laboratory for a period of time. While assigned to the Laboratory, the detailed OIG staff would be trained in the performance of penetration tests, and be supervised by the staff of the Laboratory while performing the tests. This procedure would benefit the IG community in a number of ways:

- Participating OIGs would obtain critical hands on experience for their staff in a cost effective manner
- The OIG Forensics Laboratory could reduce the number of staff permanently assigned to the Laboratory
- The OIG Forensics Laboratory could perform more tests for the IG community

By centralizing the performance of penetration testing, the OIG community can ensure that these valuable services are performed in a consistent, high quality, and cost effective manner as part of their annual computer security reviews. Centralization will also assist the IG community in meeting its statutory obligations under GISRA. 🏠

One of the most disturbing things that the Committee learned during the course of the investigation did not involve Mr. Prosser, but rather his two predecessors. The position of TVA IG was established in 1986. The first IG appointed by the Board of Directors, Norman Zigrossi, was subsequently hired by TVA as its Chief Administrative Officer (CAO). TVA IG reports show that as CAO last year he earned salary and "performance incentives" of over \$600,000. The second IG, William Hinshaw, had a completely different experience. GAO learned that Chairman Crowell and the TVA Board hired an outside firm to audit the OIG. Hinshaw and one Board member believed the purpose of the audit was to help remove the IG, who did not get along as well with the Board as his predecessor. Mr. Hinshaw later resigned. Those were the precedents for Mr. Prosser – one IG which the Board liked received a lucrative position in management and one that the Board had problems with was forced out.

In his seven-day letter, Mr. Prosser stated that the Chairman became angry with him as a result of certain reports and investigations. As with Mr. Hinshaw, Chairman Crowell contracted for an outside audit of the IG office (the audit, however, was postponed indefinitely after the IG raised questions about whether it violated the IG Act). In addition, after the acquittal of a former TVA official that the OIG had referred to the U.S. Attorney, the Chairman harshly criticized the IG and, later that same day, the CAO ordered a review of all the IG's credit card records. Mr. Prosser claimed he was told by the TVA CAO that Chairman Crowell would spend the rest of his term "sc—ing" him. Feeling that his independence was threatened, Mr. Prosser wrote to Congress.

Seven-day letters are required to be forwarded through the agency head for review and comment before being sent to Congress. Chairman Crowell attached a number of allegations to the letter regarding the IG's use of his TVA credit card. The Chairman also forwarded the allegations to the Executive Council on Integrity and Efficiency (ECIE) along with anonymous complaints that had already been reviewed and addressed. Subsequent to the seven-day letter, and throughout the GAO investigation, a number of additional allegations about Mr. Prosser were provided to the press although the TVA Board denied disseminating them.<sup>2</sup>

GAO's review of the allegations and all of Mr. Prosser's credit card records revealed that he in fact did not violate TVA policy. On the other hand, the review found that "The Chairman's actions against the IG included the release of unsubstantiated allegations to the media and the referral of unsubstantiated allegations to the ECIE. These actions could be viewed as an attempt to undermine the IG's independence."

<sup>2</sup>Jaques Billeaud, "Documents reveal new Prosser allegations; Fired TVA official Bailey also in question," Knoxville News-Sentinel, August 17, 1999, p. A1.

Another troubling aspect to this matter involved the appointment of an interim IG. As noted, Chairman Crowell sent a copy of his allegations to the ECIE which were forwarded to the Integrity Committee of the President's Counsel on Integrity and Efficiency (PCIE), which subsequently sent them to the Department of Justice and then the FBI for routine review. He then used this referral to the FBI as a basis for placing Mr. Prosser on administrative leave and appointing someone from TVA management as an interim IG. During that period, the interim IG had access to confidential audits and files, as well as investigations into top TVA management. Mr. Thompson remained as the interim IG until Mr. Prosser was reinstated despite repeated calls by myself and others to put an independent official in the position.

As a follow-up to the investigation involving the cross allegations between the TVA IG and Chairman, the Committee also asked GAO to investigate a trust established by the TVA Board and once again released a report.<sup>3</sup> The trust had been the subject of a TVA IG audit as well as an investigation by the U.S. Attorney for the Eastern District of Tennessee. As part of its investigation, GAO discovered that the U.S. Attorney ceased cooperating with the TVA IG, fearing a lack of independence due to the Board's authority to terminate the IG. As a result, GAO noted that TVA lacked sufficient oversight: "In addition, TVA's IG can be fired by the Board, thus limiting the IG's independence."

I believe that one major cause of the problems experienced by Mr. Prosser was the fact that the Chairman had the ultimate authority to hire and fire him. The experience of the first two IGs, one having been promoted to management and one having been forced out, shows the ultimate problem – an IG cannot be a watchdog and a house pet at the same time. The ability of the Chairman to hire firms and hold potential audits over the IG's head reveals just how strong the agency head's appointment authority is. And the ability to appoint an official from management as an interim IG completely breaks down the wall of independence between management and the OIG.

A survey conducted in 1998 revealed that 27% of DFE IGs believe they do not have sufficient independence to accomplish their mission (compared to 15% of presidentially-appointed IGs).<sup>4</sup> The good news is that most agency heads are conscientious public servants who, once they understand the role of the IG, are going to respect the office. And I have been told that most DFE IGs have a good working relationship with their agency heads. However, there are always going to be those that will attempt to harass or intimidate their IG.

<sup>3</sup>GAO Report, *Problems With Irrevocable Trust Raise Need For Additional Oversight*, 106<sup>th</sup> Cong. (Feb. 29, 2000).

<sup>4</sup>GAO Report, *Inspectors General: Information On Operational And Staffing Issues*, 106<sup>th</sup> Cong. (Jan. 4, 1999).



One possible solution to the special problem of independence faced by the DFE IG was put forward by Rep. John Duncan. Rep. Duncan introduced a bill last Congress which would have made all DFE IGs presidentially-appointed. Sen. Susan Collins initially proposed in her IG reform bill that some of the DFE IG offices consolidate and also proposed that IGs be given nine-year terms. However, both provisions were eventually removed from her bill before it was reported out of the Governmental Affairs Committee.

I applaud both of these members for trying to address a difficult issue. In the case of TVA, given that it was the second largest DFE IG office and larger than some presidentially-appointed OIGs, I introduced a bill, which is now law, making the TVA IG a presidential appointment. However, presidential appointment may not be the right answer for all DFE IGs. Other options that have been discussed which could enhance the independence of the IGs include: codifying the PCIE and ECIE; allowing IGs to submit budget requests directly to OMB and Congress rather than going through the agency review process; and, ensuring the removal of an IG only for cause.

While Congress sorts out the various proposals for protecting the independence of DFE IGs, one thing remains clear. Ultimately, the IGs report both to Congress and to their agency head. Therefore, when there is a problem between an agency head and an IG, no matter the size of the office, it is the responsibility of Congress to investigate and protect the independence of the IG.

In addition to Congress' responsibility, I believe the IG community has a responsibility as well. It is important that the community educate officials in both the executive and legislative branches on their role and responsibility. We currently have a new Administration forming, and many positions will be filled with individuals from the private sector who may have little or no knowledge of the mission with which Congress has charged the Inspectors General. By ensuring that each new agency head has a good understanding of the role of its IG, perhaps some misunderstandings and problems can be averted. And by educating members of Congress on the important responsibilities of the IGs, as well as the importance of independence, the IG community can ensure that Congress will continue to serve as a backstop should future problems arise.



sible, qualified instructors who are members of the IG community. The purpose of this effort is twofold: to provide more IG specificity to the courses and to place more IG investiga-

tors before the students as positive role models, thereby strengthening the pride that the students have in their community.

The identification of critical training needs will continue to be made based on a needs assessment conducted within the IG community. The Academy is currently working on a training needs assessment for programs such as Computer Intrusion, Misuse of Government Computers, Computers as an Investigative Tool, and other programs related to computer-based investigations and investigative writing. These programs will enhance the nine advanced or specialized programs currently offered. These programs are:

- Hotline Operators Training Program
- Advanced Investigative Techniques Training Program
- Undercover Operations Training Program
- Public Corruption and Employee Integrity Investigations Training Program
- Workers Compensation Fraud Training Program
- Arrest and Search Warrant Execution Training Program
- Technical Investigative Equipment Training Program
- Transitional Training Program
- Procurement, Contract, and Grant Fraud Training Program

As with the IGITP, the Academy will continue to develop the most relevant IG-specific courses utilizing the most up-to-date methods and information available. The staff will meet with or contact executives, supervisors, and training officers throughout the IG community to identify subject matter experts and to use these experts as resources in the training program development and execution. Without the various community members continuing to commit the necessary resources, the Academy will not be able to maintain its current level of success.

As of this article's printing, the Academy will have offered at least one repetition of each of these advanced programs. In many cases multiple iterations of these programs have been offered and the feedback has been very positive. The Academy looks forward to further developing relevant training courses and to meeting the needs of the OIG community.

Regardless of the success of all of the programs currently being offered or to be offered at the Academy, the environment here is dynamic and never static. It is a point of pride at the Academy that there has never been a repeat of one program that has been just like another. Quality training is an ever-evolving process of change and evaluation. Subsequent to the completion of every program, the staff will continue to conduct an extensive review of the program strengths and weaknesses identified by critique and evaluation. Appropriate changes are and will continue to be incorporated into the next offering and then reevaluated. This constant process of evaluation and reassessment ensures that the programs of instruction will remain relevant and without unnecessary redundancies.



Another important Academy responsibility is that of Federal Law Enforcement Training Center (FLETC) Agency Representative. Effective October 1, 2000, the Academy assumed the responsibility for scheduling and allocating all IG training slots for both FLETC and Academy classes. This is an enormous and very complex undertaking. The Academy has developed policies and procedures in order to meet, as equitably as possible, the training needs of the community. The Academy continues to refine its policies and procedures in order to meet this obligation. One other important aspect of a consolidated Academy is the ability to leverage the voices of 57 OIGs with 2,900 criminal investigators in the FLETC in order to ensure that the training needs of the entire community continue to be met.

Between January 2000 and the writing of this article, more than 400 students have already completed training in programs offered by the IG Academy. More than 95% of these students have rated the programs in the good to excellent range (the majority of this percentage rated the classes as excellent). Examples of specific student comments are:

- "Overall, this has been the most positive and beneficial training I have received as a government

employee. Without question, I leave this class much better prepared to perform my duties.”

- “I appreciate the atmosphere the training staff created and the professionalism they exhibited throughout every course of instruction.”
- “The entire training was very helpful to me, although I have 15 years of experience as a state investigator. This training has allowed me to go back to my office and perform in a more effective and efficient manner.”
- “The entire staff has obviously gone to extraordinary measures to create a fun yet challenging course—one of the most challenging and informative courses I have ever attended.”
- “Class content was outstanding, instructors were knowledgeable and helpful, class subjects were IG-specific, and practical exercises were realistic.”

- “This was probably the best training I have ever been to.”

None of this success could have been achieved without the dedication, commitment, and pride exhibited by each of the Academy staff, the visiting instructors, and the many others within the community who participated in developing and planning these courses. Credit must also be given to each Inspector General for commitment to training excellence and for unwavering support of this Academy.

Each member of the Academy staff is committed to instilling, within every student, a sense of pride in being a special agent or other employee of the IG community. There are many ingredients that make up integrity, but without pride, confidence, and ability, the assumption of that trait is never possible. 🏠

The OIG community's problem is further exacerbated by a heavy reliance of Offices of the US Attorney upon technical experts. Impartial scientific expert analyses and opinions are inherently more objective and often carry more weight with judges and juries than eyewitness testimony. As a consequence, an increasing number of attorneys refuse to accept cases for prosecution unless crucial evidence has been subjected to a forensic analysis. Without access to a responsive lab provider, the OIG community faces an increasing decline of its cases by Offices of the US Attorney.

## Forensic Services and Support

In the aforementioned survey, the PCIE and ECIE members were asked to define capabilities and anticipated workload for the IG Forensic Lab. This data will help structure the operation to be technically responsive, customer focused and benefit a majority of the IG community's investigations. Survey responses overwhelmingly supported the congressional intent of Senate 1707 for consistent quality and timely forensic lab services. Of the thousands of investigations conducted by respondent OIG agencies, most included physical evidence that would directly benefit from forensic lab analyses.

With the enactment of Senate 1707 and adequate appropriations, the IG Forensic Lab will be positioned to assume its role as the IG community's principal lab source, respond to agency-specific needs and help resolve complex investigations. Some of the immediate benefits the OIG can expect include:

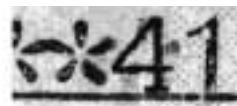
- Provide a dedicated staff of professional experts to address the OIG forensic lab needs timely.
- Conduct independent, impartial examinations of physical evidence and, as warranted by results, experts could refocus resources towards more fruitful investigative arenas.
- Provide expert advice and assistance to maximize the potential value of physical evidence.
- Assist with processing crime scenes, documenting, collecting and packaging physical evidence.
- Advise officers of the US Attorney's Office in the presentation of expert testimony.
- Provide expert testimony before judges, juries and other adjudicative bodies in the form of opinion evidence.
- Conduct relevant research and development to adapt new technology or modify methods for specific OIG case problems.

Although the specialties projected for the IG Forensic Lab include traditional forensic capabilities, it is expected that the lab will expand its expertise base dependent upon advances in the science, dynamic changes in IG community

needs and the focus of investigative efforts. Assuming adequate appropriations for this initiative, the IG Forensic Lab will include a staff of forensic experts and specialists who can bring necessary credentials and experience to OIG investigations. It is anticipated that the IG Forensic Lab will provide expertise and technical support in:

### Questioned Documents

The specialty of questioned documents covers diverse investigative problems including identifying the author of questioned writing, determining the source of an item or establishing its authenticity. Document analyses are not limited to sheets of paper but may include items such as a message scratched into a wall, graffiti, torn stamps, burned or shredded notes. Although the majority of document examiners' work is devoted to identifying the author of handwriting, they also evaluate evidence such as anonymous threats, counterfeit instruments, erased and obliterated entries, torn and/or burned documents, typewriter ribbon text, printed material (typewriters, copiers, laser printers), and altered or substituted documents.

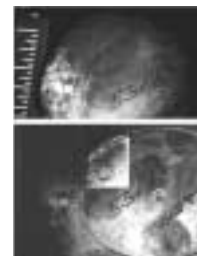


*Cashier's check was altered and the funds diverted into the suspect's bank account. The check originally read "\*\*\*\*1,396\*\*\*\*". When received by the lab it read "\*\*\*\*41,396\*\*\*\*". The asterisk preceding the "1" was erased and a "4" inserted. Using image processing technology and edge detection filters, remnants of the original asterisk were found.*

### Latent Fingerprints

Latent specialists process evidence using physical methods or chemical techniques to visualize patent or latent (invisible) prints. Developed prints are not limited to the tips of fingers but could be left by a writer's palm prints. Therefore, it is important that investigators submit major case prints so specialists can make a definitive comparison and/or elimination of suspects and victims. In instances where a suspect has not been developed, latent specialists can evaluate unidentified latent prints and determine their suitability for entry and search in national automated fingerprint identification systems (AFIS).

*Latent prints, developed on stolen laptop computer components, were compared and identified with the primary suspect.*



### Document Chemistry

Forensic chemists examine documents for evidence of alteration, insertion, authenticity or substitution, by testing documentary materials (writing inks, papers, printer ribbon inks). They compare the chemical signature of questioned materials with collected known standards or formal library samples. Indications that materials differ chemically can be extremely useful in supporting a claim of fraud.

### Digital Image Processing

Digital imaging specialists utilize sophisticated computers and specialized software to improve the image quality of negatives, photographs and damaged evidence items. Digital imaging has become an integral tool in today's forensic lab in enhancing details of latent prints found on interfering backgrounds or visualizing the remnants of an erased entry. As a relatively new science, digital imaging continues to find a growing workload in the forensic lab.

*A latent fingerprint, developed on a stolen remittance check, was difficult to compare due to interference from security printing. Digital image enhancement and Fourier transform software removed the repeating pattern and allowed the specialist to identify the latent fingerprint with a suspect.*

Latent: Interfering Background



Latent: After FFT Processing



### Audio and Video Engineering

Audio and videotaping are common techniques used during the course of an investigation to record interviews, undercover operations or surveillance. Their quality, unfortunately, is often poor and may be of little evidentiary value without some form of enhancement. Engineering specialists can often improve image or voice quality using specialized software to remove background noises, correct lens errors, and lighting problems.

*A thermal print made from security videotape depicted a defendant cashing stolen travelers checks. Pertinent date and time information on the print could not be read and the original videotape had been destroyed. During trial, the AUSA requested a lab analysis of the thermal print to decipher the crucial date and time.*

EXAMPLE 2

Thermal print still from videotape



After processing with DCP, date and time can be deciphered.



### Transitioning the IG Community to an Integrated Partnership

Since its emergence in the corner of the police department, the forensic science lab continues to evolve in its contribution to law enforcement and the judicial system. Its role in the past 25 years is best described as a functional partner. Attorneys and the courts increasingly relied on the science to resolve legal problems through an independent evaluation of evidence. Although experts incorporated new tools that better positioned them to characterize microscopically small samples and individualize them with greater certainty, the functional partnership occurred within the confines of the lab environment, divorced from criminal investigators and the process.

Today forensic labs strive to be integrated partners. Progressive federal agencies recognize the vital role forensic experts play in the investigative process and include them as essential partners on the investigative team. With continuous changes in modern technology, technical experts can offer the experience necessary to readily recognize complex evidence and interpret its significance within the investigative context. Bringing a dedicated IG Forensic Lab and technical experts into the OIG investigative process will transition the IG community into a professional and integrated partnership.

Through its partnership with the IG Criminal Investigator Academy, the IG Forensic Lab can promote a forensic approach to investigations, i.e., evidence-based thinking, and educate special agents how to recognize evidence and its potential for answering crucial investigative problems. By reinforcing forensic science's value through basic and advanced courses the IG Forensic Lab can improve both the quality of evidence submitted for evaluation and its subsequent analysis.

As a valued member of the investigative team, the IG Forensic Lab can be an active technical partner, reviewing new OIG initiatives and advising agency participants as to relevant forensic aspects of the undertaking. A dedicated lab staff can incorporate new forensic specialties to broaden its support of the IG community's efforts and bring state-of-the-art technology into its investigative arsenal. Cases will benefit from the extensive scientific background of its newest team members, an open dialogue and strong technical relationships.

An independent IG Forensic Lab will leverage the voice of 57 agencies and 2,900 criminal investigators by providing access to a dedicated lab provider. Consistent, high quality support, tailored to OIG investigations, will significantly improve delivery of services to large and small IG offices alike. Scientists will incorporate emerging resources to benefit the entire IG community and ensure services reflect the most current trends in criminal and civil law and lab techniques.

An IG Forensic Lab will promote greater efficiency of OIG cases by redirecting valuable resources early in investi-

gations. The use of lab services will promote the IG community as a progressive law enforcement partner. Scientific corroboration of allegations can significantly improve acceptance of OIG cases by Offices of the US Attorney. Analysis of physical evidence by experts using scientifically proven methods and the latest technology promotes the acceptance of expert opinions in the courtroom.

The IG Forensic Lab will elevate the OIG community to a unique position by having the first organizationally independent lab operation in the country. It will serve

as a community scientific advisor bringing consistency and conformity to all forensic aspects of OIG investigations. As a sole provider of services, the IG Forensic Lab will adhere to stringent standards and bring consistent, quality work products to investigations and the courtroom. An independent IG Forensic Lab can incorporate IG-specific needs and be a scientific source of pride for its investigative partners. OIG investigations will reach a new level of excellence by assimilating the collective experience and background of unique team members into its cases. 🏠

The Journal of

# Public Inquiry

A Publication of the Inspectors General of the United States

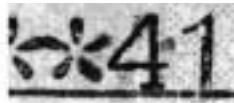
Spring/Summer 2001

## TABLE OF CONTENTS

Science Non-Fiction 1

*The Forensic Lab*

**Jo Ann L. Becker**



pg. 1

Integrity U 5

**G. Michael Baird**

All the President's Men and Women 9

**Sen. Fred Thompson**

Will the Circle be Unbroken? 13

*Meeting the Challenges of the Expanding  
Role of the Inspector General Community in  
Federal Computer Security*

**Howard W. Cox**

Net Escape 17

*Policy for Personal Use of Internet Access by Federal Workers*

**James J. Flyzik**

Online on Our Time 21

*OIG Reviews Employee Internet Use*

**Jack Talbert, Marshall Gray and Sharon Tushin**



pg. 17

The World in Your Lap 25

**Dan Devlin**

A Map of PARIS, DC! 31

**Joseph I. Hungate**



pg. 25

**Inspector General Concept 35**

**When the IGs were Pups 36**

*Reflections on the Early Years of the  
Inspector General Program*

**Howard M. Messner and  
Seymour D. Greenstone**

**Talking Heads 39**

*Inspectors General and Their Relationships  
with Agency Heads*

**Dwight Ink and Herb Jasper**

**A Non-Random Act of Kindness 45**

*Congress and the Inspectors General*

**Kenneth M. Mead**



pg. 35

**Why Knowledge Management? 53**

**Beth Serepca**



pg. 45