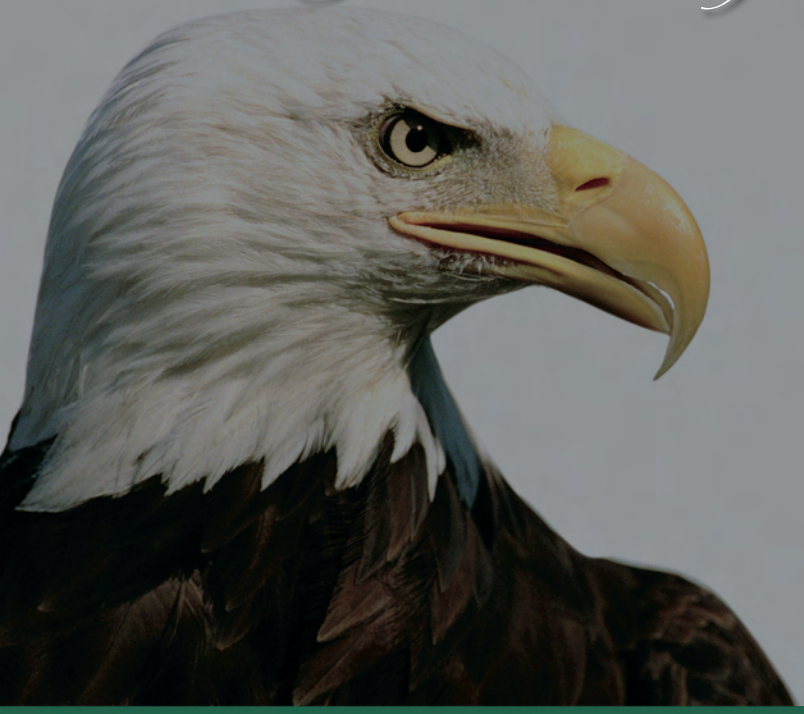
A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

# The Journal of Public Inquiry



SPRING/SUMMER

2007

PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY

EXECUTIVE COUNCIL ON INTEGRITY AND EFFICIENCY

## Staff

Editor-in-Chief
Claude M. Kicklighter, Inspector General, Department of Defense

Publisher
John R. Crane, Assistant Inspector General, Office of Communications and Congressional Liaison, Department of Defense Office of the Inspector General

Publication Manager
Jennifer M. Plozai, Writer, Office of Communications and Congressional Liaison, Department of Defense Office of the Inspector General

Editorial Services
Caitlin N. Laverdiere, Intern, Office of Communications and Congressional Liaison, Department of Defense Office of the Inspector General

Printing
Department of Defense Office of the Inspector General

# FOREWORD

Welcome to the Spring/Summer 2007 issue of the *Journal of Public Inquiry*. The articles contained in this issue of the *Journal* cover a variety of important issues related to the mission of the Inspectors General (IG). It is our hope that the *Journal* serves as a source of information that allows the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) to share knowledge regarding IG issues that transcend individual government agencies. We are working together to improve how the government serves the American people.

The *Journal* is a publication of the PCIE and ECIE, which together represent of 64 statutory Inspectors General to oversee the federal government. Our work is continuing to grow and expand. We need to share our insights and best practices with one another in the oversight community. If we see a trend developing – whether good or bad – we need to share that information. Communication within the oversight community is essential to avoid duplication and gaps in efforts; leverage each other's work; and support each other's efforts and form mutually beneficial partnerships.

We are pleased to present seven articles, one speech, a hearing statement, and two Georgetown University capstone papers. The articles encompass themes including the elements of a virtual front office, management controls, corporate compliance programs, heightening standards of accountability, the government's pension loophole, the use of digital forensics in criminal investigations, and the Federal Audit Executive Council. The selected speech in this issue is written by Department of Defense Principal Deputy Inspector General Thomas F. Gimble and discusses issues relating to information technology and the establishment of the PCIE Information Technology Committee.

We have also included a statement presented at the June 20, 2007 hearing on Inspectors General: Independence and Integrity before the Subcommittee on Government Management, Organization, and Procurement of the House Committee on Oversight and Government Reform. The testimony is by Deputy Director for Management, Office of Management and Budget, Clay Johnson III.

Finally, our two capstones were written by IG graduates of the Georgetown University Masters in Public Policy program and cover contractor cyber security reporting and information sharing within the intelligence community.

A special thanks to all the authors who contributed their expertise to this insightful issue of the *Journal of Public Inquiry*. Your efforts have not only enabled the IG community to share valuable ideas and information, but have also made our work more transparent to the American people we ultimately serve.

Claude M. Kicklighter
Inspector General

# Table of Contents


## Articles

| | Pages |
|---|---|
| ***A Virtual Front Office*** by Carrie L. Fox | 1-4 |
| ***Corporate Compliance Programs: More Than Window Dressing*** by Ginna Ingram | 5-10 |
| ***Management Controls Have Finally Gone Away!*** by Gregory Sinclitico | 11-16 |
| ***Stopping the Buck: Establishing a Heightened Standard of Accountability*** by Earl E. Devaney and Chris W. Martinez | 17-22 |
| ***A Hard Day's Work: Taking Another Look at the Government Pension Offset Loophole*** by James J. Klein and Tracy B. Lynge | 23-28 |
| ***Digital Forensics: The Value of Partnership in Support of Criminal Investigations*** by Craig M. Goscha and Eileen M. Sanchez Rehrig | 29-36 |
| ***The Federal Audit Executive Council: A Supgroup of the PCIE Audit Committee*** by FAEC Chair and Committee Chairs | 37-42 |

## Speeches

| | |
|---|---|
| ***Information Technology Issues and the Establishment of the PCIE IT Committee*** by Thomas F. Gimble | 43-48 |

## Hearing Testimony

| | |
|---|---|
| ***Hearing: Inspectors General: Independence and Integrity*** by Clay Johnson III | 49-52 |
| ***Hearing: Inspectors General: Independence and Integrity*** by Jeffrey C. Steinhoff | 53-60 |

## Capstone Papers

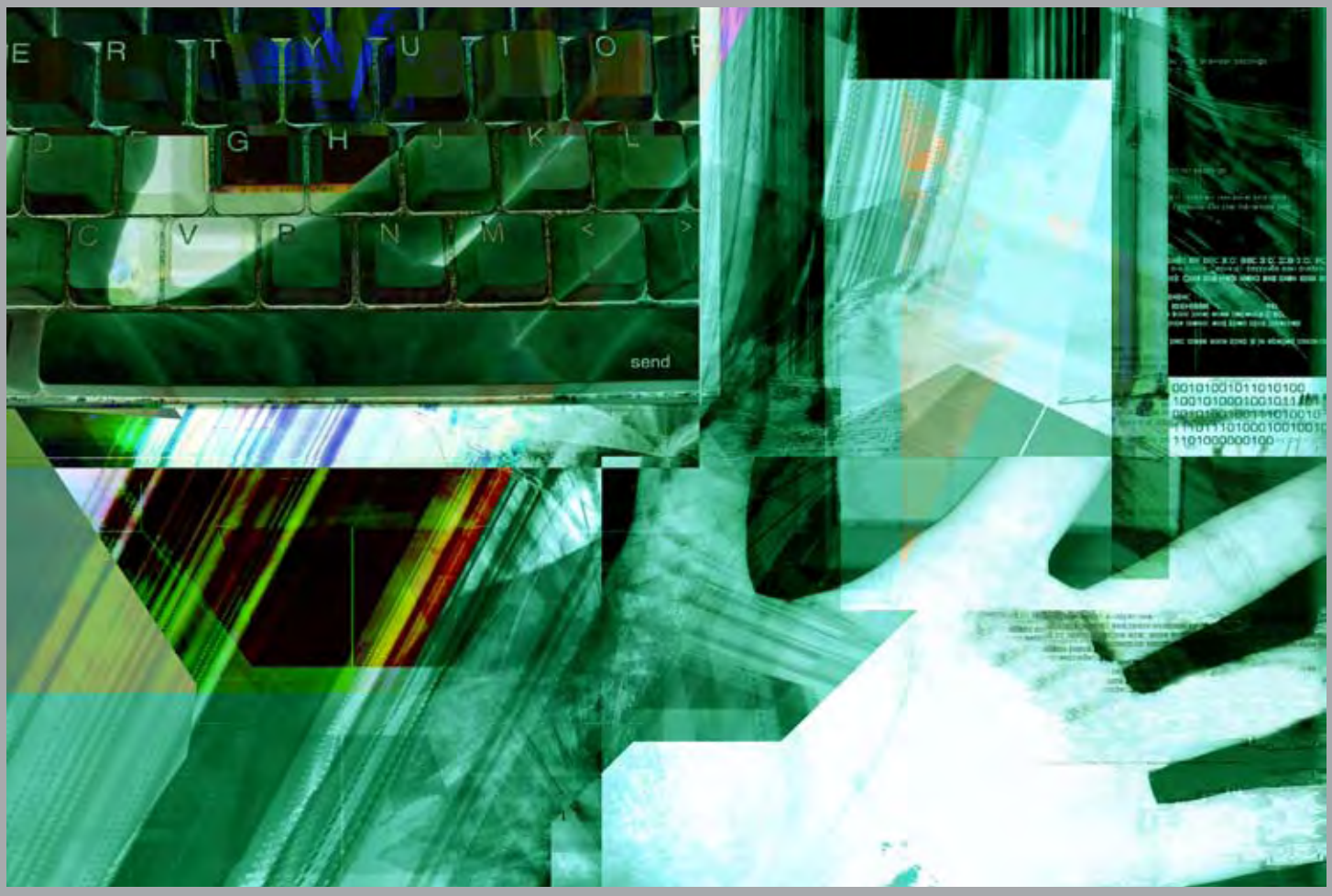
| | |
|---|---|
| ***Extending the Cyber Barricade – Closing the Gap in Defense Contractor Cyber Security Incident Reporting*** by Paul K. Sternal | 61-68 |
| ***Information Sharing Throughout the Intelligence Community*** by Scott A. Boehm | 69-74 |


⚙ Denotes the end of an article.

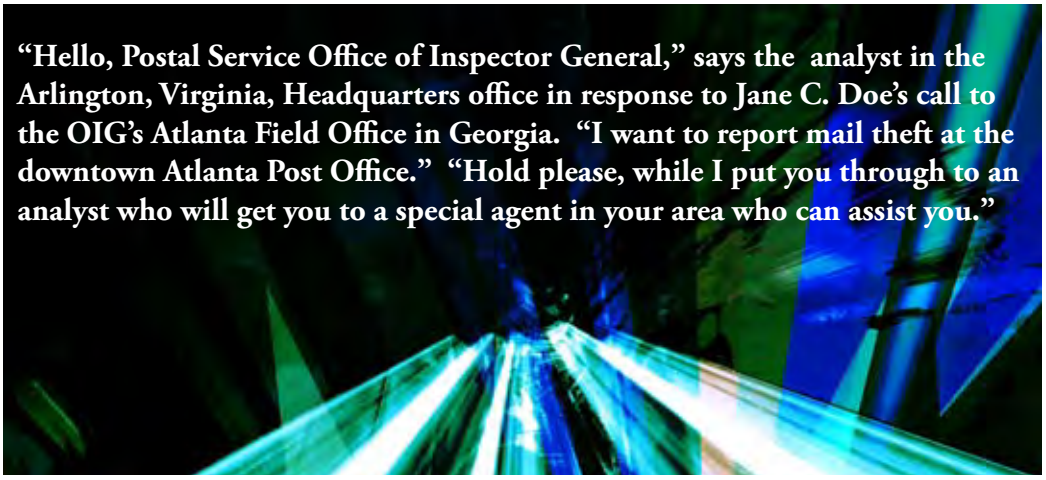
# A Virtual Front Office

by Carrie L. Fox

1




U.S. Postal Service
Office of the Inspector General



**"Hello, Postal Service Office of Inspector General," says the analyst in the Arlington, Virginia, Headquarters office in response to Jane C. Doe's call to the OIG's Atlanta Field Office in Georgia. "I want to report mail theft at the downtown Atlanta Post Office." "Hold please, while I put you through to an analyst who will get you to a special agent in your area who can assist you."**

This speedy, efficient handling of U.S. Postal Service OIG calls and headquarters visitors is an innovative concept whose genesis began with OIG management's decision to provide immediate assistance to individuals trying to report fraud, waste, and misconduct within the Postal Service. To further gain trust and respect from stakeholders, management wanted to give customers and stakeholders in other time zones live access to OIG offices through normal business hours.

The Postal Service has more than 800,000 full time and contract employees; 37,000 retail locations and facilities; annual revenues of $73 billion; and manages $42.4 billion in contracts. The size and scope of its mission alone provides many potential opportunities for fraud and corruption.

To investigate and audit the second largest civilian agency in the nation, effective management of resources is critical. The transition of certain U.S. Postal Inspection Service functions to the OIG meant more personnel, more geographic and topical areas to cover, and an ever-expanding need for timely responsiveness to those reporting violations or seeking assistance from the OIG.

OIG management recognized that the quicker the OIG focused its resources on allegations, the sooner it could achieve efficiencies and savings for the Postal Service. The OIG also wanted Postal Service management, employees, and the public to have direct and immediate channels to report fraud, waste, and mismanagement within the Postal Service at one location. OIG management specifically wanted to put callers with legitimate allegations in direct contact with special agents to lead to real time resolution and pursuit of issues affecting Postal Service operations. From this thought process, the concept of the "Virtual Front Office" was born.

## What is a Virtual Front Office?

The Virtual Front Office (VFO) is the central point of contact for the OIG. It is located at the Arlington headquarters. Staff assigned to the VFO, primarily Hotline analysts, answer calls placed to field offices around the country from 7:30 a.m., to 8 p.m., ET.

Through modern technology, telephone calls to any field office are seamlessly routed to the VFO in Arlington. Callers are then connected to the desired party or office; put in direct contact with a special agent in their local area, if it is an investigative matter; transferred to the OIG Hotline, if they wish to lodge a complaint (for non-investigatory matters); or transferred or referred to the Postal Service, as appropriate. Recognizing Postal Service managers have busy schedules, a special 800 number for managers exclusive use was established to help them reach a special agent or a Hotline analyst immediately.

## Background

Prior to the VFO, the OIG's headquarters reception received visitors, vendors, then fielded calls on its main numbers. Each field office had its own number and personnel assigned, or a voice recording, to handle calls to their office. Unfortunately, this system frustrated some callers who were unable to speak to OIG analysts immediately. Occasionally, a telephone tag game would ensue before they could actually speak to someone. This sometimes resulted in missed opportunities from individuals who wanted to report improprieties to the OIG, but who preferred to remain anonymous.

The OIG's former Hotline process required callers to file their complaints with an analyst who wrote up the complaint based on responses to the basic "who, what, where, why, when, and how" questions. The write-up was then reviewed and approved by a manager who ensured the write-up contained all required information and determined if an adequate referral was being made. The approved write-up was next referred to the appropriate investigative office electronically assigned to an agent

through the OIG's Performance and Results Information System (PARIS). Too many layers were slowing down the OIG's response process.

## What went into planning the VFO?

Once the idea was fully conceptualized, an inter-disciplinary team (staff from the Office of the Chief Information Officer (CIO), the Office of Investigations, Administrative Services, Strategic Planning, and Hotline) brainstormed, strategized, and designed every element of the VFO over a two month period. Every VFO aspect was carefully conceived and assigned to appropriate parties for development. Since the VFO would be the central point of contact for phone calls to the OIG, the reception and receiving Visitor Control Center (VCC) became an integral part of the VFO, as well. This necessitated a physical move of the VCC — to co-locate the Hotline manager and the Hotline and VCC staff (now joined together and called the VFO staff). The VFO implementation team developed a project plan and named a project manager to closely monitor the plan. The project manager ensured the many milestones were met to allow for implementation of the VFO on the scheduled date. An integral part of the project plan was a carefully thought out communication plan to trumpet the new initiative to both Postal Service and OIG audiences. The dedication and commitment of the entire VFO implementation team resulted in a smooth transition and on-time delivery of the project in April 2006.

## Implementation of the VFO

Beginning with an initial test period, the VFO was launched on April 3, 2006. Implementation required a crash course and new guidance for Hotline analysts and special agents who would now be getting the direct calls that had previously been written up by the analysts, reviewed and approved by management, and transmitted to appropriate field offices by ZIP Code through the OIG's PARIS. The CIO automated a system that allows the Office of Investigations to easily populate the names and contact information of rotating duty agents for each of the field offices for easy access by the analysts. Of course, scheduling for the expanded 12.5 hours of VFO coverage required careful coordination for staffing and on-site management to ensure availability during all hours of operation. The staff adjusted work schedules to allow for the implementation of shift assignments. Every detail was worked out down to a parking space for the person on night duty. After three months of tweaking the system, the VFO became fully operational July 3, 2006.

## What are the benefits of the VFO?

The VFO gives Postal Service managers immediate access to an OIG special agent in their local area. The special agent can obtain critical relevant information directly from the manager, which assists the special agent in assessing the allegations and determining necessary action. Therefore, nothing is lost in translation and immediate rapport is established. The same is true for contacts with other postal employees and the public. Analysts perform a brief triage to only refer appropriate calls to the special agents, since they are usually busy working cases and should only receive legitimate investigative allegations. From an administrative perspective, staff previously assigned to answering telephones and other sedentary work in field offices was now free to provide more direct mission support efforts to special agents and auditors, in those offices, contributing to personal career growth and development for those employees. The VFO hours of operation ensure OIG availability for west coast calls until 5 p.m., ET, daily (excluding weekends and holidays).

## Are there any disadvantages associated with the VFO?

Not really. The VFO has been well received by Postal Service management. The hours of operation were initially a point of contention with the Hotline staff until, together, they devised a schedule that worked for everyone. In addition, the CIO continues working with the Hotline manager to introduce new communications technology to make the job easier and more functional from off-site locations. Short of investing in a costly enterprise system, the CIO provided "hard client set-ups" that allows Hotline staff to utilize Smart Workplace, an OIG policy that permits employees to work from home and other approved locations. Remotely, they can answer the main number and their office land line, as well as work on their laptop computers. When a flood at OIG headquarters closed the Arlington office for two days, the VFO became a vital link to the office as it remained operational from one employee's home the first day. This success led to expanding the agency's investment in tools

for other analysts to utilize Smart Workplace flexibility. VFO employees are currently piloting a "hoteling" concept that decentralizes operations for essential employees and frees up space within the office. In addition, the OIG's culture helps managers establish performance standards that are easily monitored and measured to ensure operational efficiency.

## What are the next steps for the VFO?

As with any new process, the OIG continues to look for ways to improve. After a full year of operation, a new team will review what is in place and make recommendations based on lessons learned. The team is comprised of special agents and VFO staff, in consultation with CIO personnel. For example, Hotline callers currently speak briefly with the Hotline analyst, then a duty agent, and in many instances another agent in a sub-office (smaller offices assigned to larger field offices). The next phase's aim is to minimize duplication of efforts and to connect the Hotline caller to the appropriate agent as soon as possible. Therefore, the CIO's staff is working on adding sub-office contacts to the Hotline analyst's drop-down screen to allow immediate referral to duty agents in those offices. Another improvement will link the Investigative and Hotline databases to allow quick and easy follow-up from any location. Lastly, the VFO is piloting "hoteling", a shared cubicle/office concept that allows half the employees to work in the office while the other half work at home. This concept would allow an agency to free up office space, which could eventually lead to reductions in leased space and with success, VFO employees will be deemed essential employees capable of maintaining sustained communications with the OIG during periods when the office itself is closed for weather related conditions or other emergencies.

As the OIG celebrates one year of successful operation of its VFO, it continues to receive accolades from the Postal Service for this concept. The VFO allows the OIG to go into many Postal Service sites with small responsive units who rely on the VFO as their front office. Though happy with the VFO's success to date, the OIG strives for continuous process enhancements to further customer service thorough this medium. The team's efforts were recognized by the PCIE/ECIE last year thanks to an avant-garde innovation conceived by an IG with great vision.

## Carrie L. Fox, U.S. Postal Service OIG

### Director, Congressional Response/Central Intake

Carrie L. Fox joined the U.S. Postal Service Office of Inspector General in August 1997. As Director of Congressional Response/Central Intake since 2002, Ms. Fox is responsible for responses to congressional inquiries, the OIG's Virtual Front Office and Hotline, FOIA, records retention, agency manuals (policies), reviews of Postal Service workplace environment issues, and the executive secretariat function.

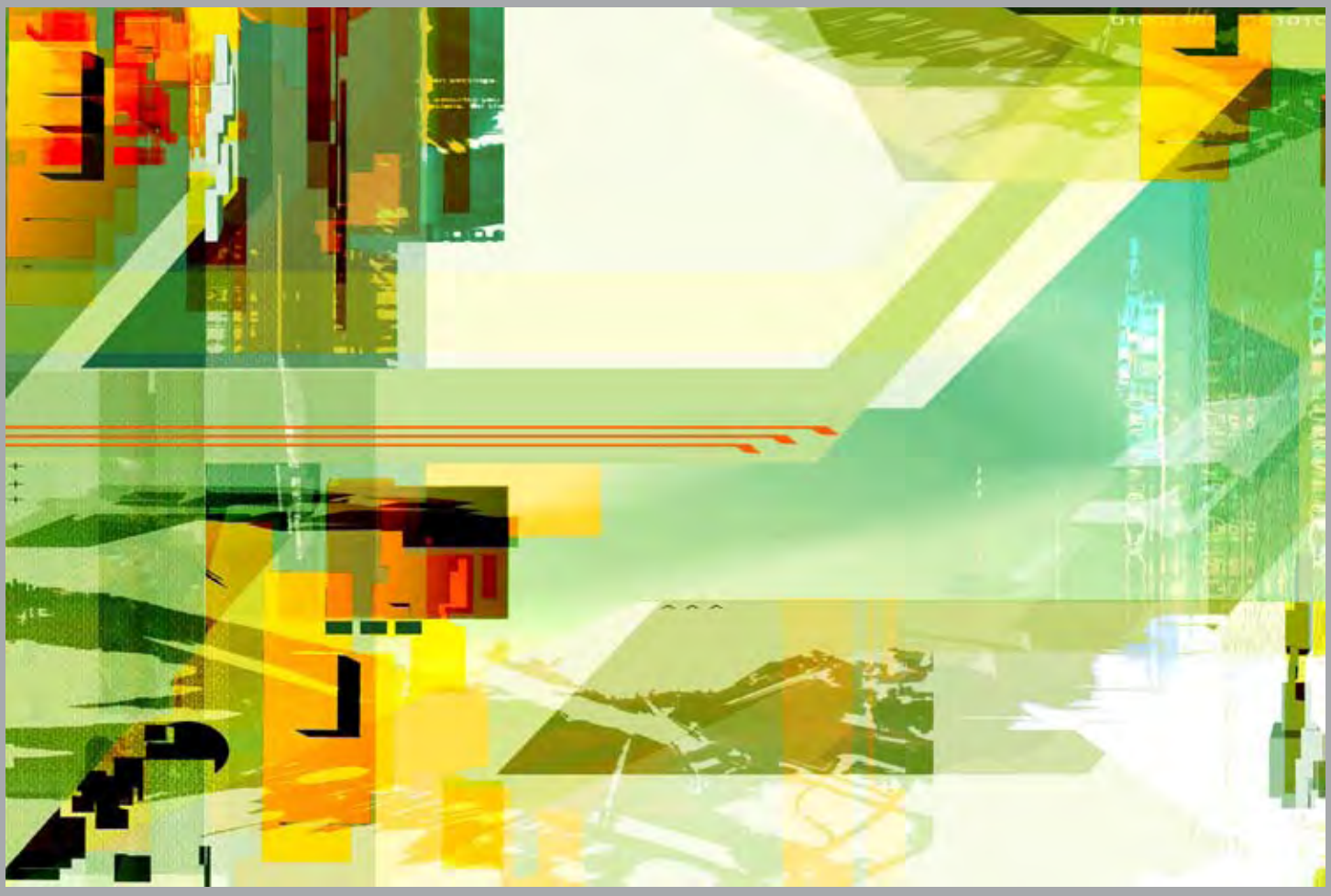
Ms. Fox formerly worked for the D.C. Department of Housing and Community Development as a Special Programs Coordinator; Equal Employment Opportunity and Affirmative Action for the Philadelphia Department of Housing as an Executive Assistant; and the city of Sumter, South Carolina Community as a Development Specialist.

Ms. Fox holds a B.S. in Business Administration, with an accounting minor, from Morris College in Sumter, where she graduated Magna Cum Laude.

# Corporate Compliance Programs

by Ginna Ingram

2



## More Than Window Dressing

[1]Compliance programs are established by corporate management to prevent and to detect misconduct and to ensure that corporate activities are conducted in accordance with all applicable criminal and civil laws, regulations, and rules.[2]

Department of Health and Human Services Office of the Inpsector General (HHS OIG) has long been a leader in this area. Their early and continuing efforts have established a trend toward a government-wide focus on compliance and ethics programs. In November 2005, HHS OIG published Draft Compliance Program Guidance for Recipients of PHS Awards for review and comment. This HHS OIG initiative was recently expanded, and now, in conjunction with the Office of Science and Technology Policy and the Research Business Models Subcommittee of the National Science and Technology Council, an effort is being undertaken to develop government-wide voluntary compliance guidelines for recipients of Federal research funding from all Federal agencies.

Compliance and ethics programs can be adopted voluntarily by an organization.[5] They demonstrate a commitment to an ethical, accountable environment and they guide business practices.

Such programs can also arise as part of the resolution of investigative issues, instituted as a term of settlement agreements or in lieu of administrative actions such as suspension and debarment.

They demonstrate a commitment to an ethical, accountable environment and they guide business practices.

Prosecutors should… attempt to determine whether a corporation's compliance program is merely a "paper program" or whether it was designed and implemented in an effective manner.[3]

## Introduction and Background

Compliance and ethics programs are an important part of a financially responsible enterprise. Whether adopted before instances of misconduct are identified or after, a well developed and implemented compliance and ethics program serves the interests of both the organization and the federal government. It is a win-win endeavor that directly supports the efforts of the inspectors general community to prevent and detect fraud, waste, and abuse.

This trend toward a government-wide focus on compliance and ethics programs was further demonstrated in a February 2007 Department of Defense, General Services Administration, and National Aeronautics and Space Administration proposal to amend the Federal Acquisition Regulation. The proposal prescribes policies and procedures for the establishment of a contractor code of ethics and business conduct and would require contactors to establish "an employee ethics and compliance training program…."[4]

The National Science Foundation (NSF) OIG, in conjunction with the Department of Justice and NSF, has used such programs to contribute to the resolution of investigations involving organizational misconduct. Through our outreach activities, we also encourage NSF's institutional grantees to proactively establish such programs to foster responsible and effective stewardship of federal funds.

In our compliance efforts we have been guided by the Federal Sentencing Guidelines (the Guidelines).[6] In 2003, compliance programs were given greater prominence through the adoption of a stand alone section in the Guidelines. Section 8B2.1 of the Guidelines, Effective Compliance and Ethics Programs, was born. Central to this stand alone section is the concept of effectiveness. Whether voluntarily initiated or imposed, the program must work.

1 Fara Damelin, Scott Moore, John Cieplak, Lee Stokes and James Evans of NSF OIG all made valuable contributions to this article.
2 Principles of Federal Prosecution of Business Organizations, United States Department of Justice, Office of the Deputy Attorney General Paul J. McNulty, at 12.
3 Id at 14. If this determination is favorable, then the prosecutor may decide not to charge the corporation for criminal misconduct undertaken by its employees and agents.
4 Federal Acquisition Regulation; FAR Case 2006-007, Contractor Code of Ethics and Business Conduct, 72 Fed. Reg. 7588, 7589 (proposed Feb. 16, 2007).
5 One need only look at the development of certification programs for compliance professionals, societies serving them, and the number of workshops training them to recognize the dramatic acceptance of compliance and ethics programs in American colleges and universities. We have witnessed the development of a "compliance industry."
6 United States Sentencing Commission, Guidelines Manual, (Nov. 2006).

In the Department of Justice's recent reissue of its Principles of Federal Prosecution of Business Organizations, the Deputy United States Attorney General stated:

While the Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees, the critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives.

The Department has no formal guidelines for corporate compliance programs. The fundamental questions any prosecutor should ask are: "Is the corporation's compliance program well designed?" and "Does the corporation's compliance program work?"

An effective compliance program reflects the direction given in Section 8B2.1. Broadly, Section 8B2.1 has three parts:

Subsection (a) defines an effective program as one where the organization exercises due diligence to prevent and detect criminal conduct and otherwise promotes a culture that encourages ethical conduct and compliance with the law;

Subsection (b) sets out seven elements that need to be present to exercise the required due diligence and to promote the desired organizational culture; and

Subsection (c) recognizes that in implementing the seven elements, it is vital that the organization periodically assess the risk of criminal conduct in its own organization and design, implement, and modify the program as appropriate.

The heart of Section 8B2.1 lies in the seven required elements. If a compliance program is to have a chance of being more than "window dressing," implementation of these elements is essential. These elements can and should be tailored to the specific nature of the organization, including its industry practices, regulatory requirements, size, and history of misconduct. In brief, the seven elements are:

(1) Establishing standards and procedures to prevent and detect criminal conduct;

(2) Ensuring managerial knowledge and specific responsibility for the content and operation of the compliance program;

(3) Avoiding employment of personnel who have engaged in illegal activities or other misconduct;

(4) Conducting periodic and effective training of personnel regarding the requirements of the compliance program;

(5) Monitoring and auditing the compliance program's effectiveness and establishing a whistleblower program;

(6) Promoting the program through incentives for success and disciplinary measures for failure;

(7) Taking timely action when wrongdoing is detected; responding appropriately to such conduct as necessary; modifying the compliance program as necessary.

While the elements described above may serve to mitigate penalties for organizations convicted of criminal offenses, they serve an equal or greater value as a recognized and authoritative "definition" of effective components of a compliance and ethics programs. For example, the Council on Government Relations (COGR) encourages that compliance and ethics programs be built around the Guidelines, which serve as the pillars of the guidance provided to the over 140 university members of the COGR.[7]

## Our Compliance Efforts

Crafting a compliance program that fully addresses these seven elements requires both flexibility and a resolute commitment to meeting the goal. Each organization we have dealt with has had different strengths and weaknesses, has been of a different size, or has engaged in conduct of varying types, scope, and duration. Also, the development of the compliance program, occurring as it has in the context of the negotiation of a settlement agreement with the Department of Justice, has involved identification of terms pertinent to the particular organization and specific investigative issues being addressed.

7 See CoGRs June 2005 "Managing Externally Funded Research Programs: A Guide to Effective Management.

Certain variables have created practical challenges to achieving the goal of a well designed and implemented compliance program. For example, one of the most critical aspects of an effective compliance program is ensuring that the institution maintains appropriate institutional oversight.

The Sentencing Guidelines require meaningful, high level managerial authority, identified individuals with specified duties, clear lines of authority, necessary expertise, and an appropriate commitment of financial and human resource support. But how does this play out in the context of a large university with its well-developed, complicated, and layered management structure? How does it work in a small, non-profit business, with limited resources and expertise?

for ensuring implementation of the compliance program. We viewed membership of the committee as key to meeting the needed high level involvement and responsibility. As a result, members included the institution's Inspector General, its Vice President for Administration and Financial Services, the Vice President of Sponsored Research, and the Provost.

In another matter involving a large university, the compliance program included a requirement that the Provost of the university chair quarterly meetings of the compliance committee. The Provost was instructed by the terms of the agreement to "immediately act upon compliance-related matters as they may arise…"

In situations involving smaller grantees, there may be an inclination to appoint a lower-level employee to serve as compliance officer. However, given the complexity of the tasks and the wide-ranging responsibility of the compliance officer, it is of particular importance for small grantees to appoint a high-level individual in order to ensure full implementation of the program.

Another area of critical importance is enforcement. We have required different mechanisms to ensure enforcement occurs. Generally, when the organization is large and the issues giving rise to the settlement are systemic weaknesses, we require an annual, statistically valid audit addressing compliance matters with regard to NSF awards. Further, we require submission of an annual written report identifying deficiencies covered by all audits and identification of steps taken to address such deficiencies.[9]

one of the most critical aspects of an effective compliance program is ensuring that the institution maintains appropriate institutional oversight.

In one matter involving a large institution, we assessed that there was a general lack of accountability within the corporate culture, a dearth of officials conversant with applicable rules and regulations, and a wide-spread breakdown of basic administrative systems. As a result, the compliance program included a new and detailed oversight structure within the institution, headed up by a compliance officer appointed by the institution's president and directly reporting to the president and to the institution's board of trustees. Supporting this compliance officer was a compliance committee responsible

In contrast, in a matter involving a small, non-profit grantee with a limited number of employees, the appointment of a compliance committee was not practicable. Thus, we relied on the General Counsel f the organization to perform all required ompliance duties.[8]

At the other end of the spectrum, if an audit specifically addressing NSF awards would be unduly burdensome given the institution's size, financial capability, or limited human resources, or because the issues giving rise to the settlement relate to individual acts of misconduct rather than systemic weaknesses, we attempt to adapt the requirements accordingly.

8 We recognize that a General Counsel serving as Compliance Officer is not the preferred structure. We are reminded of Senator Charles Grassley's observation in a September 5, 2003 press release, Grassley Investigates Tenet Healthcare's Use of Federal Tax Dollars, concerning such a structure – "It doesn't take a pig farmer from Iowa to smell the stench of conflict in that arrangement." Nevertheless, in some very small organizations, such an arrangement may necessary.

9 When audits are required to be performed, it may be advisable that the institution's internal and/or external auditor review the audit provisions to ensure that the organization understands the scope of the audit and when it should be performed. This will reduce any confusion over audit terminology and will avoid the issue of audits being performed outside of the institution's usual audit cycle.

In such situations, in lieu of a formal audit, we develop detailed provisions requiring submission of a certified annual report.

This report assesses the efficacy of the compliance program, sets out the steps performed to make the assessment, and whether written policies and procedures have been followed.

It identifies deficiencies and corrective actions, and provides the results of an annual review of the financial systems and internal controls.

In order to be effective in the monitoring and enforcement of the compliance program, information and reports must reach the appropriate individuals.

The settlement agreement sets out who must receive specific information and reports. Such information and reports are received and used collaboratively by NSF and NSF OIG to monitor and enforce compliance.

We accomplish this through a committee comprised of OIG and NSF staff set up to handle such compliance and enforcement matters.

The above examples illustrate that compliance and ethics programs do not lend themselves to a "one size fits all" model.

Rather, institutions should tailor such programs to the particular circumstances found at that institution.

Nevertheless, we believe the fundamental principles set out in the Sentencing Guidelines should serve as the basis for any such program.

## Conclusion

Establishing a compliance program benefits both an institution and the federal government. A compliance program will help the institution more effectively and efficiently manage federal funds. It will allow the institution to address problems promptly and to mitigate the institutional damage that may result from such problems.

Encouraging, and when appropriate, requiring an institution to establish a compliance program directly supports the efforts of the Inspector General community to prevent and detect fraud, waste, and abuse.

The frontline efforts of the Inspector General community in this area are not only timely and necessary, they fall squarely within our statutory responsibilities.

## Ginna Ingram, National Science Foundation OIG

Special Counsel
Investigations Division

Ginna Ingram is a Special Counsel in the Investigations division of the Office of Inspector General, National Science Foundation.

She provides legal advice to civil/criminal investigators and investigative scientists within the OIG. She also investigates civil/criminal and administrative matters and conducts special projects.

Ms. Ingram earned Bachelor of Arts degrees in History and French from the University of California, Berkeley and a J.D. degree from the University of California, Davis. She is a graduate of the Montgomery County Citizens Police Academy and she is a member of the California Bar Association.

# About the National Science Foundation OIG

## MISSION

We conduct independent and objective audits, investigations, and other reviews to support NSF in its mission by promoting the economy, efficiency, and effectiveness and safeguarding the integrity of NSF programs and operations.

## VISION

We will use our diverse and talented staff and cutting-edge technology to have a beneficial effect on NSF and the communities it supports.

We will help prevent problems, address existing issues in a timely and proportionate manner, and keep abreast of emerging challenges and opportunities.

NSF OIG contributors to this article include Lee Stokes, James Evans, Ginna Ingram, Scott Moore, Fara Damelin, and John Cieplak. (Pictured from left to right)

# Management Controls

by Gregory Sinclitico

3

# Have Finally Gone Away

The following article is reprinted with permission of the Armed Forces Comptroller Journal from Volume 52 Issue No. 2 Spring 2007; Copyright 2007 American Society of Military Comptrollers.

As a 26-year veteran of the professional audit community, it is with some disappointment that I must write that "Management Controls" have finally gone away. You may be thinking: "It's taken nearly 25 years, but finally someone has come to their senses and banished management controls."

But be forewarned, while management controls may have gone away, some very powerful and influential people have also gone away as a result of how they reacted, or failed to react, to management controls. For example:

Bernard "Bernie" Ebbers, ex-chief executive officer of Worldcom, has gone away. He was sentenced to 25 years as a result of the largest corporate fraud in United States history. Mr. Ebbers was convicted of embezzelment and fraud.

Jeffrey Skilling, ex-chief executive officer of Enron Corporation, has gone away. He was sentenced to more than 24 years. He, too, was convicted of fraud.

Dennis Kozlowski, ex-chief executive officer of Tyco International, has gone away. He was sentenced to at least 8 ½ years to perhaps as much as 25 years due to his involvement in the Tyco International grand larceny and other crimes.

In each of these examples, there were numerous instances in which internal controls were either were not in place or were circumvented to protect corporate assets.

So what's the deal with management controls going away? Well, it is true they have gone away -- but in name only. The term "management controls" has been replaced with "internal controls" (Office of Management and Budget Circular A -123, dated 21 December 2004, uses the term "internal controls" in place of "management controls.")

But this is a change in nomenclature only -- the policies and processes associated with accountability and control have not changed. All of us in federal service are stewards of the taxpayers' money, which is also our money, and internal controls help us exercise that stewardship.
So what are internal controls? We all can read, if we are so inclined, the official definition and policies and procedures, but I like to refer to internal controls as those people, processes, systems, and equipment we use to do our jobs.

Even in our everyday nonprofessional lives we have numerous internal controls that we routinely use. Things have to be approved, authorized, documented, safeguarded, overseen, etc., to ensure everything goes according to Hoyle.

For example, here are just a few controls that have influenced my job as a parent. I have two school-age children and on occasion, I ask if they have any homework, and if so, has it been completed? Surprisingly, I learned from my daughters that the school system rarely assigns any homework and when homework is assigned, it is so simple that it is completed before I arrive home.

Of course, I found out later that homework is assigned every day. Additionally, from talking to my children's teachers, I learned that the school system has in place an excellent internal control: a Web site that details each class' daily homework assignments with any corresponding due dates. It's wonderful! There are now two internal controls in place over my children's homework: first, the availability of the information, and second, my ability, as my daughters' "supervisor," to check on their homework assignment by requesting to see the completed work.

Another internal control in the school system's daily process is an online system that lets me see my daughters' running grades for each subject on a weekly basis. Some people may view these controls not so much as internal controls but rather Big Brother in action. I disagree.

These two processes are examples of every day internal controls, as are periodic reconciliation of your checkbook balances, childproof medicine bottles, paper copies of charge or debit transactions, house keys and car keys that can not be duplicated, and passports.

Internal controls are simply ways, checks and balances, to provide assurance that things go as intended: Procedures, regulations, and laws are

followed; transactions are properly documented; fraud, waste, and abuse are minimized; unapproved transactions are not processed, and desired outcomes are achieved. Controls are tools that assist you in doing a job as effectively and efficiently as you can -- and within legal and regulatory limits. They are the basic everyday things that help us live as orderly a life as reasonably possible.

These tools that help ensure success in all aspects of your professional and personal lives -- raising children, protecting your health, keeping your family safe, and doing your job.

We in the Naval Audit Service (NAS) are charged with the responsibility to review Department of the Navy (DON) internal controls and subsequently report on the effectiveness of those controls to the Secretary of the Navy.

Such things as the separation of key functions and duties (for example, one individual should not be responsible for both ordering and receiving supplies or equipment), written policies and procedures (for example, all personnel should have a complete understanding of what their jobs are, what is expected of them in performing those jobs, and to whom they are responsible), and even taking a vacation are desirable and effective internal controls.

## Why is taking a vacation a desirable internal control?

Let's say you have a team member who never relinquishes control over a process and has too much individual autonomy. He or she may be in a position to circumvent whatever controls are in place and, in turn, be tempted to commit fraud or simply act in a wasteful manner. Vacations allow another set of eyes to look at the records and sometimes identify processes or transactions that are questionable. To satisfy part of NAS's audit mission, we review internal controls at naval activities in order to determine if taxpayers' resources are accounted for, safeguarded, and effectively and efficiently used in accordance with laws and regulations.

The DON has had much success with implementing effective internal controls because its top leadership knows controls are important. That top leadership is constantly working to strengthen controls because of the value added. For example, internal controls over financial reporting ensure that decision makers have reliable financial and management data, and that resources are efficiently and effectively used. That emphasis establishes the control environment, and the effectiveness of that control environment has led to a number of success stories – most recently displayed by the DON's efforts in the aftermath of Hurricane Katrina.

At the request of top DON civilian and military leaders, the NAS performed seven major audits while DON relief efforts were underway. Our audits showed that, while there were opportunities for improvement, internal controls were in place and operating effectively.

The audits did not find any significant instances of waste or mismanagement. In fact, the audits themselves served as an internal control put in place -- by the leadership request for the audits -- to ensure good stewardship of DON resources.

Nevertheless, the Department has also experienced some control failures that may have been precluded if more effective internal controls were in place and implemented, as detailed in the following three cases.

Two holders of government purchase cards were able to create six shell companies and process fraudulent transactions, costing the DON and the taxpayer about $600,000. This was allowed to occur because the Authorizing Official (AO) did not perform required oversight. Ironically, the fraud was caught when the negligent AO was promoted to another position, and the new AO, while conducting an oversight review, found purchases that looked questionable.

One individual was given too much control over transactions processed because he was a "trusted employee." Essentially, this individual was given

"a recent audit reported substantial weaknesses in the processing of interagency procurement contracting actions valued at over **$66 million**"

super-user access to an information system used to process and pay travel claims. Using that super-user status, which overrode internal checks and balances in the system, enabled the employee to create, process, and self-audit travel claims and -- as you may have guessed -- disburse travel funds to his personal savings accounts using those self-generated claims as the basis for the payments. We could substantiate that the individual had embezzled nearly $500,000. As mentioned previously, one of the most fundamental internal controls is separating those functions and/or duties that are dependent on each other. To permit any individual to be in control of an entire process, especially a process that involves money, is poking the fraud bee's nest with a very short pole -- someone is going to get stung.

A recent headline read: "Senior Chief Stole $56G from Shipboard Food Fund." A senior chief petty officer was convicted of stealing money from the ship's chiefs' mess fund. How could that happen? The embezzlement was possible because the chief petty officer had sole signatory authority over the account used to purchase all food. He could, and did, write checks directly from the account to his personal creditors as well as himself. The basic internal control weaknesses were inadequate separation of duties and inadequate supervision. Independent and periodic review of the chief's ships' mess fund may have caught the checks written to non-Department creditors as well as directly to the senior chief. There was no independent oversight of the mess fund, and larceny occurred as a result. The senior chief petty officer pleaded guilty and was reduced in rank to seaman and fined $35,000.

The NAS has found other instances of breakdowns in internal controls that have led to outright fraud, but a vital message for you to take away from this article is that internal controls are not designed solely to prevent fraud. Lax controls most often lead to just plain waste and mismanagement, and that can either cost the DON and the taxpayers substantially more than fraud or adversely effect achievement of program goals. As an example, a recent audit reported substantial weaknesses in the processing of interagency procurement contracting actions valued at over $66 million. Ultimately, NAS's work showed that the activities audited did not have adequate internal controls to provide reasonable assurance that services were acquired efficiently and effectively or that the DON received what it paid for. Some examples of the audit findings revealed the following:

None of the 26 contracts reviewed had used a Quality Assurance Surveillance Plan for services. Only one of 26 contracts (4 percent) had evidence of adequate competition. None of the three organizations audited nor the servicing agencies proactively confirmed contractor employees' qualifications. Eight of 26 contracts (31 percent) had no evidence of the deliveries by the contractor.

These problems occurred because individual employees did not do their jobs and because the most fundamental internal control of all -- oversight by managers and supervisors -- was not effective.

The DON believes strongly in internal controls – not for audit purposes, but for management purposes. Strong internal controls can help an organization achieve performance targets and goals, prevent loss and waste of resources, ensure reliable information reporting, and attempt to avoid damage to reputations.

They also help avoid the potential erosion of public confidence in the DON's ability to be a good steward of the public's money. Such erosion always follows stories reported about fraud, waste, and mismanagement. More importantly, in the context of national defense, effective internal controls lead to efficient and effective operations that are vital to our national security and the prosecution of the Global War on Terrorism.

Conversely, every dollar lost to fraud, waste, and mismanagement, is a dollar that cannot be used to support our nation's defense, which lessens our ability to properly equip, train, and staff our forces in order to give them the best possible chance of success on the battlefield.

# Management controls may have gone away, but good internal controls are here to stay!

Some current issues facing the Department can be used as opportunities to take a fresh look at the internal control mechanisms we have in place.

These include the relatively new A-123 requirement that top executives must certify the effectiveness of internal controls, the need for auditable financial statements, the reliance on electronic data for decision-making and accountability over assets, tighter budgets, and the demographics of shrinking workforces.

Continuous reviews of internal controls are needed to ensure that they remain effective in changing times.

Such reviews could lead to strengthening the control, eliminating the control because of either redundancy or obsolescence, or merely validating that the current control in place is proper and effective. I hope this article has shed a clearer light on internal controls and how we use them every day.

I also hope this article has emphasized the importance of internal controls as a means of demonstrating to our fellow taxpayers that we are spending their tax dollars judiciously. Management controls may have gone away, but good internal controls are here to stay!

## Gregory Sinclitico, Naval Audit Service

### Assitant Auditor General for Internal Controls and Command Support Audits

Mr. Sinclitico is the Assistant Auditor General for Internal Controls and Command Support Audits for the Naval Audit Service.

He is directly responsible for all audits that evaluate the existence and proper execution of management controls, and also provides assistance to the Naval Criminal Investigative Service (NCIS) in the detection and prevention of economic crimes.

Mr. Sinclitico has 26 years of government auditing experience. He earned a Bachelor of Arts degree in English, Bachelor of Science in Accounting, and is a Certified Professional Accountant and a Certified Internal Auditor.

# NAVAL AUDIT SERVICE

The Naval Audit Service is entrusted by the **Secretary of the Navy** (SECNAV) to provide independent, professional internal audit services that assist Naval leadership in improving efficiency, accountability, and program effectiveness. The Naval Audit Service accomplishes this mission, which is set forth in SECNAV Instructions 5430.100 and 7510.7E, by **performing internal audits** of Department of the Navy organizations, programs, activities, systems, functions, and funds.

These audits are to evaluate whether:

- Department of the Navy information is reliable
- Resources have been safeguarded
- Funds have been expended consistent with laws, regulations, and policies
- Resources have been managed economically and efficiently
- Desired program performance has been achieved

Secretary of the Navy Instruction 7510.7F gives auditors full and unrestricted access to all personnel, facilities, records, data bases, documents, or other Department of the Navy information that is needed to accomplish an announced audit objective.

## Other functions

Other functions for which the Naval Audit Service is responsible include:

Providing audit policy guidance, surveillance, and review of audits conducted by nonappropriated fund organization auditors

Monitoring Department of the Navy contracts for audit services to ensure compliance with Department of Defense guidance

Supporting the Naval Inspector General in executing the DON Audit-Followup Program

Serving as the focal point for internal audit policy relative to the DON Management Control Program

Providing audit assistance to the Naval Investigative Service Command.

The Central Office of the Naval Audit Service is in the Washington Navy Yard, Washington, DC. The Audit Service has area offices in Virginia Beach, VA, and San Diego, CA.

## Review Methods, and Scope and Effect of Work

Credibility is our stock in trade. Our audit work is reliable because our review methods are careful, disciplined, and methodical.

The methodology for our review work must conform with generally accepted government auditing standards.

Strict controls and formal procedures ensure that our findings and conclusions are well supported and that the support is well documented.

Before we release our findings and conclusions, audit work is thoroughly reviewed by quality control reviewers independent of the audit team that did the work.

The operating budget of the Naval Audit Service is about $40 million per year, and the staffing is about 390 persons, most of whom are auditors or other professional personnel.

We strive to build cooperative and effective working relationships with Navy managers, while maintaining our independence. In our management consulting and capacity evaluation reviews, we work hand in hand with management personnel.

# Stopping the Buck

by Earl E. Devaney and Chris W. Martinez

4

## Establishing a Heightened Standard of Accountability

## INTRODUCTION

By far, the most effective way for government to prevent ethical and legal abuses within its ranks is not to focus myopically on individual instances of wrongdoing as they occur, but to imbue one's workforce with an affirmative, all-permeating sense of integrity – to shine a light of excellence that dispels the shadows from which malfeasance sprouts. This article is a discussion of quotes from notable historical figures, provisions of law, and other authoritative sources establishing the theoretical basis for holding high-level officials accountable for cultures of waste, fraud, abuse, or other indiscretion within their organizations. That is to say, this standard of supervisory responsibility does not depend on whether the official knew or should have known of the bad acts of his or her subordinates, or participated in them to any degree. Instead, it is the high official's duty to actively prevent, seek out, and eradicate the harmful mentalities that can result in such negligence or misdeeds. Furthermore, because no duty truly exists without a consequence for having failed it, this article also provides a theoretical basis for holding such senior officials to account for their unwillingness or inability to prevent a harmful culture from growing within their organizations.

## HISTORICAL BASIS OF HEIGHTENED ACCOUNTABILITY

A half century ago, President Harry S. Truman kept on his White House desk a famous sign that read "The Buck Stops Here." The expression, stemming from a poker term, meant that although people in government often "pass the buck" of responsibility to others, the highest executive official – in his case, the President – would accept final responsibility with vigor and aplomb.

"The Buck Stops Here" is not just a slogan, but a noble and cardinal principle of leadership. It is not merely a folksy phrase, but in fact a concept that sits at the heart of the American constitutional design, and animates the very mechanisms of our democracy. Indeed, the Founding Fathers themselves expressly intended the American executive to focus accountability on the few at the top of its hierarchy, so that the people's criticisms and agitations for change could not be dispelled fruitlessly into a generic mass of bureaucracy – so that the buck could not be passed in perpetuity.

Expanding on the theme, one might be reminded of another timeless credo, embraced by the likes of Franklin D. Roosevelt, Theodore Roosevelt, Winston Churchill, and John F. Kennedy, that "with great power comes great responsibility." The Supreme Court has echoed a similar wisdom, remarking, for instance, that "the greater power of [high-level] officials affords a greater potential for a regime of lawless conduct." The founders, understanding the importance of this concept, specifically discussed the way in which the proposed constitutional structure would bestow great power upon the Executive, while simultaneously imposing on it full accountability for actions taken on its watch. Alexander Hamilton, writing in the Federalist Papers, explained why the Constitution must create a single President and not the sort of executive council formerly used by the Crown of England and some early American states. He remarked:

***But one of the weightiest objections to a plurality in the Executive . . . is that it tends to conceal faults and destroy responsibility . . . .***

* * *

***. . . It often becomes impossible, amidst mutual accusations, to determine on whom the blame or the punishment of a pernicious measure . . . ought really to fall.***

Dispersing executive responsibility among many subordinate actors, Hamilton warned, would "deprive the people of the two greatest securities they can have for the faithful exercise of any delegated power" in that: (1) the "restraints of public opinion" would become less effective, due to the uncertainty of whom to blame; and (2) the censure or removal from office of responsible parties would be more difficult because of this same uncertainty and diffusion of accountability.

Such sentiments were not isolated to Alexander Hamilton, but formed an integral cornerstone of the proposed design and function of the American executive branch. For instance, Thomas Jefferson similarly opined, "Responsibility is a tremendous engine in a free government. Let [the Executive] feel the whole weight of it then by taking away the shelter of his Executive Council." More generally, Jefferson also wrote, "Responsibility weighs with its heaviest force on a single head," a thought mirrored with striking similarity by Hamilton, who stated, "The sole and undivided responsibility of one man will

naturally beget a livelier sense of duty and a more exact regard to reputation." Without question, Hamilton and Jefferson were in strong agreement that accountability in government must be focused on, not eschewed from, the highest strata of executive power, where concentrated responsibility would instill in this small elite a robustness of character and obligation.

Of course, to say that the President may not retain an executive counsel to dispel blame is not to suppose that the President may not appoint and oversee executive officials possessing delegated powers. Indeed, cabinet officials have existed from the very beginnings of the republic, Thomas Jefferson and Alexander Hamilton themselves being the first Secretary of State and Secretary of the Treasury, respectively. Therefore, as a matter not only of history, but also common sense, one can logically extend the founders' intent to impose accountability on the President to secretaries and other top-level officials in the government. In fact, as the Executive Branch and its delegated powers have grown, applying this tenet of responsibility to secretaries, assistant secretaries, and the like becomes a practical necessity in modern government. To do otherwise would render the axiom "with great power comes great responsibility" meaningless, allowing subordinates with tremendous authority to exempt themselves from the accountability standard applicable to the President.

## SETTING A HIGH STANDARD

Another closely related adage, so common as to defy attribution, is "leading by example." Echoed in countless forms throughout time and culture, this maxim calls for leaders to seize the initiative, be proactive, and set a standard of behavior by their conduct. This means a leader may not turn a blind eye to malfeasant or negligent behavior, but must affirmatively create – in both deeds and words – a culture or atmosphere of excellence and ethics that will pervade his or her organization throughout the moments and spaces of thought that specific admonitions and instructions do not touch.

As such, the upper-level official serves as a model of behavior for all below, and no such leader may idle in moral silence. As an unknown person cogently stated, "A leader leads by example, whether he intends to or not." In this way, the mere absence of a leader's pursuit of excellence and disdain for corruption and waste is in fact an unwitting example for the institutional sloth that inevitably follows. High-level officials possess extraordinary powers and duties; they must not behave with ordinary ethical standards.

These cardinal principles are not merely abstractions that may be intangibly lost on the day-to-day operations of government; they find specific manifestations throughout law and executive policy. For instance, federal law requires government officials to take proactive, affirmative steps to prevent corruption and waste in the programs they oversee. In general, all federal employees have an obligation to combat "waste, fraud, abuse, and corruption" in the government. However, officials also have a duty to avoid creating even the mere appearance of a legal or ethical violation. Though generally stated, this obligation to avoid the appearance of waste, fraud, abuse, and corruption underlies management's responsibility not just to address indiscretions when they arise, but also to employ prophylactic measures that will effectively head off problems before they materialize, thus minimizing any appearance of impropriety. In other words, when applied to a managing official, the duty to avoid the appearance of malfeasance is just another way of stating that the official must foster among his or her subordinates an observable culture of ethical, conscientious, and legal conduct.

More specific examples of this principle abound. For instance, federal ethics regulations provide that every agency head "is responsible for and shall exercise personal leadership in establishing, maintaining, and carrying out the agency's ethics program." This express invocation of personal leadership, rarely found in statutes and regulations, inevitably implicates the traditional leadership principles of accountability, duty, and initiative. Moreover, the President's Office of Management and Budget (OMB) has promulgated guidelines that illustrate high-level officials' obligation to take affirmative steps against financial waste. One OMB Circular requires agencies and managers to "take systematic and proactive measures" to create comprehensive internal control, identify necessary improvements, and continuously provide assurances that the internal control is operating effectively. This policy, like the ethics regulations above, unambiguously shows that upper-level managers have a responsibility to combat cultures of sloth and wrongfulness within their organizations that extends well beyond a simple duty to pursue specific violations as they become obvious.

## RECENT EXAMPLES

The consequences of allowing an atmosphere of bureaucratic indiscretion and laziness to go unchecked are very real and often quite severe. Two fairly recent examples of collapses of internal oversight in government provide a glimpse of the corruption that can manifest in neglected organizational environments.

A procurement officer at the U.S. Air Force, Darleen A. Druyun, grossly enriched herself at the taxpayers' expense by manipulating the military contracting process. In light of the far-reaching influence she had over Air Force contracting at the time, the Pentagon was subsequently forced to review 407 contracts that she may have tainted over the course of her nine years as a procurement official, in addition to "eight other contracts worth about $3 billion" that the Pentagon further realized may have been "sped up, interrupted or unduly influenced" by Druyun. Former bosses and other coworkers and associates painted a clear picture of the culture of unaccountability that allowed Druyun to execute her plans unchecked. For instance, "Air Force officials coined the term 'DSS: Darleen Says So' as a short response to dismiss questions about Druyun's decisions." Much of the time, she had no immediate supervisor whatsoever, and even when she did, the supervisor was often relegated to second chair, sometimes even feeling "like summer help." The Pentagon's acting acquisition chief, Mike Wynne, later admitted that "all of the leadership has to take responsibility for creating an environment that would have allowed" Druyun to corrupt the contracting process, and Senator John McCain remarked, "I don't know if she did it alone or not, but where was the oversight of the Secretary of the Air Force" and the official "who was supposed to be in charge of acquisition?"

Similarly, "lax oversight" and a culture highly forgiving of ethical violations allowed a National Institutes of Health (NIH) researcher to provide a pharmaceutical company with protected human tissue specimens in exchange for "hundreds of thousands of dollars in consulting fees," in violation of federal law and ethics rules. Even though the researcher was clearly required by federal rules to disclose all of his consulting arrangements, "his failure to file was not unusual" because many NIH doctors dismissed the disclosure rules as little more than "a bureaucratic nuisance." A U.S. House of Representatives investigation later concluded that "inadequate oversight and control over" human tissue repositories at the NIH had allowed the researcher to engage in such "serious misconduct" undeterred.

These two scandals provide just a tiny sample of the literally countless ethical and legal abuses that can and have resulted from government's failure to inculcate its workforce with even modest standards of integrity. In both situations, the coworkers and even the supervisors surrounding the corrupt individual greatly enabled that person to manipulate or ignore rules specifically designed to prevent such malfeasance. Truly, the hallmark of nearly every past scandal – as surely will be the case in future scandals – is a workplace riddled with systemic carelessness and disregard, a house of cards just waiting to be pulled down by individuals willing to enrich themselves at the public's great expense.

## CONCLUSION

Common sense, timeless wisdom, and public policy all strongly indicate that high-level officials have more than a duty not to engage in wrongful acts, or merely to react to problems when they become too glaring to ignore. If "leadership" and "responsibility" are to have any meaningful import, government must hold its senior officials to a higher standard than minimal, personal adherence to the law. Truly, because the greater the power, the greater the potential for harm, we must expect from our top decision-makers a level of accountability and quality of example that is no lesser than the extent of their authority.

Lastly, because every obligation requires consequences for having failed to meet it, one must consider the cost to an official for breaching the duty to maintain an atmosphere conducive to ethical conduct within his or her organization. Consequences might range from mere internal reprimand to full civil or criminal liability. Somewhere between these polar opposites is the option for the official to be removed from his or her position, consistent with the founder's encouragement that the executive branch utilize the power of appointment and removal of its own officers to effect a just and efficient government. Regardless of the specific action taken, if the "buck" is truly to stop, the consequence must be meaningful and significant enough to convey a clear sense to the public that the government will not countenance leadership that permits a culture of wrongdoing and waste to fester under its watch.

# Inspector General

Earl E. Devaney was nominated by President Clinton on July 1, 1999 to be the seventh Inspector General for the Department of the Interior. Mr. Devaney was confirmed by the full Senate on August 3, 1999. As head of the Office of Inspector General, he is responsible for overseeing the administration of a nation wide, independent program of audits, evaluations, and investigations involving the Department of the Interiors programs and operations.

Since assuming his responsibilities, Mr. Devaney has transformed the Office of Inspector General into an innovative organization dedicated not only to detecting fraud, waste, and mismanagement, but also to assist the Department in identifying and implementing new and better ways of conducting business. Mr. Devaney and his team of senior managers have worked diligently toward developing strong working relationships with senior departmental managers, congressional staff and key congressmen and senators. Armed with a philosophy that blends cooperation with strong oversight and enforcement, the Office of Inspector General for the Department of the Interior has made significant advances under the leadership and vision of Mr. Devaney.

Mr. Devaney began his law enforcement career in 1968 as a police officer in his native state of Massachusetts. After graduating from Franklin and Marshall College in 1970 with a degree in Government, he became a Special Agent with the United States Secret Service.

At the time of his retirement from the Secret Service in 1991, Mr. Devaney was serving as the Special Agent-in-Charge of the Fraud Division and had become an internationally recognized white collar crime expert regularly sought by major media outlets. During his tenure with the Secret Service, Mr. Devaney was the recipient of five U.S. Department of Treasury Special Achievement Awards and numerous honors and awards from a wide variety of professional organizations.

Upon leaving the Secret Service, Mr. Devaney became the Director of the Office of Criminal Enforcement, Forensics and Training for the U.S. Environmental Protection Agency. In this position, Mr. Devaney oversaw all of EPA's criminal investigators, EPA's Forensics Service Center, and the National Enforcement Training Institute. Mr. Devaney's years of managerial excellence were recognized in 1998 by the prestigious Meritorious Presidential Rank Award for outstanding government service.

Presently, Mr. Devaney is the Chairman of the Presidents Council on Integrity and Efficiency Human Resources Committee. Having graduated from Georgetown University's prestigious Leadership Coaching Program, Mr. Devaney's vision for the Human Resources Committee is to cultivate and advance leadership development for the entire Inspector General community.

## Chris W. Martinez, Department of the Interior OIG

Chris W. Martinez is an attorney advisor at the Department of the Interior Office of Inspector General. He has worked at the Office of Inspector General since 2005.

He was a law clerk for Kohn, Kohn and Colapinto, L.L.P. – Washington, D.C., summer 2004 and spring 2005.

He graduated with a J.D. from the George Washington University Law School in 2006.

Mr. Martinez received a B.A. in political science from the Pennsylvania State University in 2003.

ATTORNEY ADVISOR

# About the DOI

## MISSON

The mission of the Office of Inspector General (OIG) is to promote excellence, integrity and accountability in the programs, operations, and management of the Department of the Interior. The work of the OIG is designed to:

• Promote DOI's efforts to preserve and protect the Nation's natural and cultural resources and protect DOI facilities;
• Promote effective financial, grant and procurement activities;
•Further DOI's efforts to fulfill its responsibilities to American Indians, Alaska Natives and the Insular Areas;
•Promote the highest standards of integrity, impartiality and professionalism within DOI; and,
•Promote effective coordination and improved management practices among DOI's Bureaus and components.

## RESPONSIBILITIES

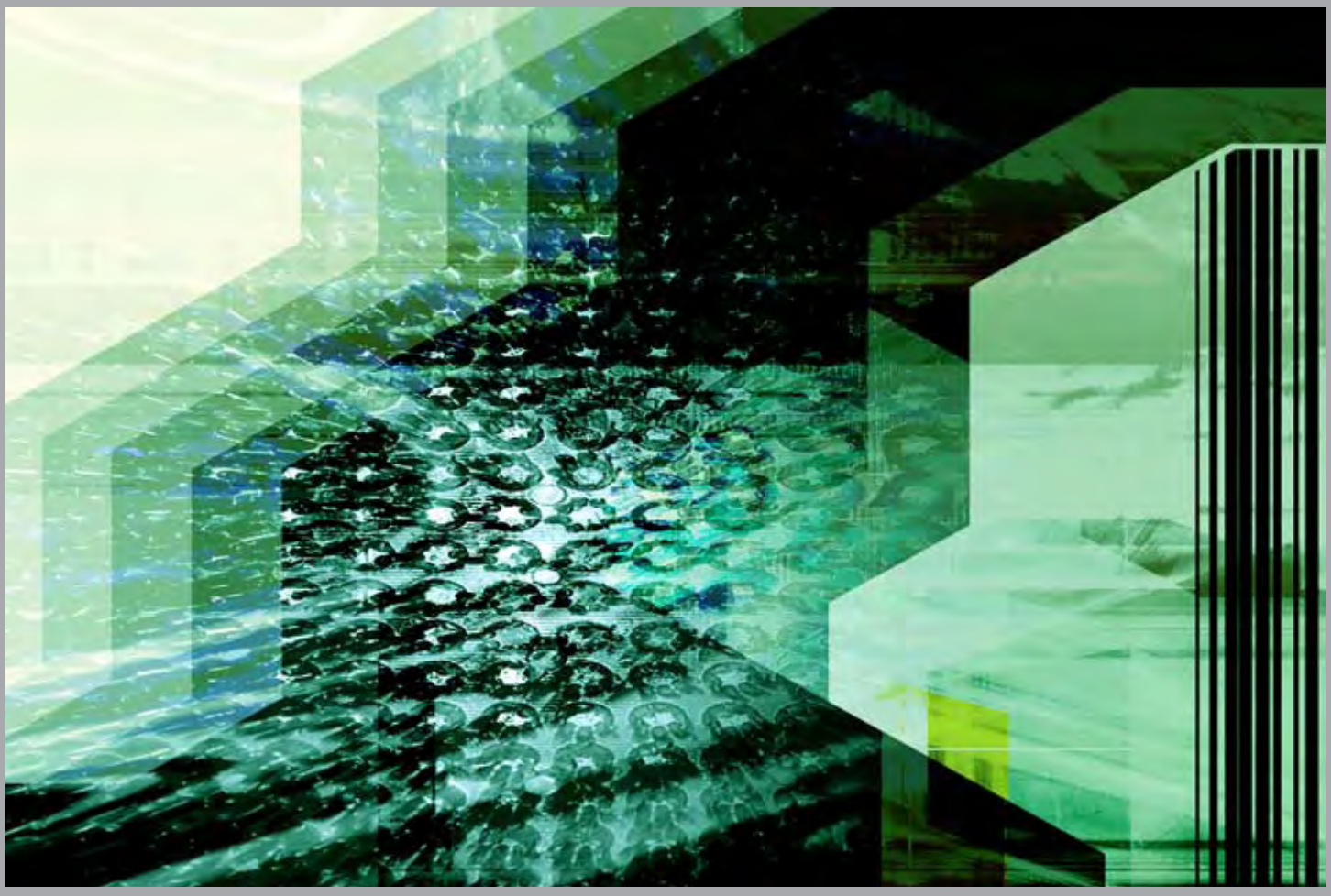
The OIG is responsible for independently and objectively identifying risks and vulnerabilities that directly impact, or could impact, the Department's ability to accomplish its mission. We are required to keep the Secretary and the Congress fully and currently informed about problems and deficiencies relating to the administration of departmental programs and operations.

Effective implementation of this mandate addresses the public's demand for greater accountability and integrity in the administration of government programs and operations and the demand for programs that work better, cost less, and get the results about which Americans care most.

# A Hard Day's Work

by James J. Klein and Tracy B. Lynge

5



## Taking Another Look at the Government Pension Offset Loophole

## Introduction

Would you be interested in earning thousands of dollars in Social Security benefits for only one day of work? When the Social Security Administration (SSA) Office of the Inspector General (OIG) received information that thousands of retiring teachers in Texas were doing just that, our Office of Audit took immediate action, launching a comprehensive review into the matter. This article will discuss the findings from the resulting audit report, Government Pension Offset (GPO) for Texas School Districts' Employees, issued in January 2007.[1]

## History of the GPO Exemption Loophole

SSA pays benefits to the spouses of retired, disabled, or deceased workers covered by Social Security. This spousal benefit was designed as a safety net for those individuals who stayed at home while their spouses worked and paid Social Security taxes. If both spouses work in positions covered by Social Security, the spousal benefit is reduced by the amount of one's own benefit. However, many local and State governments opt out of Social Security coverage, instead paying their employees from a separate pension fund. Until 1977, those government workers could receive their full government pension as well as a full spousal benefit from Social Security. In that year, Congress created the government pension offset (GPO), which mandates a reduced Social Security benefit to spouses and widows/widowers who also receive a monthly pension from a State or local government agency for work that is not covered by Social Security.

In 2002, the Government Accountability Office (GAO) received a referral through its FraudNet service, which is maintained by GAO's Office of Special Investigations. The allegation maintained that some local government employees had found a way to exploit a loophole in the GPO legislation, which stated that anyone working his or her last day in a position covered by Social Security would not be subject to the GPO. The employees were allegedly taking advantage of this "last-day" provision by working for a single day in non-teaching clerical or janitorial positions before they retired from the school system to qualify for the GPO exemption, thereby receiving full spousal benefits for the remainder of their lifetimes in exchange for a few dollars in Social Security taxes deducted from a single day's wages.

GAO issued a report and later testified before Congress that while the use of this loophole appeared to be legitimate, its use raised fairness and equity concerns and could cost the Federal Government $450 million over the long term. GAO recommended a legislative fix due to "potential for abuse of the last-day exemption and the likelihood for its increased use."[2] Congress subsequently closed the loophole with a provision included in the Social Security Protection Act of 2004. As of July 1, 2004, an individual's last five years of employment must be in a Social Security-covered position to qualify for the GPO exemption.

## Why SSA OIG Became Involved

Despite the legislative change, SSA continues to pay full benefits to individuals who retired prior to July 1, 2004 and who claim the GPO exemption based on one day of work. In October 2005, the SSA OIG received a fraud allegation from Joseph Fried, a certified public accountant and director of the Public Program Testing Organization. Fried had followed up on the 2002 GAO report by conducting his own study, and was now alleging that some teachers should not be exempted from the GPO based on one day of work in Social Security-covered positions. Fried's allegation concerned approximately 22,000 teachers who, before they retired from 15 Texas school districts, had paid the districts special fees to work their last day of employment as non-professional employees, specifically to avoid the GPO and collect full Social Security benefits. Fried claimed that these improper GPO exemptions would cost the Social Security Trust Fund $2.1 billion over the employees' lifetimes.

Based on the information received, we decided to conduct our own independent review. Although the allegation named 15 school districts, we limited our review to the seven school districts that hired the largest numbers of these 1-day workers. According to the allegation, these

1 The entire audit can be found at http://www.ssa.gov/oig/ADOBEPDF/A-09-06-26086.pdf.

2 "Congress Should Consider Revising the Government Pension Offset Loophole," GAO Testimony before the Social Security Subcommittee, Committee on Ways and Means, 2/27/03.

seven districts hired approximately 19,000 (86 percent) of the 22,000 employees. Using data from the school districts and SSA's Master Earnings File, we identified a population of 20,248 individuals and randomly selected a sample of 665 individuals for review. We obtained employment information for these individuals from the school districts, interviewed school officials, and reviewed policies and other documentation related to the 1-day worker programs at the seven school districts.

## What Our Audit Found

Of the 665 individuals in our review sample, we determined that 629 (95 percent) should not be exempt from the GPO based on their 1 day of work. Of the 665 individuals, 170 were already receiving spousal benefits at the time of our review, and SSA had exempted 168 of them from the GPO. Projecting our sample results to the entire population, we estimate that 19,212 individuals will receive $110 million in spousal benefits annually for which they may not be eligible—for a lifetime benefit total of about $2.2 billion.

We found that individuals employed as 1-day workers by the seven Texas school districts did not appear to meet the requirements to receive a GPO exemption, due to the questionable nature of the employment. Specifically, we found significant evidence to indicate that the fees paid by these workers were a reimbursement of the wages they received from the school districts, which would preclude the employees from claiming a GPO exemption based on that work. The individuals hired as 1-day workers were generally paid minimum wage, but paid fees to the school districts of up to $750 each, which far exceeded any wages earned. The seven school districts collected approximately $7.4 million in fees from their 1-day workers while only paying them about $900,000.

Our interviews with school district officials indicated that the employees were hired primarily to generate revenue for their districts, rather than to fulfill any actual need for their services. In fact, some officials stated that they would not have hired all of the 1-day workers if they had not collected fees. The school districts used the revenue generated by their 1-day worker programs to pay the wages of the individuals hired, pay general expenses, and finance capital improvements, including resurfacing parking lots; constructing a new nurse's station; building and installing new seating and lighting for auditoriums; building a distance-learning center; and improving the school board's conference room.

## Authority to Provide Social Security Coverage

We determined that five of the seven school districts did not have the authority to provide their 1-day workers Social Security coverage. These five school districts had agreements with SSA, pursuant to section 218 of the Social Security Act, which precluded them from providing Social Security coverage to part-time employees.[3] Although school district officials stated they hired the 1-day workers for full-time positions, we

### Fees Collected and Wages Paid by Seven Texas School Districts

| School District | Number of 1-Day Workers | Total Fees Paid to School Districts | Total Wages Paid to 1-Day Workers |
|---|---|---|---|
| West | 1,860 | $1,069,478 | $62,273 |
| Hudson | 1,887 | 493,100 | 77,744 |
| Lindale | 4,313 | 1,335,205 | 177,696 |
| Premont | 2,186 | 1,052,035 | 87,440 |
| Coleman | 3,642 | 699,498 | 218,520 |
| Sweeny | 2,958 | 1,428,703 | 121,870 |
| Kilgore | 3,402 | 1,289,215 | 140,162 |
| TOTAL | 20,248 | $7,367,234 | $885,705 |

3 The Social Security Act § 218 (a)(1), 42 U.S.C. § 418 (a)(1).

found there was no intent or expectation by either party that the employment would last longer than 1 day.

The application packages provided to individuals interested in the 1-day worker programs at three of the five school districts included letters stating, "In response to your request, this packet is being mailed to you in order for you to work your final day in the Texas Teacher Retirement System under the (insert school district name) as a non professional…" The fourth school district required that applicants submit a resignation letter before their scheduled day of work. The fifth school district called its 1 day worker program the "…one day offset program for Social Security."

Our review of 475 employees from these 5 school districts disclosed that 450 were hired as 1-day workers, and none worked longer than 1 day. Since these individuals did not intend to work more than 1 day, their employment should not fall under positions covered by Social Security on their last day of employment.

## Impact of GPO Exemption on Benefit Eligibility

On average, each GPO exemption is valued at approximately $113,000, based on the average life expectancy of an individual receiving spousal benefits. To illustrate the financial impact of a GPO exemption, consider the case of an individual included in our review. This individual paid a $250 fee to work for one day, and was paid $41.20, from which $2.55 in Social Security taxes was withheld. The individual is now receiving full spousal benefits of $288.80 with no offset for a monthly government pension of $2,177.50. The $250 fee the individual paid was recovered by the value of the GPO exemption for 1 month of spousal benefits. Had SSA imposed the GPO, the monthly spousal benefit payable would have been reduced to zero.

## Beyond Our Findings

The allegation we received in October 2005 identified 8 other Texas school districts that hired approximately 3,285 1-day workers. If the same conditions we found at the 7 school districts we reviewed occurred in these 8 school districts, about 3,107 of these individuals should not be exempt from GPO. Furthermore, we estimate these 3,107 individuals will receive approximately $17.8 million in spousal benefits annually to which they may not be entitled. Over their lifetimes, they could receive about $353 million in spousal benefits.

Our audit disclosed that the 1-day worker programs were generally limited to state and local government entities in Texas. To determine the extent to which this could be occurring in other states, we reviewed SSA's payment records. This review identified 1,303 spousal beneficiaries for whom SSA noted the state of the pension payments and who were exempt from GPO based on the last-day provision. Of these, 1,276 (98 percent) had been employed by a state or local government entity in Texas. We estimate that 995 of the 1,276 individuals were from the 15 Texas school districts identified in the allegation submitted to the SSA OIG.

## What We Recommended to SSA

We found that, generally, SSA relied on documentation provided by the 1-day workers to determine whether they should be exempt from GPO. This documentation included pay stubs and letters addressed to SSA from the school districts stating the individual was employed in a position covered by both the Texas Teachers Retirement System and Social Security on their final day of employment. According to SSA policy, this documentation is considered acceptable evidence that a GPO exemption applies.

Our findings suggest, however, that SSA needs to revise its policies and procedures concerning acceptable proof and evidence for a GPO exemption based on last-day employment. Relying solely on this documentation does not provide SSA sufficient information to determine whether it should exempt an individual from the GPO.

To determine whether an individual should be exempt, we recommended that SSA examine the terms and conditions of these workers' employment and the school districts' agreement with SSA that precludes the districts from providing Social Security coverage to part-time employees.

We also recommended that SSA reexamine the decisions to grant an exemption from GPO for the 168 spouses in our sample, and for other individuals in the population of 20,248 1-day workers employed by the seven school districts.

Finally, we recommended that SSA review the 1-day worker programs at the other eight Texas independent school districts identified in the allegation to determine whether their 1-day workers programs would result in inappropriate GPO exemptions.

## SSA's Response

SSA did agree to review the agreements that are in force between the Agency and the school districts, and take appropriate action if any problems were identified.

However, SSA stated that it has appropriately granted exemptions to the employees in our review, as well as to others who retired prior to July 1, 2004 and who claim a GPO exemption based on 1 day of work. SSA noted that the payment of a fee does not affect the validity of the wages unless the fee is considered a reimbursement of wages paid to the worker.

Regarding the authority for Social Security coverage, SSA stated that because the school districts in our review paid social security taxes for the workers, the school districts considered the positions full time and, therefore, covered under their agreements with SSA.

In our response to SSA's comments, we advised that our review found significant evidence to substantiate that the fees were, in fact, a reimbursement of the wages paid for the one day of work.

We also cautioned SSA that it should not rely on the school districts to determine whether the positions were properly covered by Social Security simply because they paid social security taxes.

## Conclusion

The GPO exemption loophole is only one of the many sensitive and timely issues that our auditors address on a daily basis. As we are, in many ways, the guardians of Social Security's trust funds, the SSA OIG is called on to conduct objective, thorough reviews of issues that are of great importance and concern to people in many sectors of American society.

Although SSA disagreed, in part, with our findings with regard to this particular issue, we have generally enjoyed a productive and mutually beneficial relationship with our partner Agency. And as always, we will continue to strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste, and abuse.

## About the SSA OIG


## Who We Are

The Office of the Inspector General (OIG) is directly responsible for meeting the statutory mission of promoting economy, efficiency and effectiveness in the administration of Social Security Administration (SSA) programs and operations and to prevent and detect fraud, waste, abuse, and mismanagement in such programs and operations.

## James J. Klein, Social Security Administration OIG

### Director, San Francisco Audit Division

James J. Klein is the Director of the San Francisco Audit Division for the Social Security Administration (SSA) Office of the Inspector General (OIG). In this capacity, Jim oversees nationwide performance and financial audits of SSA programs. He also directs regional audits in Alaska, Arizona, California, Hawaii, Idaho, Nevada, Oregon and Washington. Mr. Klein began his Federal career with SSA's Office of Operations in 1982. In 1989, he joined the Department of Health and Human Services OIG as a program analyst, focusing on audits of SSA's programs and operations. When SSA became an independent agency in 1995, Jim joined its OIG as an auditor. Prior to holding his current position, Jim was an Audit Manager in OIG's General Management Audit Division in Baltimore, Maryland. During his career, Jim has received numerous awards for meritorious service, including the President's Council on Integrity and Efficiency Glenn/Roth Award for Exemplary Service and two Audit Awards for Excellence. Jim is also a recipient of the Inspector General's Award and the Commissioner's Citation--the Agency's highest award. Jim received a Bachelor's degree from the University of Delaware.

## Tracy B. Lynge, Social Security Administration OIG

### Senior Public Affairs Specialist

Tracy B. Lynge is a senior public affairs specialist in the Social Security Administration Office of the Inspector General. She reports to the Deputy Chief Counsel for External Relations and is responsible for developing speeches and presentations for senior OIG officials, as well as producing the Semiannual Report to Congress and responding to inquiries from the media, Congress, and the public.

Ms. Lynge was previously a writer-editor in the SSA OIG's Office of Investigations. She came to the OIG in 2004 from SSA's Office of Program Development and Research, where she served as project officer to 10 grantee organizations participating in a national disability-based demonstration. Ms. Lynge began her career with SSA in 2000 as a Presidential Management Fellow. She has a Master of Science in International Affairs from the Georgia Institute of Technology and a Bachelor of Arts from the University of North Carolina at Asheville.

# Digital Forensics

by Craig M. Goscha and Eileen M. Sanchez Rehrig

6

## The Value of Partnership in Support of Criminal Investigations

## INTRODUCTION

E-mail, the Internet, laptops, USBs, MP3 players, cell phones, PDAs, video equipment – today, nearly every crime has the potential to leave digital fingerprints. A scan of the headlines is evidence of this. Everything from white collar crimes to murders has been successfully prosecuted using digital forensics. As crimes become increasingly sophisticated, it is imperative that progressive law enforcement agencies incorporate the collection, preservation, and analysis of digital evidence into their routine investigative efforts.

Recognizing this need and considering budget constraints, in September 2005, the U.S. Department of Agriculture, Office of Inspector General (USDA OIG) entered into a Memorandum of Understanding (MOU) with the Federal Bureau of Investigation (FBI), to become a participating agency in the Heart of America Regional Computer Forensic Laboratory (HARCFL). In partnering with HARCFL, the agency has gained access to a nationwide network of state-of-the-art digital evidence laboratories and training centers.

Participation in the HARCFL has been beneficial in obtaining training, sample policies and procedures, and, as needed, FBI assistance in our forensic examinations. As part of the MOU, USDA OIG's National Computer Forensic Division (NCFD) details Forensic Examiners to the HARCFL. In doing so, we have direct access to a Regional Computer Forensics Laboratory's (RCFL) policies, procedures, and training. This ensures that our NCFD Laboratory's guidelines parallel those of a RCFL – moving us one step closer to our goal of becoming an accredited laboratory and ensuring that our digital forensics work is readily accepted in court.

As an additional benefit, all NCFD Forensic Examiners have access to the RCFL's multimillion dollar examination hardware and software, allowing us to maximize our equipment budget.
Because of the sizable investment in both equipment and training needed to support a digital forensics unit, collaborating with the RCFL Program is an economical solution to help law enforcement meet its digital forensics needs. By partnering with one of the RCFLs, agencies obtain the use of secure, full-service digital evidence laboratories and training centers that provide expert assistance to law enforcement agencies within their designated service area. These services are provided to partnering agencies at no cost.

This article focuses on the benefits that USDA OIG has realized as a participating agency with the HARCFL.

Everything from white collar crimes to murders has been **successfully prosecuted** using digital forensics.

## History of USDA OIG's National Computer Forensic Division

"It is the mission of the NCFD to provide computer forensic services, courtroom testimony and clear and understandable results of computer forensic examinations aid in the preservation, seizure and collection of computer evidence to the USDA OIG and any agency affiliated with the United States Department of Agriculture."

The USDA OIG computer forensic unit was created in 1987 with one forensic examiner who was supervised by a fieldspecial agent-in-charge.

Since then the unit has evolved into a national program that reports directly to the Deputy Assistant Inspector General for Investigations.

The staff currently includes a director and four Forensic Examiners who are located in Kansas City, MO. The NCFD provides service to six USDA OIG regions across the United States.

These services include pre-search guidance, on-site assistance, complete forensic examinations, and related testimony in support of criminal prosecutions.

USDA OIG's use of the NCFD has increased steadily over the last few years. NCFD has already performed work on more OIG criminal cases in the first eight months of Fiscal Year 2007 (36 cases involving 9,058 gigabytes (GB) of data) than it performed in all of FY 2006 (33 cases involving 7,500 GB of data).

Some recent examples of NCFD's work include developing forensics evidence that was essential to negotiating a guilty plea from a USDA employee who had reproduced and sold 41 pirated copies of USDA-licensed software on two internet auction sites, and the recovery of computer evidence that was used to convince a subject to confess to the receipt and interstate transfer of stolen infant formula.

The NCFD is also being called upon by USDA agencies to provide technical support for their employee misconduct investigations.

Since most USDA agencies do not have the ability to analyze electronic evidence obtained during personnel investigations, they request assistance from NCFD.

In the first 8 months of Fiscal Year 2007, NCFD provided forensic analysis for 17 non-criminal cases referred from other USDA agencies. This compares to 13 cases in FY 2006. NCFD's work on such cases has had the added benefit of fostering stronger relations between USDA OIG and other USDA agencies.

NCFD responsibilities have recently been expanded to include investigating intrusions into the Department's computer systems as well as investigating allegations of compromised personal identifying information (PII).

Requests for technical support have recently come from USDA's Office of the Chief Information Officer, Cyber Security Division for forensic analysis of USDA network intrusions. Network intrusions are considered a homeland security issue that must be reported to the Department of Homeland Security.

As part of this expanded role, NCFD recently determined that two USDA computer servers had been compromised multiple times by hackers but that the database containing PII for 26,000 USDA employees had not been compromised or transferred from USDA computers.

The work that NCFD performed was critical in reassuring the Secretary of Agriculture that the sensitive and private information contained on these servers had not fallen into the hands of the identify theft industry.

## History of the Regional Computer Forensics Laboratory Program

The RCFL Program is a nationwide FBI-funded network of state-of-the-art digital forensic laboratories and training centers devoted entirely to the examination of digital evidence in support of investigations such as:

- Terrorism
- Crimes of Violence
- Child Pornography
- Internet Crimes
- Financial Crimes
- Fraud
- Theft or Destruction of Intellectual Property

From its beginning as a pilot project in 1999, the RCFL Program has grown to a network of 14 laboratories and training centers across the United States as illustrated in the map below.

Collectively, the RCFL Program is available to 4,321 law enforcement agencies in 17 states. In 2002, the RCFL National Program Office (NPO) was established to oversee the operations of all the RCFLs and to facilitate the creation of new facilities.

As part of a cooperative partnership, talented and experienced personnel are detailed from Federal, State, and local law enforcement agencies to the RCFLs. The details are performed on a full time basis and last approximately two years.

Individuals detailed to the RCFLs provide digital forensic examinations that benefit the entire law enforcement community. In return, the examiners are provided access to state-of-the-art forensic equipment and training at no cost to the participating agency. Typically, an RCFL consists of 15 people – 12 Examiners and 3 support personnel.

## How do RCFLs Operate?

The RCFLs operate under detailed MOUs with each participating law enforcement agency. Funding for the RCFLs is provided by the FBI's RCFL NPO.

Local Executive Boards, comprised of the heads of the participating Federal, State, and local law enforcement agencies, provide operational guidance

and oversight of their respective RCFL. The local boards oversee the activities of their RCFL, and in that capacity, may review any policy, procedure, practice, and/or rule affecting the day-to-day operations of the RCFL.

Currently, the USDA OIG NCFD Director is serving as the co-chair on the board of directors for the HARCFL. This provides NCFD with an opportunity for input into the operational guidance and oversight of the HARCFL. It also affords the NCFD the chance to establish relationships with the other partnering agencies.

As a benefit of the partnership between the RCFL and the participating agencies, the RCFL provides extensive training – free of charge – to the assigned Forensic Examiners and ensures that they become FBI Computer Analysis Response Team (CART) certified Forensic Examiners. All RCFL Examiners must be CART certified to conduct examinations.

By requiring CART certification for each RCFL Forensic Examiner, we are ensured of the highest level of competence and proficiency for digital evidence examinations.

## What Is the Heart of America Regional Computer Forensic Lab?

Part of the nationwide network of RCFLs, HARCFL provides complete digital and electronic forensic analysis to all law enforcement agencies in Kansas and the western two-thirds of Missouri at no cost.

To this end, its examiners are available to provide pre-search guidance, on-site assistance, complete forensic examinations, and related testimony in support of criminal prosecutions.

## Benefits of the USDA OIG Partnership with the HARCFL

The nearly 3-year-old partnership between USDA OIG and HARCFL has resulted in numerous benefits for USDA OIG including technical training; access to policies and procedures; research and development; exposure to the most technologically advanced computer equipment available; access to digital forensics examination and advisory services; broad experience in a variety of digital forensics cases; and a stake in the management of the RCFL.

## Technical Training

The HARCFL serves as a training laboratory for its participating members. By detailing USDA OIG Forensic Examiners to the laboratory, we have received the following key training benefits:

• Two of the NCFD examiners have received at least seven weeks of training to become certified forensic examiners under the FBIs CART program. This training cost approximately $15,000 and was paid for by the RCFL NPO. No USDA OIG funds were expended for this training.

• Following CART certification, the examiners were equipped with approximately $60,000 in forensic tools and materials and received advanced forensic training to remain a certified examiner. The examiners were also provided the opportunity to achieve specialization in various related sub-disciplines, such as MAC, Linux, PDAs, cell phones, etc. Again, no USDA OIG funds were expended for the equipment or training.

• Our entire agency has gained access to the laboratory's state-of-the-art training room, allowing all NCFD employees and USDA OIG agents the ability to participate in a variety of digital forensics courses and workshops offered by the laboratory.

## Associate Examiner Certification

USDA OIG has been rotating NCFD staff through the HARCFL to take advantage of the training, thus allowing each member to receive

and maintain their FBI CART certification through the Associate Examiner Program.

USDA OIG recently became the first participating agency in the RCFL program to have an examiner attain Associate Examiner Certification through the newly created formalized program.

Following certification under the Associate Examiner Program, the RCFL NPO continues to provide and/or pay for all training expenses that may be required for a Forensic Examiner to maintain his or her FBI CART certification.

In fact, the examiner is not only afforded the ability to maintain the certification in his or her primary discipline of digital forensics but may also maintain certification in various sub-disciplines. Completion of this training will normally require participation in two 40-hour courses and the successful completion of competency and proficiency tests, with final training requirements determined by the RCFL NPO.

In exchange, the Associate Forensic Examiner is required to conduct and complete five forensic examinations per year, involving digital evidence as assigned by the HARCFL. The required examinations may include USDA OIG cases.

## Policies and Procedures

In 2005, the USDA OIG NCFD was a rapidly growing forensic unit. As the NCFD continued to evolve into a routine part of USDA OIG investigative efforts, we saw participation with the HARCFL as a means of ensuring that NCFD laboratory policies and procedures would parallel those of a state-of-the-art forensic laboratory.

Currently, the HARCFL is applying to become an American Society of Crime Laboratory Directors (ASCLD) accredited laboratory. In order to obtain certification a laboratory must demonstrate that its management, personnel, operational and technical procedures, equipment, and physical facilities meet ASCLD established standards.

While not currently required, accreditation may become necessary for all digital forensic labs desiring to present digital evidence in federal court. Keeping this expectation in mind, the President's Council on Integrity and Efficiency (PCIE) formed a working group to develop standards for digital forensics performed within the OIG community.

Members of the NCFD are currently participating in this working group. The first phase of this project resulted in the working group developing a series of questions to be included in the PCIE Investigations Peer Review Guide. During the second phase of the project, NCFD will play a significant role in developing a best practices guide on digital forensics for the PCIE IT Roundtable.

Through our work with HARCFL and the PCIE IT Roundtable, we have been able to develop internal policies and procedures that ultimately can be shared with the PCIE community and we expect to be well positioned when we seek laboratory accreditation. We expect to realize both cost and time savings when seeking our accreditation by learning from the experience of the HARCFL in obtaining their accreditation and from the PCIE IT Roundtable's work on establishing best practices for computer forensic units.

## Research and Development

The RCFL Program continuously tests current forensic hardware and software. Our affiliation with HARCFL allows our Forensic Examiners access to these forensic tools as well. The ability to "test before you buy" provides the NCFD with valuable information that helps formulate our yearly budget request for the procurement of forensic hardware and software. Due to budget constraints, when procuring technology and training for our lab and its Forensic Examiners, we, like any other agency, must be sure that our return on investment is very high.

Participation in the HARCFL has enabled us to make extremely sound training and procurement decisions for the NCFD with little or no capital outlay or personnel commitment, based on the testing and research and development effort provided by the HARCFL, the RCFL NPO, and CART.

## Other Benefits

The RCFL NPO provides each Forensic Examiner with a baseline set of equipment valued at approximately $26,000.

For Forensic Examiners certified in specific digital forensics examinations of such devices as cellular telephones, personal data assistants, video equipment, or specialized operating systems (e.g., Linux, Macintosh, etc.), the RCFL NPO provides additional advanced equipment and software.


Because forensic technology must be updated approximately every 18 to 24 months, joining the HARCFL represents a significant cost savings to our agency.

In addition, our examiner participates in a collegial and collaborative work environment where knowledge obtained by the laboratory is shared among all examiners and problems and issues are addressed collectively.

Furthermore, the expertise and knowledge gained by our examiners remains in and enhances our agency, with the individuals assigned to the HARCFL sharing their new found techniques with their colleagues at NCFD.

## USDA & HARCFL Joint Efforts

The partnership between the USDA and the HARCFL has already proven to be valuable on multiple occasions.

For example, a USDA OIG investigation requiring the examination of 750,000 emails from 3 different email formats (Notes, Outlook, and GroupWise) was made possible through the utilization of state-of-the-art HARCFL software and hardware. The investigation, involving a health and safety issue with national and international ramifications, required the NCFD to provide the Inspector General with timely and accurate results from the analysis.

This could not have been accomplished had we not been provided access to the HARCFL equipment, software, and support staff. Through the use of HARCFL's Storage Area Network, NFCD was able to store and analyze the large volume of data in a timely fashion.

Access to this type of technology also provided NCFD management invaluable insight into the type of hardware and software that the NCFD would need to purchase to handle these types of large cases in the future.

Similarly, prior to the execution of a USDA search warrant in Houston, the NCFD was informed that there were a minimum of 15 computers located within the search warrant site and that all computers would need to be imaged on-site.

Through our participation in the RCFL program, we were able to contact the Director of the Greater Houston RCFL and coordinate its participation in the warrant with just one phone call. The Greater Houston RCFL not only furnished five highly skilled examiners, but also provided the equipment necessary to image what ended up being a total of 18 workstations and 3 file servers.
Having the Greater Houston RCFL on-site allowed USDA OIG to save resources and travel expenses by only sending one examiner to Houston. Additionally, because of our close working relationship with the RCFLs, we had confidence in knowing that the RCFL members providing on-site assistance were highly skilled and well-trained forensic examiners.

USDA OIG's partnership with HARCFL was vital when we received a request for forensic analysis of a video surveillance system seized during a USDA OIG search warrant. As part of the investigation, the case agent requested an analysis of the seized video equipment. This request had an unusually short time frame as the evidence was needed in court for the arraignment of a suspect. This proved to be problematic since NCFD did not have the capability to analyze video systems in-house.

Specialized equipment to perform forensic analysis of video systems is extremely cost prohibitive for the NCFD. Because of our affiliation with the HARCFL, we were able to call upon them for the analysis. Within two days of submitting our request to HARCFL, their analysis of the video surveillance equipment was complete. This video analysis proved critical to the advancement of the case

and could not have been performed in such a timely manner if the NCFD had not been a participating agency at the HARCFL.

## Conclusion

Since we began our partnership with the RCFL program, the benefits realized by the USDA OIG have far exceeded any expectations.

While the potential monetary savings to the USDA OIG were obvious, we did not anticipate the value of the indirect benefits such as direct access to the hardware, software, and personnel detailed to some of the most advanced computer forensic laboratories across the nation at a moment's notice.

Recent publications and expert opinion suggest that in the future, federal courts may require all digital evidence that is to be presented to have been analyzed by an accredited lab.

By continuing to align our policies and procedures with those of the RCFL, we will be in the best position possible to achieve the certification in a timely and cost effective manner.

Our gratitude to Kevin Steck, Director, HARCFL, who contributed to this article.

### The Office of Inspector General was legislatively established in 1978 with the enactment of the Inspector General Act (Public Law 95-452). The act requires the Inspector General to independently and objectively:

- Perform audits and investigations of the Department's programs and operations;
- Work with the Department's management team in activities that promote economy, efficiency, and effectiveness or that prevent and detect fraud and abuse in programs and operations, both within USDA and in non-Federal entities that receive USDA assistance;
- Report OIG activities to the Secretary and the U.S. Congress semiannually as of March 31 and September 30 each year;

### We accomplish this mission by:

- Investigating allegations of fraud and abuse;
- Using preventive audit approaches, such as reviews of systems under development;
- Conducting audits of the adequacy and vulnerability of management and program control systems; and
- Auditing the adequacy of large USDA payments, such as insurance and deficiency payments, major loans, and retailer food stamp redemptions.

## MISSION

OIG exists as a statutorily created independent and objective unit within USDA, the purpose of which is to conduct audits and investigations; provide leadership and coordination to promote economy, efficiency, and effectiveness and prevent fraud in USDA's programs and operations; and keep the Secretary and the Congress informed as to deficiencies in such programs and operations. USDA's mission is to provide leadership on food, agriculture, natural resources, and related issues based on sound public policy, the best available science, and efficient management. OIG, though independent, must work toward USDA's effectiveness to serve its statutory purpose.

## Craig M. Goscha, U.S. Department of Agriculture OIG

### Director, National Computer Forensic Laboratory

Craig Goscha is the Director, National Computer Forensic Laboratory (NCFD), Office of Inspector General, U.S. Department of Agriculture (USDA OIG). Prior to joining USDA OIG, Craig spent the previous eight years as a Senior Network Engineer and a Network Security Specialist for the Kansas Department of Transportation and Zurich North America in Kansas City, Missouri.

Craig joined USDA OIG in April 2001 as a Computer Specialist in the National Computer Forensic Unit. In March of 2003, Craig was promoted to Supervisory IT Specialist in the National Computer Forensic Unit. The NCFU was elevated to the National Computer Forensic Division in August 2006 at which time Craig was promoted to Director of the Division. Craig has spent the last six years developing the NCFD's presence within USDA as well as within the IG community. He has participated in the PCIE IT Roundtable group, the Computer Crimes and Intellectual Property Section group at the Department of Justice, multiple Curriculum Review Conferences for the Federal Law Enforcement Training Center, and as co-chair of the Local Executive Board of the FBI's Heart of America Regional Computer Forensic Lab in Kansas City.

## Eileen M. Sanchez Rehrig, U.S. Department of Agriculture OIG

### Management Analyst Office of Inspections and Research

Eileen Sanchez Rehrig is a Management Analyst in the Office of Inspections and Research at the Office of the Inspector General, U. S. Department of Agriculture (USDA OIG).

Ms. Rehrig began her federal career in 1991 with the U. S. Department of Justice as a Paralegal Specialist. She then transferred to USDA OIG in 1992.

While at USDA OIG, Ms. Rehrig has held a number of positions including Management Analyst, EEO Specialist, and Planning Specialist. Ms. Rehrig is a graduate of the Pennsylvania State University and holds a Bachelor of Arts in Foreign Service and International Politics. She holds a certificate in Project Management from the George Mason University.

# The Federal Audit Executive Council

by FAEC Chair and and Committee Chairs

7

## A Subgroup of the PCIE Audit Committee

## FAEC Holds Annual Conference

The Federal Audit Executives Council held their annual conference in Virginia Beach, VA on August 8 – 10. The conference, attended by nearly 100 Federal Audit Executives from 38 different agencies, was held at the Founder's Inn Conference Center. The conference focused on Information Technology challenges and issues that face the Federal audit community. Presentations were made by 15 guest speakers from the Federal sector, private sector, and various councils. In addition to IT topics, a panel of IGs discussed independence issues facing the oversight community, the GAO provided an update on the revised auditing standards, the Department of Justice discussed current cybercrime initiatives, an expert in the field of Knowledge Management provided tips on ways to better share information within Agencies, and participants completed an exercise which identified their conflict management style. The conference was chaired by Mary Ugone, Deputy Inspector General for Auditing, DOD. Ms. Ugone is also the current FAEC Chair.

## Federal Audit Executive Council

The FAEC is a Subgroup of the PCIE/ECIE Audit Committee. The PCIE/ECIE Audit Committee is one of seven standing committees formed within the PCIE/ECIE membership to accomplish the mission of the PCIE/ECIE. The Audit Committee's goals are to develop and maintain the highest standards in the conduct of audits in the Federal sector, focus audit activities on high impact areas, actively promote cooperative audit efforts and strategies, and to train and develop professional skills and specialized knowledge within the Office of Inspector General community. The Honorable John P. Higgins, Jr., Inspector General of the Department of Education, is the current chair of the PCIE Audit Committee.

The FAEC is a subgroup of the PCIE/ECIE Audit Committee and serves to provide input on Federal audit policies, organizes joint audit projects, and coordinates with the Government Accountability Office (GAO), Office of Management and Budget (OMB), and other Federal organizations on matters affecting audit policy. The scope of activities of the FAEC also includes issuing guidance on the external peer review process and coordinating joint audit projects.

FAEC membership is voluntary but generally consists of the Assistant Inspectors General for Auditing, or equivalent, from all Federal agencies with an Inspector General; the Director of the Defense Contract Audit Agency; and the Auditors General of the military services. Currently there are about 124 members from 65 agencies who represent about 10,000 auditors in the Federal Government. Mary Ugone, Deputy Inspector General of the Department of Defense, is the current chair of the FAEC and William Maharay, Deputy Inspector General for Audit, Department of Energy, is the current Vice-chair. Both are volunteers.

The FAEC currently operates with five standing committees: Audit Issues, Financial Statements, Information Technology, Human Resources, and Training. Each of these committees takes on significant projects that are of common concern and interest to the Federal audit community. Ms. Ugone proposed the formation of a new contracting committee at the August FAEC conference. The contracting committee would operate similar to the other FAEC standing committees and would focus on issues and concerns that are of common interest to the Federal audit community. Each FAEC committee is Chaired or Co-chaired by senior audit leaders within the FAEC and serves for a one year term. Committee chairs, co-chairs, and committee members are all volunteers from the FAEC community. A complete FAEC committee membership list can be found at the FAEC website: http://www.ignet.gov/pande/faec/faecdir061907.pdf

## Audit Issues Committee

The Audit Issues Committee is responsible for addressing any non-financial statement audit issue that comes before the FAEC related to audit, accounting, or internal control standards. Issues related to annual Federal financial statement audits are addressed by the FAEC Financial Statement Committee (described later), although the two committees coordinate their efforts. The FAEC Audit Issues Committee is also responsible for coordinating the scheduling of external peer reviews that are required by Government Auditing Standards.

The Audit Issues Committee is comprised of 12 members representing as many agencies, including two co-chairs. The current co-chairs of the Audit Issues Committee are Elliot Lewis, Assistant Inspector General for Auditing, Department of Labor, and Joseph Vengrin, Deputy Inspector General for Auditing, Department of Health and Human Services. A few examples of the significant efforts undertaken by the Audit Issues Committee follows.

In April 2005, the PCIE/ECIE Audit Committee issued a major revision to the peer review guide used by OIGs to conduct peer reviews required by Government Auditing Standards. The objective of these peer reviews is to determine whether the reviewed audit organization's internal quality control system is adequate and provides reasonable assurance that applicable auditing standards, policies, and procedures were met. The FAEC Audit Issues Committee assembled a team to revise the 2005 guide to address the 2007 revision of Government Auditing Standards. The team is currently planning to develop and conduct training on the peer review process before the next cycle of peer reviews (scheduled to begin in 2009).

The peer review schedule team was formed specifically to ensure that all PCIE agencies have peer reviews scheduled as required by Government Auditing Standards. The team coordinates with ECIE agencies and OIG investigative operations peer review plans to prevent any conflicts in schedules. The team will also address any implementation issues stemming from anticipated yellow book changes to the peer review requirements and make any recommendations, as appropriate, to the FAEC Audit Committee.

The Audit Issues Committee also has a team of members who are currently developing a standard audit guide that OIGs can use to audit Federal Employees' Compensation Act (FECA) operations within their agencies. FECA is the workers' compensation program that covers Federal employees. Although FECA is administered by the Department of Labor, employing agencies play a significant role in the process. This group was developed in response to requests from several FAEC agencies.

## Financial Statements Committee

The Financial Statements Committee is co-chaired by Deborah Cureton, Assistant Inspector General for Auditing, National Science Foundation, and Joel Grover, Deputy Assistant Inspector General for Audit, Department of the Treasury. The Financial Statements Committee is focused on matters related to auditing financial statements issued by Federal Agencies. Much of the group's recent and ongoing efforts relate to financial statement audit guidance.

The Financial Statements Committee has been working with the Financial Statement Audit Network (FSAN) to address issues affecting the annual financial statement audits, including issues on the interpretation and application of audit standards and requirements, and working relationships with CPA contractors, GAO and agency CFO offices. The FSAN is a subcommittee of the FAEC Financial Statement Committee and provides the federal financial statement audit community with a forum to identify, discuss, and resolve key issue concerning the preparation and audit of federal financial statements. The FSAN is comprised of representatives form a wide spectrum of the federal financial audit community, including the smaller Offices of Inspector General, the GAO, the Federal Accounting Standards Advisory Board, and the OMB. The Network currently has more than 120 members and is led by Greg Spencer, Director, Financial Audit Team, Department of Education.

The FSAN is in the process of working with the GAO to update the GAO/PCIE Financial Audit Manual (FAM). The FAM provides guidance for performing financial statement audits of federal entities and is a key tool for enhancing accountability over taxpayer-provided

resources. The GAO and PCIE are committed to keeping the FAM current. This project has been ongoing since late spring of last year and is expected to be completed by the end of this year. Specifically, this project involves updating the FAM for changes that have been made since 2001 to the professional and government audit standards. The FAM Working Group updated these sections for consistency with new auditing standards issued by the AICPA and guidance issued by OMB.

Earlier this year, FSAN began working with OMB to revise OMB Bulletin 06-03, "Audit Requirements for Federal Financial Statements". This effort continues and the revised bulletin is expected to be issued by the end of July 2007. OMB Bulletin 06-03 establishes minimum requirements for audits of Federal financial statements and implements the audit provisions of the Chief Financial Officers Act of 1990. The provisions of this bulletin apply to audits of financial statements of executive departments, agencies, and government corporations.

## Information Technology Committee

The Federal government is the world's largest procurer of Information Technology (IT) services and products, and faces significant challenges in managing its IT portfolio, including information security and privacy. The IG community plays a key role in helping the government meet management challenges related to IT. The IT Committee is an innovative group that provides a forum to share information and coordinate IT projects across the IG community and related stakeholders.

Members of the IT Committee previously served on the prior IT Security Committee for the FAEC, which initiated efforts to establish a more unified oversight response for the Federal Information Security Management Act of 2002 (FISMA). In addition to their IT audit responsibilities within their respective Federal agencies, IG representatives on the IT Committee currently provide a wide range of support for the IG community by leading efforts to address audit considerations for specific IT risk areas that impact Federal agencies, facilitating collaboration within the IG community through outreach and information sharing that focus on specific IT audit responsibilities, and consolidating comments on key IT legislation and guidance affecting the IG community. The Co-chairs of the FAEC IT Committee are also members of the PCIE IT Committee. Their participation facilitates coordination and promotes efficiency in the IG community's efforts to address cross-cutting IT issues.

Since the summer of 2006, the IT Committee has completed two major government-wide projects that address high-risk IT areas including: (1) a framework to guide Inspectors General annual independent evaluations required under FISMA, and (2) a review guide and data collection instrument to quickly assess government-wide efforts to protect sensitive information, in accordance with OMB Memorandum M-06-16, "Protection of Sensitive Agency Information." The IT Committee draws expertise from a cadre of individuals across the IG community and is lead by co-chairs Andrew Patchan, Assistant Inspector General for Audits at the General Services Administration and Gale Stone, Deputy Assistant Inspector General for Audits at the Social Security Administration. The IT Committee initiates audit projects through the overarching PCIE and FAEC leadership structures, and the co-chairs ensure close coordination with key stakeholders, including the OMB, GAO, the National Institute of Standards and Technology (NIST), and the Information Security Privacy and Advisory Board (ISPAB).

On September 19, 2006, the PCIE issued a FISMA framework, developed by the IT Committee which was designed to enhance the consistency, comparability, and completeness of annual information security evaluations provided by IGs under the provisions of FISMA. Recognizing the diverse technical and audit resource capabilities across the IG community, the FISMA framework is designed to assist the IG community in determining the status of their respective agencies information security programs through a risk based approach that does not mandate specific methodologies to be followed with the annual security evaluations. The FISMA framework was developed with input from the entire Federal IG community and through consultation with NIST, OMB, GAO, and the ISPAB. The IT Committee fully recognizes the dynamic environment we all face with IT security and continues to monitor

evolving legislative and policy requirements under FISMA. The IT Committee also stands ready to make necessary changes, as needed, to ensure that the FISMA framework adequately reflects changing requirements and captures the basic information and instructions necessary to support the IG community in meeting annual FISMA reporting responsibilities.

Last fall the IT Committee responded to a special OMB request for Federal Agencies to heighten their focus on IT controls for protecting sensitive information, including Personally Identifiable Information (PII) and the need to better protect privacy data entrusted to Federal Agencies. In July 2006, to streamline data gathering and reporting, the IT Committee developed a review guide and data collection instrument for IGs to assess agency efforts to protect sensitive information as required by OMB Memorandum M-06-16, Protection of Sensitive Agency Information. This fast-paced, highly collaborative, and extremely productive effort included a government-wide question and answer session and a review methodology for PII controls and enabled Offices of Inspectors General to complete over 50 agency reviews during the period of August 7 to September 22, 2006. The targeted assessments produced valuable status information required by OMB and supported Federal efforts to strengthen controls for sensitive PII data, which is associated with the growing threat of identity theft.

The rapidly changing IT environment for Federal Agencies underscores the importance of maintaining a focal point for audit leadership to help unify the IG community on management issues related to IT audits and external requests for IT audits that cover all Federal agencies. Early accomplishments for the IT Committee clearly reflect the overall success achieved by this well-qualified and highly flexible IT audit-oriented team and bode well for the shared leadership approach demonstrated by the co-chairs. The IT Committee is engaging in activities and working with the IG community to promote best practices in IT auditing and to address risks with security, privacy, e-government, and capital planning and investment management controls. As such, the IT Committee will continue to serve an ever-important function for the IG community by fostering collaboration and IG independence by enabling prompt, consolidated responses to Congressional and OMB inquires regarding all types of risks for Federal IT assets. More consistent and effective audit approaches on such issues will result in value-added audit products and services and IG recommendations that address recognized IT weaknesses and priorities.

## Human Resources Committee

The Human Resources (HR) Committee, co-chaired by Melissa Heist, Assistant Inspector General for Audit, Environmental Protection Agency, and Karen Scott, Senior Audit Manager, National Science Foundations, consists of 6 other members from 5 different agencies. The HR Committee is focused on identifying and addressing human resource issues affecting the Federal audit community. Last year, the HR Committee devoted much of their efforts in surveying members. The purpose of the survey was to identify human capital management challenges within the Federal audit community, identify actions taken or planned to address each of those challenges, and to identify areas of human capital management where assistance is needed. The committee analyzed the survey results and identified three top human resource priorities in the Federal audit community: core competencies, recruiting, and training and development.

In an effort to facilitate learning and development, in February 2007, the HR Committee announced a call for human resource "best practices." As a result, best practices in the following HR areas were submitted by four different agencies:

- leadership development and training programs
- recruitment and retention, including accelerated promotion policies, streamlined hiring processes, and performance measures for human resource activities
- core competencies systems, including position descriptions that include all core competencies
- promotion requirements
- 360 degree feedback assessments

Additional information about FAEC best practices can soon be found at the IGnet business website. The HR Committee plans to continue to identify and share best practices with the FAEC community in order to enhance the skills and knowledge within the OIG community.

## Training Committee

The Training Committee was established in January 2005. With participants from 13 different Federal audit organizations, the focus/mission initially was to assist the PCIE/ECIE Audit Committee in achieving its strategic goal to identify and provide useful, relevant, and cost-effective training at IGATI for auditors working in the various IG offices. To that end, the committee set out to review each IGATI course at least once every 3 years. Collectively the group carried out that commitment by establishing a standard methodology, report format, and matrix of courses to be reviewed by fiscal year. In all the committee reviewed 17 courses between the time they were established and the dissolution of IGATI in fiscal year 2007. The Committee's accomplishments were collectively recognized by the community in 2006 with a PCIE Award for Excellence.

Marla Freedman, Assistant Inspector General for Audit, Department of the Treasury and current committee chair, indicated that the committee is currently undergoing a bit of a transformation. In short, it is moving itself away from a course "review" function to one of a training "resource" function. Looking forward, the committee plans to provide an exchange where organizations can team-up to provide auditor training, share best practices for acquiring training from commercial sources (establishing a repository for statements of work), and provide an environment to share information on training/seminar providers.

# PCIE/ECIE & FAEC Committee Structure

## 7 PCIE/ECIE Committees:

- Human Resources
- Information Technology
- Inspections & Evaluation
- Integrity
- Investigations
- Legislation
- Audit

## Federal Audit Executive Council

(Subgroup of the PCIE Audit Committee)

- Audit Issues
- Financial Statements
- Information Technology
- Human Resources
- Training
- Contracting (Proposed)

**This article was authored by the FAEC Chair Mary Ugone and Committee Chairs.**

*A special thanks to John Koch, Executive Assistant, Auditing, DoD IG for his contributions to the article.*

# Information Technology

by Thomas F. Gimble

Speech at the PCIE/ECIE Annual Conference
April 16, 2007

8

and the

# Establishment of the PCIE IT Committee

Good afternoon. My goal today is to get us all thinking about the importance of information technology in the Inspector General community and discuss some of the issues we are facing today. Information technologies have revolutionized the way we conduct business. There are countless benefits that enhance and facilitate the audits, evaluations, and investigations conducted by IGs. However, these benefits are often accompanied by serious security risks and challenges.

How many of our organizations have lost personally identifiable information? How many are experiencing security issues? How many are concerned about IT acquisition? These are topics that affect us all and we need to work as a community to share ideas and best practices.

What I would like to focus on is exploring the role of the IG community with respect to information technology issues within the Federal government such as:

- Personally Identifiable Information;
- Unclassified data loss;
- The Federal Information Security Management Act;
- IT acquisition; and
- Forensics IT issues

As you all know, the subject of protection of personal information remains a very big concern within the information technology community and across the entire Federal government. The Office of Management and Budget has been requiring annual reports from Federal managers for several years regarding implementation of the requirements of the Privacy Act of 1974 and the E Government Act of 2002 as they pertain to privacy. The IG community has been offered the chance to comment as well, but is not required to do so. This situation is constantly changing as the OMB reaches out more and more to us for assistance in assessing the status of privacy protections across the government.

On January 11th, Karen Evans, OMB Administrator for E-Government and Information Technology, issued OMB memorandum, "Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials," to the Chief Information Officers. That memorandum indicated that the PCIE would be asked to review agency processes and help ensure they were consistent with Homeland Security Presidential Directive 12 and Federal Information Processing Standard 201 regarding credentials. Previously, Ms. Evans had asked the PCIE for assistance in verifying that policies were in place regarding privacy impact assessments required by the E-Government Act and also those regarding incident response reporting. It is expected that a major new requirement will be issued shortly to all Executive departments and agencies by OMB, adding numerous additional safeguards for the protection of personal information in addition to those previously mandated by the Congress and the OMB.

Further, it is expected that the OMB will request the PCIE to assist in verifying agency compliance with the new safeguards, such as those mandating encryption. We need to be prepared to respond to these and future requests.

Besides the loss of PII, the compromise of unclassified systems and the data contained in them also pose a security challenge for our community.

Today's news is filled with reports of data loss by the Government and corporations alike. The causes vary from hackers breaking into corporate networks, to Government employees losing hard drives, to thieves stealing laptops from cars and homes. The losses become public when the data owners make mandatory disclosures to downstream victims of potential identity theft. What happens, however, when an organization falls victim to data theft that does not involve personal, Privacy Act, or financial data? What happens when the data belong to the Federal Government and reside on a contractor system?

Are contractors required to report cyber security incidents involving systems that carry sensitive unclassified Federal Government data? In the case of the Defense Department, This data, while unclassified, could relate to weapons systems, military operations, or technology used or planned for military use. Finding the answer to this question has become a policy dilemma.

Within the DoD, when a contractor's computer network is compromised, resulting in the potential loss of sensitive but unclassified information, there is no requirement for the incident to be reported to law enforcement or DoD officials. The lack of reporting requirements and enforcement mechanisms presents a national security vulnerability. As a result, the exact size of this vulnerability is unclear. The exposure of defense information to unauthorized personnel cannot be evaluated when unreported, thus preventing a reliable impact assessment. A mechanism is needed to insure the reporting of data loss by DoD contractors.


*PCIE IT Committee Website*

I briefly want to touch on another important topic to the IG community regarding information technology, which is the Federal Information Security Management Act.

The PCIE Community has been providing annual assessments to OMB and the Congress, as required by the FISMA and its predecessor, the Government Information Security Reform Act, for many years. There have been annual congressional hearings on the consolidated OMB report of management and IG assessments, and both OMB and Congress have issued scorecards to grade the results of the assessments. How much has the security of our government's information improved from this activity? Are the reports the OIG Community is providing telling the whole story regarding IT security? I have met with Karen Evans to discuss FISMA and the OIG role.

The Government Accountability Office has been asked by Congress to do a review of the impediments to effective implementation of FISMA requirements and should be issuing a report of the results of its effort shortly.

We should have dialog with OMB about what questions to ask the IG community each year to elicit real and timely information regarding the security posture of our agencies.

For example, the DoD does not have an accurate inventory of its IT systems. Reporting, as a percentage, the number of systems with current certifications and accreditations on an incomplete inventory does not tell the entire IT security story.

There's another set of issues I'd like to mention – and they involve IT acquisition, Exhibit 300s, and other IT expenditure reporting.

The Exhibit 300 is used, in conjunction with the annual budget submissions, to collect agency information required by the Federal Acquisition Streamlining Act and the Clinger-Cohen Act to ensure the business case for investments are made and tied to the mission statements, long term goals and objectives, and annual performance plans. Essentially these exhibits are top level capital asset plans and business cases for major IT investments, as well as items of particular interest to OMB and therefore on the OMB "Watch List", such as the Navy-Marine Corps Intranet.

However, the number of Exhibit 300s has declined noticeably over the years, at the same time that the number of systems and the size of the IT budgets have increased dramatically. I would have to agree with the GAO that review of the Exhibit 300s does not give an accurate picture of Federal IT expenditures.
The PCIE recently collected information regarding the OMB Exhibit 300s from the PCIE community at the request of OMB. This request stemmed from questions

raised by the GAO regarding the accuracy and reliability of the Exhibit 300s.

We have a very serious problem answering questions pertaining to IT expenditures, for example in DoD, because of the lack of an accurate IT inventory and inconsistency of reporting across our very large department. Estimates of actual DoD expenditures for IT range from the "official" estimate of around $35 billion annually to in excess of $160 billion annually. I suspect DoD is not the only department with difficulty pinning down an accurate number.

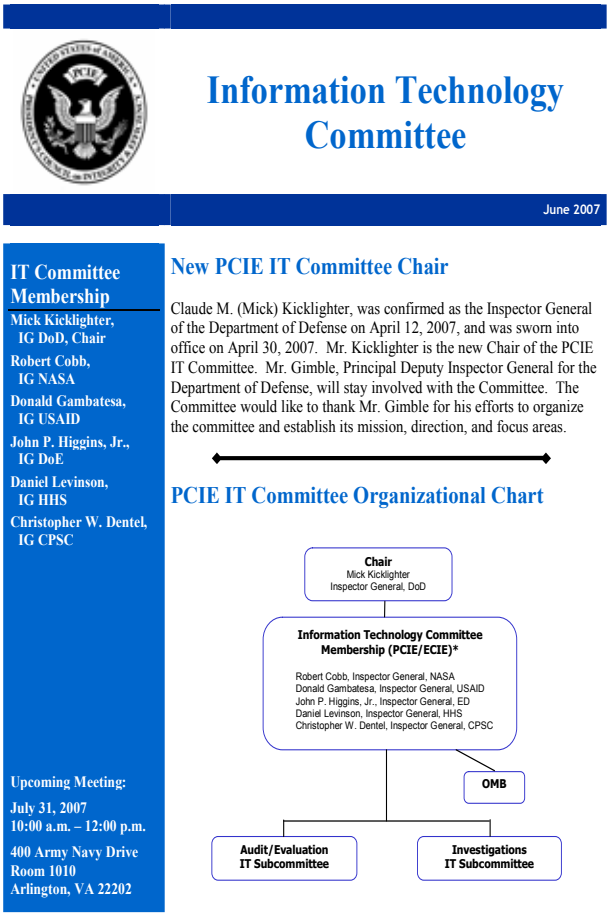
Getting back to the Exhibit 300s and other IT expenditure reporting. A case can be made that there should be a correlation between what agencies are reporting as FISMA inventories and as IT investment inventories. Currently, this cannot be done in DoD and possibly not in other agencies either. As Inspectors General, how can we help our departments devise ways to obtain more accurate information on the annual expenditure of the Federal Government for IT goods and services? How can we tie financial statement auditing into the equation? What sort of oversight questions would yield truly informative data which might also be subject to IG assessment? This type of inquiry needs to be undertaken if we are to contribute to the quality of the discussion on IT expenditures.

Another IT issue that is a hot topic within the law enforcement community is the frequent changes in digital technology, which pose complex challenges and require continual improvements in forensic process methodology.

Our investigators need access to the latest forensic software in order to keep up with the fast pace of changing technology. The recent release of Microsoft Vista continues to challenge the digital forensic community which is scrambling to push tools and training out to the field in preparation for encounters with this new operating system.

IT training for incident responders and computer crime investigators is an ongoing process. While not many certification programs exist for computer forensic examiners—DoD has one by the way—these programs should be supported and encouraged. Collaboration among these investigators across agencies occurs on a daily basis and they need a common ground from which to operate forensics IT systems. The IG community could potentially benefit from a centralization of certification authorities and other related topics.

The link between high tech crime investigations and the information assurance community is vital. We continue to investigate instances of computer intrusions, unauthorized access, and data theft—involving both Government data and personal information. Education is key—both for information technology personnel and end users—in protecting their data and information systems. Instances of keyloggers and other malicious software continue to challenge our investigators who are working related cases involving our pay system, e-mail communications, and defense contractor networks. It's vital that computer breaches get reported to law enforcement in a timely manner—whether the victim



Information Technology Committee

June 2007

IT Committee Membership

Mick Kicklighter, IG DoD, Chair
Robert Cobb, IG NASA
Donald Gambatesa, IG USAID
John P. Higgins, Jr., IG DoE
Daniel Levinson, IG HHS
Christopher W. Dentel, IG CPSC

Upcoming Meeting:
July 31, 2007
10:00 a.m. – 12:00 p.m.
400 Army Navy Drive
Room 1010
Arlington, VA 22202

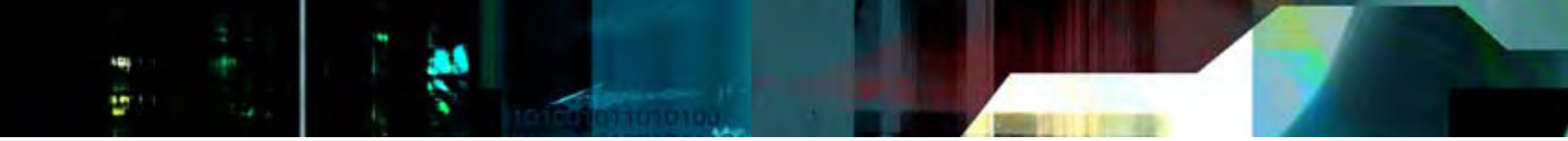
New PCIE IT Committee Chair

Claude M. (Mick) Kicklighter, was confirmed as the Inspector General of the Department of Defense on April 12, 2007, and was sworn into office on April 30, 2007. Mr. Kicklighter is the new Chair of the PCIE IT Committee. Mr. Gimble, Principal Deputy Inspector General for the Department of Defense, will stay involved with the Committee. The Committee would like to thank Mr. Gimble for his efforts to organize the committee and establish its mission, direction, and focus areas.

PCIE IT Committee Organizational Chart



*PCIE IT Committee Newsletter*



is a Government organization or a contractor housing Government data on its victimized network.

As technology leaps forward with innovative ways to share and store increasingly large amounts of data, the challenges to protect PII and Government data and investigate its loss or theft will continue to grow. I challenge you to be vigilant over your organization's acquisition processes—to insure that newly procured technologies offer robust security and that new contracts include provisions for reporting cyber crime and data loss.

We must broaden our view beyond our own IT issues by educating ourselves and our people about the issues I've mentioned here this afternoon. And then, we have to act.

To address these many concerns we share regarding information technology, the PCIE IT Committee has been established.

The President's Council on Integrity and Efficiency's Information Technology Committee mission is to facilitate effective information technology audits, evaluations, and investigations by Inspectors General, and to provide a vehicle for the expression of the IG community's perspective on Government-wide IT operations.

Our operating principles have been established to:

• Promote participation by Office of Inspector General community members in IT Committee activities.

• Encourage communication and cooperation with colleagues in the IT field (including the Federal Chief Information Officers and staff, security professionals, members of the Executive Council on Integrity and Efficiency).

• Promote effective teamwork in addressing Government-wide initiatives, improving OIG IT activities, and safeguarding national IT assets and infrastructure.

The IT Committee will be supported by the IT Community Forum Subcommittee and the Specific Area Subcommittees. The committee will meet at least quarterly. The forum and subcommittees will meet as necessary.

The OMB is also participating in the IT Committee on an advisory level, aimed at sharing OMB IT concerns with the IG Community.

The IT Community Forum Subcommittee will be made up of representatives from the Investigations, Audit, and Inspections and Evaluations communities. Our goal is to have at least two IT subject matter experts from each of the communities. Their purpose will be to Chair the specific area subcommittees and report the IG membership on their actions and proposed next steps. The IT Community Forum Subcommittee will meet as needed.

The IT Committee is focusing our initial efforts on three IT areas:

1. Personally Identifiable Information or PII;

2. Federal Acquisition Security Management or FISMA; and

3. IT Acquisition to include Exhibit 300s and Earned Value Management Systems

Specific area subcommittees have been established for each of these areas; subcommittees can be added or disbanded as appropriate.

The specific area subcommittees will be composed of representatives from each of the IG communities (investigations, audit, and inspections and evaluations). The membership of the specific area subcommittees will carry out the actions brought down from the IT Community Forum Subcommittee. Participation in the issue specific committees is not limited to the IG community; inclusion of any interested party is encouraged. I encourage you to share your IT expertise and participate in the IT Committee.

I hope the effects of the IT Committee on the IG community will be: In the short term, improved communication and knowledge sharing among our colleagues, identification of the problems we are facing, and the discussion of the effects of the problems on our organizations. In the long term, we will be able to advance our information technology issues by implementing solutions collectively to benefit our community as a whole.

Maybe if we can get our organizations and leaders working together to share our thoughts and ideas about information technology solutions we can start looking towards a more secure future. Thank you and I look forward to working with you.

## Thomas F. Gimble, Department of Defense

### Principal Deputy Inspector General

Mr. Gimble resumed his duties as the Principal Deputy Inspector General on April 30, 2007, after serving since September 10, 2005, as Acting Inspector General. As Principal Deputy Inspector General, Mr. Gimble reports directly to DoD Inspector General Claude M. Kicklighter.

Prior to his initial appointment as Principal Deputy Inspector General in September 2005, Mr. Gimble was the Deputy Inspector General for Intelligence and served as the principal advisor to the Inspector General on matters relating to DoD-wide intelligence programs and operations.

Mr. Gimble has also held other senior positions within the DoD Office of Inspector General. He served as the Acting Deputy Assistant Inspector General for Auditing and was responsible for directing audits regarding logistics, financial management, contracts, readiness, intelligence, information technology, military construction, housing programs, morale, welfare, recreation, and environmental policies. Additionally, Mr. Gimble served as Director of the Acquisition Management Directorate, and as Director of the Readiness and Operational Support Directorate.

Mr. Gimble began his Federal civilian career with the Air Force Audit Agency at Kelly Air Force Base, Texas, and then joined the Defense Audit Service in 1976. Mr. Gimble served with the U.S. Army as an infantry soldier in Vietnam, where he awarded the Bronze Star, the Purple Heart, and the Combat Infantry Badge. He later attended Lamar University where he received a BBA, and the University of Texas at San Antonio, where he received an MBA. He is a Certified Public Accountant and Certified Government Financial Manager.

In 2006, Mr. Gimble received the Alexander Hamilton Award, which is the highest honor bestowed by the President's Council on Integrity and Efficiency, awarded for outstanding achievement in improving the integrity, efficiency or effectiveness of Executive Branch agency operations. He also received the Presidential Rank Award for Distinguished Executive in 2006. In addition, he is a recipient of the Secretary of Defense Medal for Exceptional Civilian Service.

# Congressional Hearing

by Clay Johnson III

9

Testimony given before the Subcommittee on Government Management, Organization, and Procurement of the House Committee on Oversight and Government Reform June 20, 2007

# Inspectors General Independence and Integrity

*Statement of the Honorable Clay Johnson III Deputy Director for Management Office of Management and Budget before the Committee on Homeland Security and Government Reform of the United States Senate July 11, 2007.*

Thank you, Mr. Chairman, Ranking Member Collins, and members of the Committee for allowing me to testify today. Per Executive Order 12805, as Deputy Director for Management at OMB, I am the Chairman of the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE), the two Inspector General councils.

I believe the general quality and quantity of IG work today is superb, and that IGs are currently held accountable for the quality and quantity of their work, as they should be.

In their most recent report to the President, the PCIE and ECIE report that their work has resulted in:

$9.9 BILLION IN POTENTIAL SAVINGS FROM AUDIT RECOMMENDATIONS;

$6.8 BILLION IN INVESTIGATIVE RECOVERIES;

6,500 INDICTMENTS AND CRIMINAL INFORMATIONS;

8,400 SUCCESSFUL PROSECUTIONS;

7,300 SUSPENSIONS OR DEBARMENTS; AND

4,200 PERSONNEL ACTIONS.

These performance levels are consistent with previous years' efforts: IGs have been and continue to be a primary means by which we identify and eliminate waste, fraud, and abuse.

I believe IGs and Agency leadership currently share the goal of making their agencies successful, as they should. Both want to eliminate waste, fraud and abuse. Both want to identify and fix processes and programs that don't work.

I believe IGs are not and should not be treated by agency leadership as the enemy. Like internal auditors in the private sector, IGs are expected to report on and provide recommendations for improvement in those areas where opportunities or deficiencies are identified. They are agents of positive change. IGs are generally respected, not feared, by agency leadership.

I believe IG-agency relationships need to be actively managed to be as independent but still as functional and constructive as they should or could be. I believe the attached Relationship Principles, developed by the IG community and me three years ago, should be used by IGs and agency heads to manage their relationship with each other.

## Working Relationship Principles for Agencies and Offices of Inspectors General

The Inspector General (IG) Act establishes for most agencies an Office of Inspector General (OIG) and sets out its mission, responsibilities, and authority. The IG is under the general supervision of the agency head. The unique nature of the IG function can present a number of challenges for establishing and maintaining effective working relationships. The following working relationship principles provide some guidance for agencies and OIGs.
To work most effectively together, the Agency and its OIG need to clearly define what the two consider to be a productive relationship and then consciously manage toward that goal in an atmosphere of mutual respect.

By providing objective information to promote government management, decision-making, and accountability, the OIG contributes to the Agency's success. The OIG is an agent of positive change, focusing on eliminating waste, fraud and abuse, and on identifying problems and recommendations for corrective actions by agency leadership. The OIG provides the agency and Congress with objective assessments of opportunities to be more successful.

The OIG, although not under the direct supervision of senior agency management, must keep them and the Congress fully and currently informed of significant OIG activities. Given the complexity of management and policy issues, the OIG and the Agency may sometimes disagree on the extent of a problem and the need for and scope of corrective action. However, such disagreements should not cause the relationship between the OIG and the Agency to become unproductive.

To work together most effectively, the OIG and the Agency should strive to:

**Foster open communications at all levels.** The Agency will promptly respond to OIG requests for information to facilitate OIG activities and acknowledge challenges that the OIG can help address. Surprises are to be avoided. With very limited exceptions primarily related to investigations, the OIG should keep the Agency advised of its work and its findings on a timely basis, and strive to provide information helpful to the Agency at the earliest possible stage.

**Interact with professionalism and mutual respect.** Each party should always act in good faith and presume the same from the other. Both parties share as a common goal the successful accomplishment of the Agency's mission.

**Recognize and respect the mission and priorities of the Agency and the OIG.** The Agency should recognize the OIG's independent role in carrying out its mission within the Agency, while recognizing the responsibility of the OIG to report both to the Congress and to the Agency Head. The OIG should work to carry out its functions with a minimum of disruption to the primary work of the Agency.

**Be thorough, objective and fair.** The OIG must perform its work thoroughly, objectively and with consideration to the Agency's point of view. When responding, the Agency will objectively consider differing opinions and means of improving operations. Both sides will recognize successes in addressing management challenges.

**Be engaged**. The OIG and Agency management will work cooperatively in identifying the most important areas for OIG work, as well as the best means of addressing the results of that work, while maintaining the OIG's statutory independence of operation. In addition, agencies need to recognize that the OIG also will need to carry out work that is self-initiated, congressionally requested, or mandated by law.

**Be knowledgeable**. The OIG will continually strive to keep abreast of agency programs and operations, and Agency management will be kept informed of OIG activities and concerns being raised in the course of OIG work. Agencies will help ensure that the OIG is kept up to date on current matters and events.

**Provide feedback**. The Agency and the OIG should implement mechanisms, both formal and informal, to ensure prompt and regular feedback.

## Clay Johnson III, Office of Management and Budget

### Deputy Director for Management

The Deputy Director for Management provides government-wide leadership to Executive Branch agencies to improve agency and program performance.

Prior to this he was the Assistant to the President for Presidential Personnel, responsible for the organization that identifies and recruits approximately 4000 senior officials, middle management personnel and part-time board and commission members. From 1995 to 2000, Mr. Johnson worked with Governor George W. Bush in Austin, first as his Appointments Director, then as his Chief of Staff, and then as the Executive Director of the Bush-Cheney Transition.

Mr. Johnson has been the Chief Operating Officer for the Dallas Museum of Art and the President of the Horchow and Neiman Marcus Mail Order companies. He also has worked for Citicorp, Wilson Sporting Goods and Frito Lay.

He received his undergraduate degree from Yale University and a Masters degree from MIT's Sloan School of Management. In Austin, he helped create the Texas State History Museum, and was also an Adjunct Professor at the University of Texas Graduate School of Business.

In Dallas, he served as President of the Board of Trustees for St. Marks School of Texas, and as a Board Member of Equitable Bankshares, Goodwill Industries of Dallas, and the Dallas Chapter of the Young Presidents Organization.

# Congressional Hearing

by Jeffrey C. Steinhoff

Testimony given before the Subcommittee on Government Management, Organization, and Procurement of the House Committee on Oversight and Government Reform June, 20, 2007

10

# Inspectors General

# Independence and Integrity

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss current legislative proposals intended to enhance the independence and operations of the inspectors general (IG) offices. The IG offices play a key role in federal agency oversight. They were created to prevent and detect fraud, waste, abuse, and mismanagement in agencies' programs and operations; conduct and supervise audits and investigations; and recommend policies to promote economy, efficiency, and effectiveness. In the past almost 3 decades since passage of the landmark IG Act of 1978, the IGs have played a very important role in enhancing government accountability and protecting the government against fraud, waste, abuse, and mismanagement.

The IG Act recognized IG independence as one of the most important elements of the overall effectiveness of the IG function. In fact, much of the IG Act, as amended (IG Act), provides specific protections to IG independence that are unprecedented for an audit and investigative function located within the organization being reviewed. These protections were necessary due in large part to the unusual reporting requirements of the IGs who are both subject to the general supervision and budget processes of the agencies they audit while at the same time being expected to provide independent reports of their work externally to the Congress. Many of the provisions in the Improving Government Accountability Act, H.R. 928, seek to further strengthen the independence of the IGs to help ensure their ability to effectively carry out their dual internal and external reporting roles.

Today, I will discuss (1) the key principles of auditor independence, (2) the proposals in H.R. 928 regarding IG independence and operations and the establishment of a statutory council of IGs, and (3) additional matters concerning IG independence and the coordination of federal oversight from GAO's recent IG work.

My testimony today draws on provisions of the IG Act, professional auditing standards, prior GAO reports, and information reported by the IGs. In May 2006, the Comptroller General hosted a panel discussion on many of the issues to be discussed today. I will draw upon information gained from the panel to address several issues in H.R. 928.

## Auditor Independence:

Key to a consideration of H.R. 928 are the principles of auditor independence and how they apply in the IG community. Independence is the cornerstone of professional auditing. Without independence, an organization cannot do independent audits. Lacking this critical attribute, an organization's work might be classified as studies, research reports, consulting reports, or reviews, but not independent audits. Government Auditing Standards state, "In all matters relating to the audit work, the audit organization and the individual auditor, whether government or public, must be free from personal, external, and organizational impairments to independence, and must avoid the appearance of such impairments to independence. Auditors and audit organizations must maintain independence so that their opinions, findings, conclusions, judgments, and recommendations will be impartial and viewed as impartial by objective third parties with knowledge of the relevant information."

- Personal independence applies to individual auditors at all levels of the audit organization, including the head of the organization. Personal independence refers to the auditor's ability to remain objective and maintain an independent attitude in all matters relating to the audit, as well as the auditor's ability to be recognized by others as independent. The auditor needs an independent and objective state of mind that does not allow personal bias or the undue influence of others to override the auditor's professional judgments. This attitude is also referred to as intellectual honesty. The auditor must also be free from direct financial or managerial involvement with the audited entity or other potential conflicts of interest that might create the perception that the auditor is not independent.

- External independence refers to both the auditor's and the audit organization's freedom to make independent and objective judgments free from external influences or pressures. Examples of impairments to external independence include restrictions on access to records, government officials, or other individuals needed to conduct the audit; external interference over

the assignment, appointment, compensation, or promotion of audit personnel; restrictions on funds or other resources provided to the audit organization that adversely affect the audit organization's ability to carry out its responsibilities; or external authority to overrule or to inappropriately influence the auditors' judgment as to appropriate reporting content.

• Organizational independence refers to the audit organization's placement in relation to the activities being audited. Professional auditing standards have different criteria for organizational independence for external and internal audit organizations. The IGs, in their statutory role of providing oversight of their agencies' operations, represent a unique hybrid of external and internal reporting responsibilities.

External audit organizations are organizationally independent under professional auditing standards when they are organizationally placed outside of the entity under audit. In government, this is achieved when the audit organization is in a different level of government (for example, federal auditors auditing a state government program) or different branch of government within the same level of government (for example, legislative auditors, such as GAO, auditing an executive branch program). External auditors also report externally, meaning that their audit reports are disseminated to and used by third parties.

Internal audit organizations are defined as being organizationally independent under professional auditing standards if the head of the audit organization (1) is accountable to the head or deputy head of the government entity or to those charged with governance, (2) reports the audit results both to the head or deputy head of the government entity and to those charged with governance, (3) is located organizationally outside the staff or line-management function of the unit under audit, (4) has access to those charged with governance, and (5) is sufficiently removed from political pressures to conduct audits and report findings, opinions, and conclusions objectively without fear of political reprisal. Under internal auditing standards, internal auditors are generally limited to reporting internally to the organization that they audit, except when certain conditions are met.

The IG offices, having been created to perform a unique role in overseeing federal agency operations, have characteristics of both external audit organizations and internal audit organizations. For example, the IGs have external reporting requirements consistent with the reporting requirements for external auditors while at the same time being part of their respective agencies. IGs also have a dual reporting responsibility to the Congress and the agency head. The IG Act also contains many unique provisions to provide for independence under this model.

Under the IG Act, the IGs (1) may perform any audit or investigation without interference from the agency head and others except under specific conditions, (2) report to and receive general supervision only from the heads or deputy heads of their agencies and no other agency officials, and (3) have direct and immediate access to their agency heads. The IGs' external reporting requirements in the IG Act include reporting the results of their work in semiannual reports to the Congress. Under the IG Act, the IGs are to report their findings without alteration by their respective agencies, and these reports are to be made available to the general public.

The IG Act also directs the IGs to keep the agency head and the Congress fully and currently informed by these semiannual reports, and otherwise, of any fraud and other serious problems, abuses, and deficiencies relating to the administration of programs and operations administered or financed by their agencies. Also, the IGs are required to report particularly serious or flagrant problems, abuses, or deficiencies immediately to their agency heads, who are required to transmit the IG's report to the Congress within 7 calendar days. Finally, depending on the IG's appointment process, either the President or the agency head must provide the Congress notification as to the reasons for the removal of any IG.

A key provision in the IG Act regarding IG independence is for certain IGs to be appointed by the President with the advice and consent of the Senate. This appointment is required to be without regard to political affiliation and is to be based solely on an assessment of a candidate's integrity and demonstrated ability. These presidentially appointed IGs can

only be removed from office by the President, who must communicate the reasons for removal to both houses of the Congress. Government auditing standards recognize this external appointment/removal of the IG as a key independence consideration for IGs as external audit organizations.

Organizational independence differs between the offices of presidentially appointed IGs and agency-appointed IGs. In 1988, the IG Act was amended to establish additional IG offices in designated federal entities (DFE) named in the legislation. Generally, these IGs have the same authorities and responsibilities as those IGs established by the original 1978 Act, but they have a clear distinction in their appointment--they are appointed and removed by their entity heads rather than by the President and are not subject to Senate confirmation. In addition, the DFE IGs do not have the requirement that their appointment is to be without regard to political affiliation and based solely on integrity and demonstrated ability. The DFE IGs, while they are covered by many of the same provisions of the IG Act as the IGs appointed by the President with Senate confirmation, are more closely aligned to independence standards for internal auditors rather than external auditors. At the same time, Government Auditing Standards recognize that additional statutory safeguards exist for DFE IG independence for reporting externally. These safeguards include establishment by statute, communication of the reasons for removal of the head of an audit organization to the cognizant legislative oversight body, statutory protections that prevent the audited entity from interfering with an audit, statutory requirements for the audit organization to report to a legislative body on a recurring basis, and statutory access to records and documents related to agency programs.

We believe that the differences in the appointment and removal processes between presidentially appointed IGs and those appointed by the agency head do result in a clear difference in the organizational independence structures of the IGs. Those offices with IGs appointed by the President are more closely aligned with the independence standards for external audit organizations, while those offices with IGs appointed by the agency head are more closely aligned with the independence standards for internal audit organizations. However, as I mentioned earlier, the IGs represent a unique hybrid of external auditing and internal auditing in their oversight roles for the federal agencies.

## Provisions of H.R. 928:

In May 2006, at the request of the Senate Committee on Homeland Security and Governmental Affairs, the Comptroller General convened a panel of recognized leaders of the federal audit and investigative community to discuss many of the same proposals that are in H.R. 928, Improving Government Accountability Act. We drew the panel from the current IG leadership, former IGs, knowledgeable former and current federal managers, representatives of academia and research institutions, a former member of the Congress, and congressional staff, including the congressional staff person closely involved in the development of the 1978 Act. Among other issues, the panel members discussed terms of office and removal for cause, submission of IG budgets, a proposed IG Council, and investigative and law enforcement authorities for agency-appointed IGs. The panel members did not discuss the proposal in H.R. 928 calling for establishing IG offices as separate agencies for purposes related to personnel matters. In September 2006 we issued the results of the panel discussion.

I would now like to highlight the overall perspectives of the panel in the context of H.R. 928.

## Terms of office and removal for cause:

Depending on the nature of their appointment, IGs serve at the pleasure of either the President or their agency head. The IGs appointed by the President with Senate confirmation may be removed only by the President, while the IGs appointed by their agency heads may be removed or transferred from their office only by the agency head. However, in both types of removal, the reasons must be communicated to the Congress after the action has taken place.

H.R. 928 includes a provision to specify a 7-year term of office for each IG with more than one term possible. In addition, the bill provides a removal-for-cause provision whereby an IG may be removed from office prior to the expiration of his or her term only on the basis of

permanent incapacity, inefficiency, neglect of duty, malfeasance, conviction of a felony, or conduct involving moral turpitude.

The majority of the panel participants did not favor statutorily establishing a fixed term of office for IGs. The reasons included the panelists' belief that the proposal could disrupt current agency/IG relationships and that agency flexibility is needed to remove a poor- performing IG if necessary. On the other hand, a statutory term of office and removal for specified causes was viewed positively by some panelists as a means of enhancing independence by relieving some of the immediate pressure surrounding removal. The panel members did generally support a statutory requirement to notify the Congress in writing in advance of removing an IG, with an explanation of the reason for removal. The participants cautioned that this procedure should consist only of notification, without building in additional steps or actions in the removal process.

## IG Budget:

The IG Act Amendments of 1988 require the President's budget to include a separate appropriation account for each of those IGs who are appointed by the President or otherwise specified by the act. In this context, IG budget requests are generally part of each agency's budget process and are submitted as a separate budget line item to the Office of Management and Budget (OMB) and the Congress as a part of each agency's overall budget. In contrast, most IGs appointed by their agency heads do not have a separate appropriation account.

H.R. 928 would give the IGs an opportunity to justify their funding requests directly to OMB and the Congress in addition to being a part of their agencies' budget processes. In those cases where the IGs make their budget requests directly to OMB and the Congress, H.R. 928 would also require a comparison of the budget requests submitted by the IGs to the funds requested by the agency heads for their IGs included in the Budget of the United States Government. The panel members had mixed views about whether IGs should submit their budget requests directly to OMB and the Congress. The panel believed that the current system of separate budget line items for the presidential IGs works well and that all IGs should have separate budget line items. This is an issue the Congress would need to consider in the context of the broader budget and appropriations process.

## IG Council:

In accordance with Executive Order No. 12805 issued in 1992, the IGs meet and coordinate as two groups. The IGs appointed by the President and confirmed by the Senate are members of the President's Council on Integrity and Efficiency (PCIE), and the IGs appointed by their agency heads are members of the Executive Council on Integrity and Efficiency (ECIE). Both the PCIE and ECIE are chaired by the OMB Deputy Director for Management.

H.R. 928 provides for a combined IG Council with duties and functions similar to the current PCIE and ECIE, including (1) identifying, reviewing, and discussing areas of weakness and vulnerability in federal programs and operations with respect to fraud, waste, and abuse; (2) developing plans for coordinated governmentwide activities that address these problems and promote economy and efficiency in federal programs and operations; and (3) developing policies and professional training to maintain a corps of well-trained and highly skilled IG personnel. The bill also provides for a separate appropriation account for the IG Council.

In a prior report we recommended establishing an IG Council in statute with a designated funding source. We believe that by providing a statutory basis for the council's roles and responsibilities, the permanence of the council could be established and the ability to take on more sensitive issues could be strengthened. In contrast, the participants in our May 2006 panel discussion had mixed views about statutorily establishing a joint IG Council but did favor establishing a funding mechanism.

H.R. 928 also provides for an Integrity Committee of the IG Council to review and investigate allegations of IG misconduct. The Integrity Committee's function would be similar to that of the current Integrity Committee of the PCIE and ECIE, which is charged with receiving, reviewing, and referring for investigation, where appropriate, allegations of wrongdoing against IGs and members of the IG's senior staff operating with the IG's

knowledge. Currently, the Integrity Committee receives its authority under Executive Order 12993, signed in 1996, and is chaired by a representative of the FBI. Other members of the committee are the Special Counsel of the Office of Special Counsel, the Director of the Office of Government Ethics, and three IGs representing the PCIE and the ECIE. Cases investigated by members of the Integrity Committee may be forwarded to the PCIE and ECIE Chairperson for further action.

We believe that H.R. 928 would provide the IG councils--formed currently through executive order--with needed statutory permanence, and we continue to support formalizing a combined council in statute, along with the Integrity Committee. We also strongly support the concept behind the Integrity Committee. We believe it is imperative that the independence of the Integrity Committee be preserved and view this legislation as being directed to ensure permanence of this important function and not to change the basic underpinnings.

## IG offices as separate agencies:

In order to better attract and retain highly qualified IG employees, H.R. 928 would provide the IGs with personnel authority separate and apart from that of their agencies. To accomplish this, the bill would consider each IG office to be a separate agency for purposes of implementing certain provisions in Title 5 of the United State Code dealing with employment, retention, separation, and retirement.

We have concerns about this proposal. First, we are concerned about the inherent inefficiencies in enforcing a splitting of administrative processes currently often being shared by agencies and their IGs. Secondly, in providing such authorities to the IGs, there could be a great disparity in how this would be implemented by each IG office. The IG community has suggested that, as an alternative, the IGs could seek legislative authorization to apply to the Office of Personnel Management (OPM) for certain personnel authorities. We believe that if implementation is properly coordinated through the PCIE and ECIE, the IGs' proposal represents a good alternative and would address the intent of H.R. 928.

H.R. 928 also covers all provisions in Title 5 relating to the Senior Executive Service including receiving pay increases and bonuses. Issues over IG pay and bonuses have arisen over the past few years due to recent requirements that rates of pay for the federal Senior Executive Service (SES) be based on performance evaluations as part of a certified performance management system. IGs who are subject to these requirements must therefore receive performance evaluations in order to qualify for an increase to their pay. The IGs are provided general supervision by their agency heads in accordance with the IG Act. However, independence issues arise if the agency head is evaluating IG performance when that evaluation is used as a basis for an increase in the IG's pay or for providing a bonus. As a result, some IGs have effectively had their pay capped without the ability to receive pay increases or bonuses.

The majority of panel participants believed that the pay structure for IGs needs to be addressed. The discussion emphasized the importance of providing comparable compensation for IGs as appropriate, while maintaining the IGs' independence in reporting the results of their work, and providing them with performance evaluations that could be used to justify higher pay. However, responses to IGs' receiving performance bonuses were mixed, mainly due to uncertainty about the overall framework that would be used to evaluate performance and make decisions about bonuses. We believe that an independent framework could be established through the PCIE and ECIE, in cooperation with OPM, to conduct performance evaluations of the IGs.

## IG investigative and law enforcement authorities:

The IG Act has been amended by subsequent legislation to provide IGs appointed by the President with law enforcement powers to make arrests, obtain and execute search warrants, and carry firearms. The IGs appointed by their agency heads were not included under this amendment but may obtain law enforcement authority by applying to the Attorney General for deputation on a case-by-case basis. In addition, the Program Fraud Civil Remedies Act of 1986 provides agencies with IGs appointed by the President with the authority to investigate and report false claims and recoup losses resulting from fraud below $150,000. The agencies with IGs appointed by their agency heads do not have this authority.

Also, the IG Act provides all IGs with the authority to subpoena any information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to perform the functions of the IG Act. This subpoena authority does not specifically address electronically stored information or other forms of data.

H.R. 928 would allow IGs appointed by their agency heads to apply to the Attorney General for full law enforcement authority instead of having to renew their authority on a case-by-case basis or through a blanket authority that must be renewed after an established period of time. The bill would also provide the designated federal entities with IGs appointed by their agency heads the authority under the Program Fraud Civil Remedies Act to address and prosecute false claims and recoup losses resulting from fraud. In addition, the bill would provide the authority for all IGs to require, by subpoena, information and data in any medium, including electronically stored information as well as any "tangible thing."

Panel participants overwhelmingly supported the provisions to (1) allow IGs appointed by their agency heads to apply to the Attorney General for full law enforcement authority instead of having to renew their authority on a case-by-case basis or through a blanket authority, (2) provide designated federal entities with IGs by their agency heads the authority under the Program Fraud Civil Remedies Act to investigate and report false claims and recoup losses resulting from fraud, and (3) define IG subpoena power to include any medium of information and data.

## GAO and IG Coordination:

In May of this year the Comptroller General hosted a meeting with the IGs for the principal purpose of improving the coordination of federal oversight between the IGs and GAO. We believe that effective, ongoing coordination of the federal audit and oversight efforts of GAO and the IGs is more critical than ever, due to the challenges and risks currently facing our nation, including our immediate and long-term fiscal challenges, increasing demands being made for federal programs, and changing risks. Closer strategic planning and ongoing coordination of audit efforts between GAO and the IGs would help to enhance the effectiveness and impact of work performed by federal auditors. Working together and in our respective areas of expertise, GAO and the IGs can leverage each other's work and provide valuable input on the broad range of high-risk programs and management challenges across government that need significant attention and reform.

We will continue in our coordination with the IGs to help achieve our mutual goals of providing the oversight needed to help ensure that the federal government is transparent, economical, efficient, effective, ethical, and equitable. Significant coordination has been and is occurring between GAO and the IGs on agency-specific issues and cross- cutting issues. The Comptroller General in testifying[Footnote 8] on the 25th anniversary of the IG Act, suggested, in light of this increased need for a well-coordinated federal audit community, the creation of a more formal mechanism going forward for a governmentwide council. In addition, panel participants recognized a critical need for a governmentwide council to address broad accountability issues among GAO, the IGs, and OMB. The structure of this council could be similar in concept to the Joint Financial Management Improvement Program (JFMIP), whose principals[Footnote 9] meet at their discretion to discuss issues of mutual concern to promote governmentwide financial management. An accountability council could share knowledge and coordinate activities to enhance the overall effectiveness of government oversight and to preclude duplicate actions.

A good example of a strong formalized partnership between the GAO and the IGs is in the area of financial auditing. Under the Chief Financial Officers Act of 1990, as amended, the IGs at the 24 agencies covered by the act are responsible for the audits of their agencies' financial statements. In meeting these responsibilities, most IGs have contracted with independent public accountants to conduct the audits either entirely or in part. In some cases, GAO conducts the audits. GAO is responsible for the U.S. government's consolidated financial statement audit, which is based largely on the results of the agency-level audits. GAO and the IGs have agreed on a common audit methodology, the GAO-

PCIE Financial Audit Manual, which is used by all auditors of federal financial statements, whether the IG, an independent public accounting firm, or GAO. In addition, we have established formal ongoing coordination and information-sharing throughout the audit process so that both the IGs and GAO can successfully fulfill their respective responsibilities in an effective and efficient manner.

In closing, under the landmark IG Act, the IGs have continued to be an essential component of the government accountability framework and the contributions of the IGs have been most noteworthy. IG independence is critical to the effectiveness of the IG offices in carrying out their unique roles of overseeing federal agencies. Independence not only depends on organizational characteristics, but also on the personal independence of the individual appointed to the office and this individual's freedom from external factors that can impair independence. The IG must maintain this independence while reporting to two organizations--its agency and the Congress. This task requires an IG to maintain a prudent balance between loyalty to the agency and responsibility for conducting objective and independent audits and investigations as required by the IG Act. We believe that a number of the provisions in H.R. 928 would help to enhance IG independence and effectiveness, and we would be pleased to assist the Subcommittee as it considers this legislation.

This completes my formal statement. Mr. Chairman, I would be pleased to answer any questions that you or the Subcommittee members may have at this time.

## Jeffrey C. Steinhoff, U.S. Government Accountability Office

### Managing Director for Financial Management and Assurance

Jeff Steinhoff heads GAO's largest audit unit, with responsibility for oversight of financial management and auditing issues across the federal government. Included is the audit of the government's consolidated financial statements, the establishment of Government Auditing Standards and internal control standards, reviews of internal control, forensic auditing, financial management systems reviews, cost management, improper payments, and the full range of accountability and corporate governance issues.

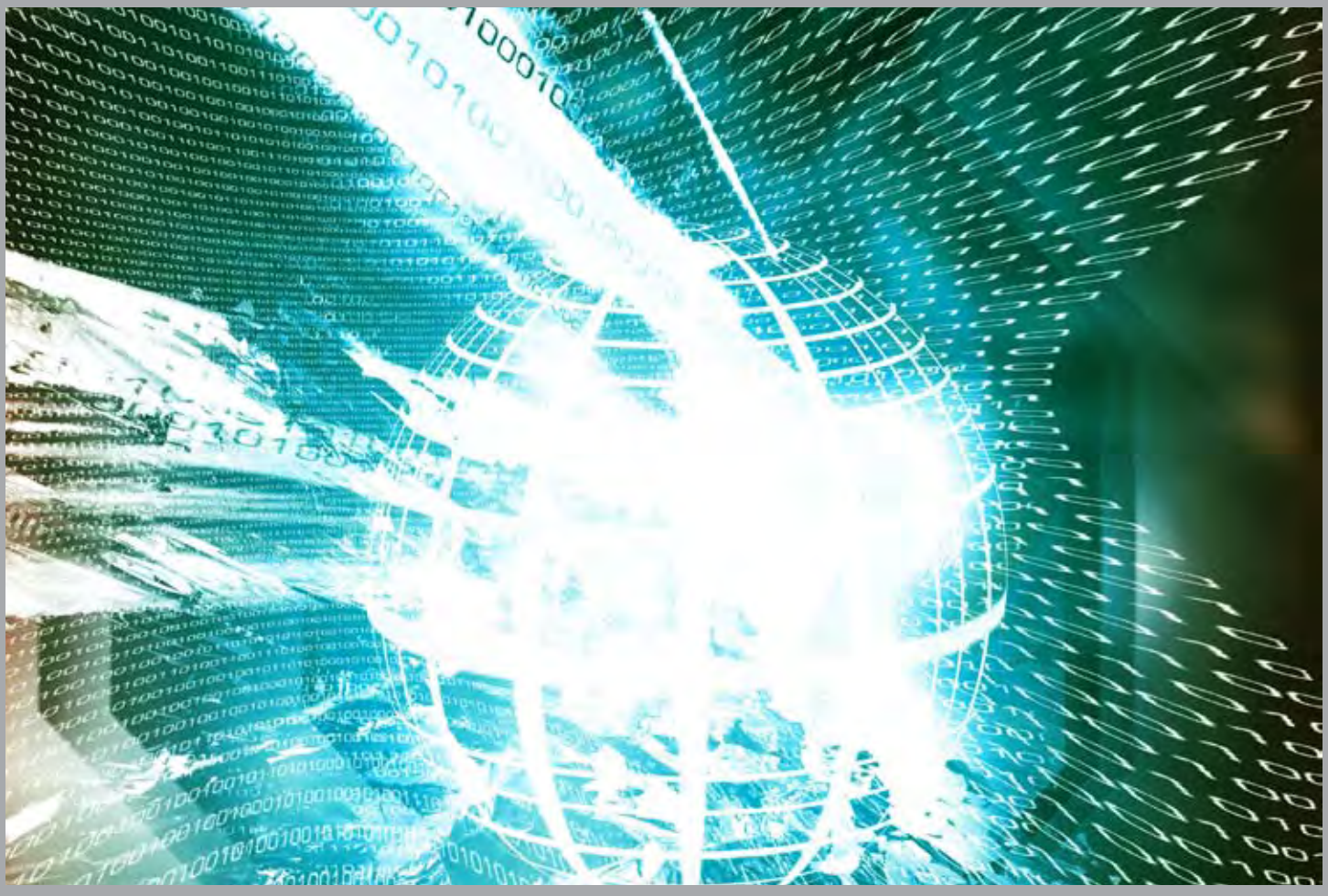
He represents GAO on the Public Company Accounting Oversight Board Standing Advisory Group. He has served on the staff of the Senate Governmental Affairs Committee and was a principal architect of the Chief Financial Officers Act of 1990. He is involved with government-wide implementation of the Act and other financial management improvement legislation.

Mr. Steinhoff graduated from the College of William & Mary. He has completed the Information Systems Program at the Wharton School of the University of Pennsylvania and the Senior Executive Program at Harvard University. He is a Certified Government Financial Manager, a Certified Public Accountant, and a Certified Fraud Examiner. He is a Past National President of the Association of Government Accountants (AGA) and is a member of its Professional Certification Board, which he founded and chaired from 1994 to 1998.

# Extending the Cyber Barricade

by Paul K. Sternal

11



## Closing the Gap in Defense Contractor Cyber Security incident Reporting

## INTRODUCTION

Military contractors are subject to the same epidemic of cyber eavesdropping and data theft as the rest of modern society. However, some of the data held by these contractors, though unclassified, contains sensitive defense technology important to U.S. national security. Since 2004, the defense industrial base has been victimized by increasing numbers of cyber data theft incidents—only a fraction of which have been reported to the government despite the inclusion of sensitive but unclassified (SBU) defense data in their losses. What happens, then, when a member of the defense industrial base falls victim to data theft and the data taken belongs to the Department of Defense (DoD)?

This very question has echoed through the halls of the Pentagon where concerns over incidents of data theft are on the rise. Originally focused on the security of its own networks, the DoD has begun to receive a stream of reports about defense contractor networks being compromised and losing data. And some of that data belongs to the DoD. Some reports come in officially, others through informal channels or third parties, and sometimes not at all. As DoD continues to shore up its own network defenses, it's beginning to wonder what vulnerabilities may threaten its sensitive unclassified data residing in outlying contractor systems and whether those contractors are reporting losses. This data, while unclassified, could relate to weapons systems, military operations, or technology used or planned for military use. The answer to this question has become a policy dilemma.

No provisions, in law or regulation, now require defense contractors to report the loss of SBU defense data through cyber theft. In fact, there are strong reputational incentives not to report. This lack of reporting requirements presents a national security vulnerability, but the exact size of the vulnerability is unclear. The loss of defense information cannot be evaluated when unreported, making a valid damage assessment nearly impossible.

This paper will set forth a recommended course of action expected to result in the needed reporting of data theft incidents among DoD contractors.

## IDENTIFYING THE PROBLEM

Today government or corporate data loss is an increasingly common occurrence. While Government regulations mandate the reporting of data theft involving personal, Privacy Act, and financial data, other categories of information, such as sensitive but unclassified (SBU) defense data residing on contractor networks, are left unregulated. There is growing concern over the protection of defense data that raises the question, what happens when an organization suffers a loss involving data that belongs to the DoD and resides on a contractor system?

This was a question, until recently, left unasked by the DoD as its focus was on the security of its own internal networks. However, in 2004 a DoD contractor suffered an intrusion into its network and decided to report the incident to authorities. Possibly for lack of knowing who actually had jurisdiction or interest in the matter, a multitude of federal agencies were contacted—one of which was the DoD.

The ensuing two year long investigation revealed that this computer intrusion involved the theft of terabytes of sensitive, unclassified DoD data. During the course of the investigation, it was determined that the contractor had actually discovered the malicious activity months before reporting it but tried to deal with the situation internally. While there are several reasons that reporting finally occurred, it's likely the overarching reason was that the theft included data governed by the International Trafficking in Arms Regulation (ITAR). ITAR data is governed by the U.S. Department of State, and the ITAR-related data loss required reporting.

The 2004 contractor intrusion was also a wakeup call for the DoD. It launched a yearlong independent damage assessment to gauge the impact of the data loss on national defense. The assessment, which involved all of the uniformed services and multiple DoD agencies, was the first undertaking of its kind. It was the cyberspace equivalent of the National Transportation Safety Board's response to an airline crash. As a result, the DoD started to pay closer attention to cyber events outside its enclave and pressed the Defense ecurity Service (DSS)[1] and the Federal Bureau of

1 DSS is the designated DoD agency that provides counterintelligence and security liaison to the cleared DoD contractor community. DSS is the primary intake for reportable security incidents among contractors (e.g., espionage, theft of classified data, etc.).

Investigation (FBI) to be vigilant for DoD contractor computer intrusions. Sources close to the Department began to provide information on DoD contractors that were actively combating intrusions involving DoD data with support from third-party information technology (IT) security firms. Other reports indicated that DoD contractors were working with the FBI on computer intrusions. These reports emphasized the need for DoD's awareness of such incidents and its active participation in the response. But how widespread was the problem? And why was there a reluctance to report losses when data stolen from DoD contractors included defense information?

## WHY CYBERCRIME GOES UNREPORTED

While the compromise of defense contractor IT systems and subsequent loss of defense data might appear as a new problem to the DoD, it's likely the only reason it's considered "new" is because the DoD hasn't been looking. Data loss trends from cyber incidents among both government and commercial victims paint quite a different picture—and non-reporting isn't unique to the contractor community. In June 2004, the National Nuclear Security Administration's (NNSA) Albuquerque service center was victimized by a computer intrusion and lost personal information on over 1,500 government and contractor employees. While NNSA didn't discover the loss until a year later, neither officials at the Department of Energy (DOE)[2] nor victims were notified of the incident until June 2006.[3]

A 2005 Washington Post report on a separate cyber theft highlights concerns for government data: "It's not just the Defense Department but a wide variety of networks that have been hit, including the departments of State, Energy, Homeland Security as well as defense contractors…

This is an ongoing, organized attempt to siphon off information from our unclassified systems." [4] The top 3 categories of cyber-related dollar losses to victims come from viruses, unauthorized access, and theft of proprietary information.[5] Of the $130 million of losses reported in 2005, almost 25% was from the theft of proprietary information. And that figure doesn't account for the costs associated with potential loss in strategic and intellectual advantage resulting from the theft of proprietary data. These trends are alarming and, although the DoD hasn't seen this as a problem until recently, the FBI has been working to encourage reporting for a number of years.

Data loss trends from cyber incidents among both government and commercial victims continue to rise, while reporting of incidents by the private sector is on the decline. Reasons for non-reporting include uncertainty over who to report to, fear of bad publicity shaking investor confidence, concern over loss of control of IT systems, and inadequate reporting rules.

Given the well documented trends of increasing cybercrime and infrequent reporting as seen by DOJ, does this trend hold true among DoD contractors? Insiders with access to information on DoD incident intake and defense industrial base activities believe the trend does cross into the DoD contracting community. These insiders are also aware of multiple instances of defense contractor incident reporting to IT security consultants, with reports never reaching DoD for analysis or review. As recently as 2007, a DoD investigation uncovered multiple instances of successful intrusions and data theft among large and small defense contractors. This investigation developed the information independently and did not receive intrusion reports from most of the victim contractors.

## NATIONAL SECURITY IMPLICATIONS

Loss of SBU defense data by DoD contractors impacts national security in a variety of ways. The U.S. military relies not only on the skill and training of its personnel in battle but also on the technical advantage offered by advanced weapons systems. Loss of sensitive defense data erodes that advantage. The compromise of proprietary or sensitive weapons systems data may help an adversary to develop countermeasures against U.S. systems or to identify vulnerabilities. As noted by Jay Kistler, Deputy Director for Joint Force Operations in the Office of the Under Secretary of Defense for Acquisition, Technology & Logistics [USD(AT&L)], divulging vulnerabilities or susceptibilities [to countermeasures] of national defense systems could increase an adversary's ability to produce better or more accurate weapons. In an interview for

2 NNSA is a federal agency that falls under the DOE.
3 Patience Wait, "Energy ups security efforts after loss of employee data," Government Computer News, 19 June 06.
4 Bradley Graham, "Hackers Attack Via Chinese Web Sites," Washington Post, 25 Aug 2005, A01.
5 2005 CSI/FBI Computer Crime and Security Survey.

this study, Kistler spoke specifically about a significant investment by DoD in low observable technology and the protections surrounding that technology. A data loss related to it could result in the compromise of a subsystem causing it to react in an unintended way to certain external stimuli. Would DoD take direct action on this type of data loss? It's hard to say. However knowledge of the loss would surely tell those safeguarding defense technologies what to look for.

## THE POLICY GAP

Given the threat of computer compromise and data theft, and the important role the defense industrial base plays in national security, are DoD contractors that process sensitive unclassified DoD data held to a high enough standard? The simple answer to this question is "no." There are no legal, regulatory, or policy requirements for a DoD contractor to report a computer intrusion that involves the loss of sensitive unclassified DoD data.

• Relevant legislation regulating the security of government information systems and data (Federal Information Security Management Act and Sarbanes-Oxley Act of 2002) does not extend to data held by contractors.

• Pending legislation (Cyber-Security Enhancement and Consumer Data Protection Act of 2007) is a step in the right direction, dictating cyber data loss reporting by industry. But this legislation only covers personal identification information and not government data (e.g., Social Security numbers but not SBU DoD technology).

• DoD and government regulations do not cover protection and loss reporting of defense data when held within contractor information systems.

## POSSIBLE SOLUTIONS

The DoD is taking steps to mitigate the lack of reporting requirements. The DSS is providing contractors with more information about computer security vulnerabilities and communicating with them about incidents of non-reporting. An effort is underway to establish connectivity between DoD cleared contractors and the DoD's classified intranet so contractors may benefit from classified cyber threat warnings. The defense criminal investigative organizations (DCIO) and the FBI are working together when reports are received of intrusions into DoD contractor networks. USD(AT&L) has begun to hold cyber summits with representatives from the top 100 DoD contractors to discuss IT security, protection of defense data, and incident reporting. Further, USD(AT&L) has directed that the Under Secretary of Defense for Intelligence [USD(I)] and Assistant Secretary of Defense for Networks and Information Infrastructure [ASD(NII)] review requirements and make recommendations for protecting DoD information possessed or controlled by contractor systems and notifying DoD in the event of an incident.[6] While this study is ongoing, tentative recommendations are to increase training provided to contracting officers and make changes to the acquisition regulations that would require appropriate reporting by DoD contractors.

The challenge to developing a new reporting requirement for DoD contractors is to balance the government's need for information with the defense industrial base's willingness and ability to supply it. Three alternatives for addressing this challenge are: (i) mandated reporting through contracts; (ii) mandated reporting through legislation; and (iii) encouraged reporting through liaison and outreach.

## THE WAY FORWARD

While DoD would likely have more control by mandating reporting through a change in contracts, the legislative route appears likely to yield success faster and at lower cost. Once signed into law, the legislative alternative could be implemented immediately and, theoretically, at no cost to contractors if it simply requires reporting and remains separate from existing requirements to maintain best practice security mechanisms. The political environment seems ripe for any type of legislation protecting victims of cyber data theft. Now would be the time to advocate changes that expand protection for confidential data, from personal data to sensitive government data. However, even with the current positive political climate, the legislative option may take too long to implement given the history of delays in similar legislation. The contracting option is a strong competitor, given the degree of control DoD can exercise in its implementation and enforcement. The third

6 Mark Hall, "IA Issues for Controlled Unclassified Information and the National Cyber Response Coordination Group," Department of Defense, 2006.

option, encouraged reporting, should also be pursued, alongside the legislative or acquisition regulation changes, as it will be the foundation upon which the operational reporting and incident response actions are built.

Given a plan to address the problem, what will it take to move forward with implementation? Due to the sensitive nature of data processed by DoD contractors, the stakes are high. In a worst case scenario, unreported data loss is amassed by an adversary who uses the information to build countermeasures to a certain U.S. weapons system. Then, at some point in the future, the U.S. engages a less sophisticated adversary who is able to defeat "superior" U.S. weapons resulting in higher than anticipated friendly casualties. It's not wise to wait for this scenario to play out before taking action to prevent it from happening. However, there are powerful stakeholders on either side of the debate over reporting that must come to some type of consensus.

While some DoD contractors have been forthcoming in reporting security breaches, that is by no means a broad reflection of the defense industrial base. Many DoD contractors are highly suspicious of any additional requirements for reporting and regulation and prefer to avoid reporting in order to protect their reputation and shareholder value. The contractor community feels overregulated and sees any new attempts to impose IT requirements as an additional resource drain.

The DoD looks at the problem from quite a different perspective. It sees the loss of defense data, whether in government or contractor custody, as a significant national security vulnerability. Aside from taking action to help prevent the future loss of defense data from information systems, DoD identifies, quantifies, and then assesses the impact to national security after any data loss. Based upon this impact assessment, it may require changes to weapons systems or in their method of employment.

However, to take any of these actions, the DoD must be informed of the loss at the onset. DoD officials have expressed frustration at the fact that DoD, as the owner of defense data, can't simply require the defense industrial base to report losses. And further frustration arises when it appears that, in order to reduce overhead costs, DoD contractors who also sell information assurance services don't use those services to protect their own networks that process DoD data.

## PRIVATE SECTOR FEEDBACK

While dealing with cyber-based data loss among the defense industrial base is somewhat new for the government, addressing these concerns within the banking industry is not. Melanie Teplinsky is an attorney in the e-commerce practice of an international law firm who has provided extensive advice to banking clients on reporting cyber security incidents to law enforcement. In her experience, the main issue for clients when it comes to reporting these incidents among banks, or corporations in general, is their legal obligation. Beyond the legal obligation, organizations must weigh how best to handle such incidents from a customer perspective—especially among banks whose reputation is everything. They must carefully consider the timing of an investigation, the impact of bringing in federal investigators, and when to make a press release. Despite the myriad of considerations related to reporting, Teplinsky's assessment of the financial sector is that firms generally feel it is better to disclose than not to disclose. This willingness to report incidents is undoubtedly influenced by recent changes made by regulators to require cyber incident reporting in the financial sector.

The Bank Secrecy Act of 1970 requires financial institutions to report certain types of suspected criminal activity to the Department of the Treasury's Financial Crimes Enforcement Network.[7] In 2000, the Treasury added computer intrusions as a type of criminal activity that required reporting. This reporting is very straightforward and done via a two-page Suspicious Activity Report (SAR) Form available on the Internet. The form must be filed within 60-days of the initial detection of activities such as the cyber theft of funds, theft of customer account information, or damages to critical systems of the institution.[8] Federal law provides a "safe harbor" for institutions filing SARs, protecting them from liability for making the disclosure and prohibiting those institutions from disclosing the fact that a SAR was submitted to authorities.[9]

7 Sandeep Junnarker, "Anatomy of a hacking," CNET News.com, 1 May 2002.

8 Suspicious Activity Report Instructions, June 2003 (http://www.fincen.gov/forms/f9022-47_sar-di.pdf).

9 31 United States Code 5318(g)(2) and 31 United States Code 5318(g)(3).

The Treasury Department has also put mechanisms in place through the Code of Federal Regulations (12 CFR Part 21 Subpart C §21.21) to verify compliance with the Bank Secrecy Act by requiring internal controls and independent testing. The model requiring the reporting of cyber thefts among financial institutions may be of use in addressing similar problems among defense contractors. And if defense contractors fall in line with other large private corporations, federal reporting requirements may not be entirely unwelcome.

Having worked with a large number of private corporations, Teplinsky indicates that most are eager to meet their legal requirements—inclusive of federal regulation and non binding guidance. She notes that if the Government is clear in what it wants, then generally corporations and contractors will comply, as regulations are often viewed as legal requirements.

Within the context of defense contractor reporting, Teplinsky opines that, while a defense contractor may not have a legal or regulatory requirement to report a cyber data loss involving SBU defense data, they may still be under some [implied] obligation to report such a loss. However, without clear guidance on how and where to report, reporting is unlikely to occur. Should reporting requirements be clearly defined and easy for the contractor to accomplish (similar to a SAR), then a mandated reporting requirement may actually help contractors by taking the decision out of their hands and evening the playing field among those who report voluntarily versus those who do not. This would help undermine some of the reputational concerns long held by the private sector when weighing the decision to disclose.

A Top 25 DoD contractor, who agreed to anonymous participation in this research, shared their insight and experience with cyber incident reporting. Of paramount concern to the contractor was the lack of information sharing by the government to industry. According to him/her, if the government doesn't clearly communicate the threat to industry, how can they detect and report incidents of interest? This contractor had an incident in the not-too-distant past that was reported to the government. According to the contractor, once it was reported, the government (over)classified the incident and the result was poor communication back to the contractor. "This can't be just us," said the contractor. "At the time, it was totally classified what was going on…."

Large contractors do put an emphasis on information security and the protection of their networks, if not before a cyber security incident, then certainly afterwards. One Top 25 contractor conducts regular information technology security audits of its various business units and continues to increase the requirements within those audits. It also understands the value of counterintelligence threat information. Just because it's the private sector, doesn't make it immune to threats from foreign governments—especially if it has close ties to the DoD. Gaining access to the DoD's secret Internet is a high priority for this Top 25 contractor in order to further information sharing as well as reporting. And they see a significant amount of activity to report, "…[We] often see attacks on Friday afternoon before long weekends…see them go on smoke breaks and everything." This contractor described the activity as, "espionage by remote control."

Absent regulation or legislation, this Top 25 contractor is already taking steps to better share information with the government by participating with other large defense contractors and the FBI and DoD in an information sharing forum and other working groups. However, reporting incidents to the DoD is viewed as very disjointed. As the contractor described it, with the DSS, Air Force Office of Special Investigations, Defense Criminal Investigative Service, and the Counterintelligence Field Activity, "…[DoD] has a lot of horses in the barn…"—in fact, too many horses to make reporting simple. That's why their primary reporting is done to the FBI.

When asked what DoD could do to elicit cyber incident reporting from the defense industrial base, the Top 25 contractor had specific recommendations: 1) create some type of "fusion center" for the sharing of information, 2) remove attribution from reporting, 3) clearly define the scope of a reportable incident, 4) identify the critical program information that needs protection at the start of a contract, and 5) insure a feedback loop exists for information return to contractors. The act of reporting incidents in and of itself is viewed as a limited cost to the contractor. However, the solution goes far beyond setting up a system to receive reports but rather a big picture approach to address current cyber threats. This Top 25 contractor sees the problem clearly: "We're all targets and we're constantly being targeted."

## PUBLIC SECTOR FEEDBACK

Government officials seem to agree that the best way to tackle the problem of defense contractor incident reporting is through acquisition channels. But, beyond that, they are still struggling with just how to implement these requirements.

Jay Kistler has a big picture view of the larger problem of defense contractor intrusions and five areas for improvement that must be addressed by the government: 1) contractor security and prevention, 2) government/industry response, 3) monitoring and oversight, 4) the damage assessment process, and 5) the use of counterintelligence data. The issue of defense contractor reporting is interwoven among these five areas. Without reporting, the effectiveness of security and prevention will remain unknown and the counterintelligence information cycle will run flat for lack of input. However, in order to achieve effective reporting, the government needs to provide clear guidance and policy to direct response efforts and maintain oversight.

The problem isn't as simple as receiving notice from a contractor that they've had a computer intrusion with data loss and filing that document away in some archive. The notice should launch a chain of events that begins with a law enforcement response to the victim contractor, includes a review of defense programs on which the contractor works, involves a damage assessment to determine the impact to national security from the data loss, and concludes with feedback to the defense community on how security can be improved to avoid future such breaches. Currently there isn't much policy on how the DoD should interact with its contractors on what used to be considered strictly an internal security issue.

## EVALUATION OF ALTERNATIVES

Given the input from members of the public and private sectors familiar with this policy issue, the previously discussed alternatives can be reexamined in terms of feasibility to implement, ability to enforce, and likelihood of success. The most critical factor is the likelihood of success, followed by enforcement, then implementation considerations. Table 1 below summarizes how the three policy alternatives compare based upon these criteria.

The likelihood of successful widespread reporting is truly the barometer of success for any of the alternative policy solutions. There currently exist limited and sporadic cases of contractor incident reporting. Thus, anything less than a broad increase would simply be the status quo. To achieve such an increase would require active participation by contractors to identify incidents within their own networks, then positive steps to inform the government. Alternatives 1 and 2 offer the best chance at achieving widespread reporting as each would establish requirements for reporting and penalties for non-compliance that are applicable to the entire defense industrial base. Alternative 3 does not positively require reporting and would have less of an impact than the previous alternatives.

The ability to enforce any of the alternative policy solutions rests in the mechanism with which the government implements the reporting requirement. Therefore, if contractors are simply informed they have an obligation to report but that obligation is not reinforced by some law or regulation, the government has no recourse or ability to enforce the reporting requirement. As alternatives 1 and 2 are based in law and regulation, they carry with them mechanisms to conduct oversight and penalize non-compliance through actions such as imposing fines and cancelling contracts. The remaining alternative offers little by way of enforcement mechanisms as it relies on voluntary participation.

Given the fact that contractors are losing SBU defense data today, it must be feasible for the selected policy solution to be implemented in a timely manner. Moreover, it is not only important that the policy can be implemented quickly, but that it can be adjusted with relative ease. Alternatives 1 and 3 are within the control of DoD and, thus, can be implemented the fastest. Alternative 2 relies on time consuming legislative action.

## RECOMMENDATION

Based on the criteria above and analysis of the alternatives, mandating reporting through a contractual mechanism is the best policy alternative for DoD to quickly implement a solution that is enforceable and will have widespread impact. Implementation through a change to the FAR can cover not only those contractors working directly for the DoD, but also contractors that hold sensitive defense data under contract to other government departments.

## Evaluation of Alternatives

| Policy Alternative | Feasibility for timely Implementation | Ability to Enforce | Likelihood of Successful Widespread Reporting |
|---|---|---|---|
| Contractual | √ | √ | √ |
| Legislative | | √ | √ |
| Encouraged-Liaison | √ | | |

As DoD has traditionally looked inward to detect and address cyber security incidents, and the outward focus of the proposed remedy is something new, the measure will most likely undergo some adjustments through the initial stages of implementation.

The new FAR language would need to specify guidelines on cyber incident reporting such as a timeline (e.g., "within 48 hours"), parameters (e.g., "a known or suspected loss"), definitions (e.g., "sensitive defense data" and "cyber security incident"), penalties for non-reporting, and to whom to report. The FAR amendment would be advertised in the Federal Register and, after comments had been reviewed and addressed, it would be published. The Defense Security Service (DSS), if appropriately staffed, is the recommended recipient of the incident reports. DSS would train its personnel on receiving and staffing the reports, and publish implementing guidance to its internal staff and the defense industrial base while keeping the Defense Criminal Investigative Organizations and FBI appraised of how it planned to disseminate information to them in a timely manner.


## Paul K. Sternal, Department of Defense IG

### Special Agent

Special Agent Sternal is the cyber crimes program manager for the Defense Criminal Investigative Service. He began his law enforcement career in 1993 as a special agent with the U.S. Air Force Office of Special Investigations (OSI), and was assigned to Yakota AB, Japan. During that time, he served as a computer crime investigator operating throughout the Pacific Rim at bases in Guam and Korea as well as Japan.

In 1995, Paul entered the Air Force communications field, holding assignments at the Air Intelligence Agency in San Antonio, Texas and the White House Communications Agency in Washington, D.C. As a Reservist, he is currently a Major assigned to the Defense Information Systems Agency.

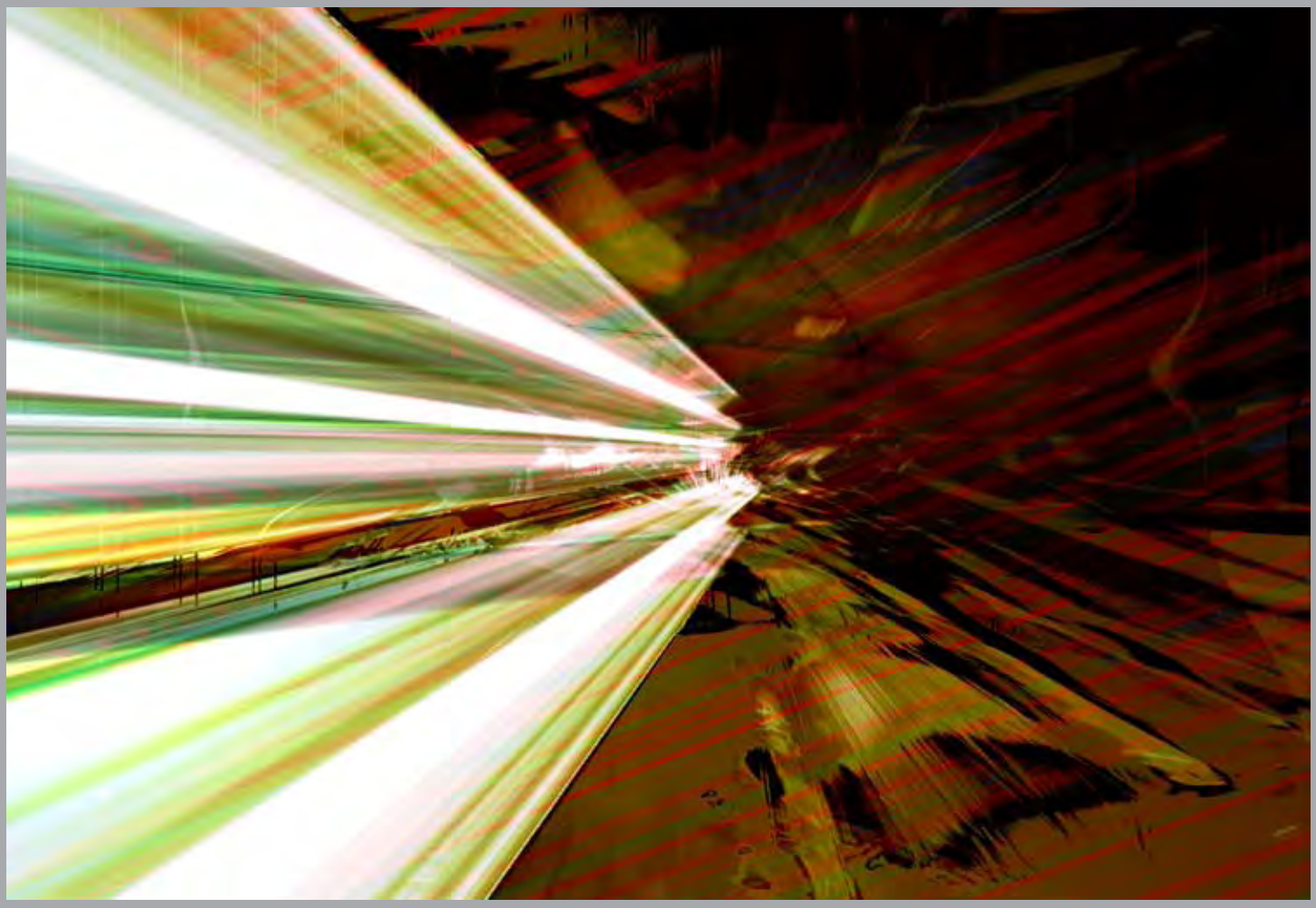
In 2002, Paul joined DCIS as a computer crime investigator in the Mid-Atlantic Field Office. Since joining DCIS, he has specialized in high technology crime investigations and computer forensics. He has been intricately involved in several high-profile intrusion investigations. In 2004, he served a three month tour as a DCIS Special Agent with the Middle East Task Force - Baghdad, Iraq, Coalition Provisional Authority.

SA Sternal is a graduate of George Washington University and holds a Bachelor's Degree in Computers and Information Systems. He holds a Master's Degree in Business Administration from Rutgers University and a Master of Public Policy degree from Georgetown University.

# Information Sharing

by Scott A. Boehm

12



## Throughout the Intelligence Community

## PROBLEM STATEMENT

The National Security Act of 1947 established the Central Intelligence Agency (CIA) and the Intelligence Community (IC), both under the direction and authority of the Director of Central Intelligence (DCI). Since the Intelligence Community's creation, collectors of intelligence information have unilaterally determined how to disseminate the collected information without allowing any objective input or appeal from intelligence consumers regarding proper or even alternative dissemination, resulting in a lack of information access within the community.

## INTRODUCTION

This phenomenon is the result of competing cultures within the Intelligence Community. Collectors of intelligence information spend vast amounts of money and time to recruit, vet, and hide the identities of their human sources. For the technical intelligence disciplines (SIGINT, IMINT, and MASINT), collectors spend billions of dollars and years of effort developing scientific methods to collect extremely sensitive information. Therefore, it is no surprise that collectors tend to value security foremost and continually demonstrate a "risk averse" mentality when disseminating their information to analysts and other consumers who need the information to produce intelligence.

The result of this "risk averse" approach often leads to a lack of information access within the United States Intelligence Community. Its net effect is either incomplete analysis or a lack of competing analyses among similar organizations working to provide comprehensive intelligence for a given policy maker or consumer.

## BACKGROUND

The National Security Act of 1947, as amended, established the National Security Council (NSC), the Secretary of Defense, the Joint Chiefs of Staff, the DCI, and the CIA, among others. The Act also established the Committee on Foreign Intelligence, within the NSC, to "conduct an annual review of the elements of the Intelligence Community in order to determine the success of such elements in collecting, analyzing, and disseminating the intelligence required to execute U.S. national security interests." However, the Committee on Foreign Intelligence has been reluctant to address the issue of collection organizations unilaterally determining dissemination of the information they collect. Instead, the Committee has focused its attention on the value of the national intelligence produced and not the internal Intelligence Community methodology for producing and dissemination the intelligence.

The National Security Act of 1947 does not address dissemination of collected intelligence. The Assistant Director of Central Intelligence for Collection was tasked with "assisting the Director of Central Intelligence in carrying out the Director's collection responsibilities in order to ensure the efficient and effective collection of national intelligence." The Assistant Director of Central Intelligence for Analysis and Production was tasked to "direct competitive analysis of analytical products having national importance, and identify intelligence to be collected for purposes of the Assistant Director of Central Intelligence for Collection."

## THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 (IRTPA)

As a result of the 9/11 intelligence failures, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The IRTPA amended the National Security Act of 1947 by eliminating the Director of Central Intelligence and replacing him with the Director of National Intelligence. This change was not merely a semantic one. The Congress realized that having a single individual responsible for directing both the CIA and the entire Intelligence Community created an inherent conflict of interest when information access and competing analysis issues arose. Congress placed a prohibition on dual service by stating "the individual serving in the position of Director of National Intelligence shall not, while so serving, also serve as the Director of the Central

Intelligence Agency or as the head of any other element of the Intelligence Community."

## ALTERNATIVES

There are three alternative strategies to explore regarding how to solve or mitigate the problem that Intelligence Community collectors of intelligence information have unilaterally determined how to disseminate the collected information without allowing any objective input or appeal from intelligence consumers regarding proper or even alternative dissemination, resulting in a lack of information access within the community.

***ALTERNATIVE 1***: The Director of National Intelligence should place all intelligence dissemination authorities within the Office of the Associate Director of National Intelligence/Chief Information Officer (ADNI/CIO).

Recommendation 9.2 of the WMD Commission Report states, "The DNI should give responsibility for information sharing, information technology, and information security within the Intelligence Community to an office reporting directly to the DNI or to the Principal Deputy DNI."

Notwithstanding the DNI CIO's fiscal authorities over the Intelligence Community's information technology (IT) budget, the CIO's office is not equipped to handle the myriad of information sharing policy and oversight tasks implicit within WMD recommendation 9.2.

***EVALUATION***: Upon analysis, this alternative was discarded. Policy and oversight responsibilities should be an organization's sole responsibility. Just as the ODNI's responsibility is oversight of the Intelligence Community and not the actual collection and production of intelligence, a policy office should not be involved in the day-to-day implementation of that policy from an IT perspective. This situation could lead to conflict-of-interest issues if policy and implementation are commingled.

***ALTERNATIVE 2***: The Director of National Intelligence should establish a Deputy Director for Dissemination. Although the intelligence cycle consists of five phases - planning and direction; collection; processing; analysis and production; and dissemination; the responsibility for dissemination within the ODNI has been trifurcated. Dissemination is the only phase of the intelligence cycle that is not the sole responsibility of a single office within the ODNI. By statute, the Director of National Intelligence can have no more than four Deputy Directors. This option clearly requires the Director to shift responsibilities within the Directorates. If analysts or policy makers had concerns that they were not receiving the intelligence information required to perform their mission from an Intelligence Community collection organization, they could appeal to the Deputy Director for Dissemination to adjudicate their request. However, this alternative presupposes that analysts and policy makers know the universe of collection within the Intelligence Community.

***EVALUATION***: Establishing a Deputy Director for Dissemination would promote efficiency by placing all dissemination authorities within one national-level office. This office would act as a "Dissemination Czar" and provide intelligence consumers with an appeals process for dissemination issues. This alternative would also prioritize dissemination within the intelligence cycle by placing all authorities under a Deputy Director.

Notwithstanding the placement and access of a Deputy Director for Dissemination, one weakness with an appeals system concerns the long-standing cultural divide between collectors and their consumers. Within this construct, it is likely that intelligence consumers and the Deputy Director for Dissemination would not know if they were receiving all of the collected information. Without direct oversight, exercised on a daily basis within collection organizations, collectors may be inclined to limit dissemination of intelligence information. This alternative does not include any daily, direct oversight within collection organizations. It is, in fact, inherently unfair to ask collectors to both protect sources and methods and assume all the risk of making dissemination decisions on the information they collect.

This alternative's political feasibility, its acceptability within both the existing Intelligence Community bureaucracy and the Legislative Branch of the federal government, remains dubious at best. By statute, the DNI cannot have

more than four Deputy Directors. Therefore, if the DNI wishes to establish a Deputy Director for Dissemination, he must request that Congress amend the Intelligence Reform and Terrorism Prevention Act (IRTPA) to allow for a fifth Deputy Director. The political feasibility of such a move would be problematic at best. The DNI, and the President, would expend a tremendous amount of political capital in asking Congress to amend the law, especially when Congress did not stipulate which four Deputy Directors the DNI could choose.

The robustness of this alternative is also questionable. Since the collection community contains highly-competitive, enterprising personalities, the chance that information will not be shared remains high. Collectors are much more comfortable protecting their sources and methods than ensuring access to the information under their direct control. Absent an outside presence within collection organizations, providing daily oversight of the dissemination of their information, collectors have continually demonstrated a unilateral default toward protecting their sources and methods at the expense of increased dissemination.

***ALTERNATIVE 3***: The Director of National Intelligence should establish Dissemination Coordination Offices (DCOs) within Intelligence Community collection organizations with an appeals process to a newly-appointed Assistant Deputy Director for Dissemination within the Office of the Deputy Director for Requirements.

The CIA, Department of State, DIA, FBI, NSA, and NGA are the main collectors of intelligence information within the Federal government. Each of these collection organizations currently exercises unilateral authority to determine the dissemination of the information it collects. However, the IRTPA grants the Director of National Intelligence broad dissemination authorities:

"The DNI shall have principal authority to ensure maximum availability of and access to intelligence information . . . In order to maximize the dissemination of intelligence, the DNI shall establish and implement guidelines for access to and dissemination of intelligence, both in final form and in the form when initially gathered."

By establishing Dissemination Coordination Offices (DCOs) within each collection organization, with a formal appeals process to the Assistant Deputy Director for Dissemination, the DNI may be able to eliminate the phenomenon that analysts and policy makers "don't know what they don't know." This alternative places analytic community representatives closer to the sources of information. It also leverages the representatives' analytic expertise to determine which individuals from their parent organization can best synthesize the reporting to conduct competing analyses.

Coordination Officers, who would be embedded within IC collection organizations, would provide dissemination guidance to collectors and collection managers. In the event of a dissemination impasse, the DCOs would appeal to the Division Director within the collection organization. If the Division Director still felt that further dissemination would compromise the source or method whereby the information was gathered, the DCO could appeal to the Director of the collection Agency. The Agency Director would have the authority to decide the appeal in favor of the DCO. If the Agency Director also decided to limit dissemination, the DCO would have the authority to appeal the decision to the Assistant Deputy Director for Dissemination. The Assistant Deputy Director would adjudicate the request for dissemination, weighing the need to protect the source or method against the requirement to ensure information access throughout the Intelligence Community. The Assistant Deputy Director would then consult with the Director of National Intelligence and render the final dissemination verdict.

***EVALUATION***: If efficiency is defined as maximizing consumer access to collected intelligence information, this alternative has several attractive features. First, this alternative places analytic community representatives closer to the sources of information. It also leverages the representatives' analytic expertise to determine which individuals from their parent organization can best synthesize the reporting to conduct competing analyses. If collectors built a personal relationship with an analyst, or group of analysts, the collectors would be more inclined to share their information with this select group of individuals.

However, since 9/11 the Intelligence Community has grown significantly as a federated enterprise. Most intelligence analysts are scattered worldwide, supporting a variety of intelligence missions, and are not physically collocated with the collectors to "build a relationship." Dissemination Coordination Offices (DCOs), located at the source of collection, could provide direct oversight over the dissemination process and agency-specific expertise in determining where the information should go within their own parent organization.

Most intelligence information originates within the CIA, DIA, FBI, NSA, NGA, and State Department. Further, financial, counterterrorism, counter proliferation, weapons of mass destruction, and military intelligence information are no longer isolated bits of data. The Global War on Terrorism has proven that these seemingly disparate types of information are all interrelated. Merely providing all counterterrorism information to a Counterterrorism Center (CTC) and making dissemination decisions at the Center risks excluding other possibly pertinent information.

Since most intelligence information originates within these six organizations, to fully implement this alternative we must address the resource implications of the DCO concept. DCOs would include five personnel within each of the above collection organizations, encumbering joint IC billets, for a total of 30 officers. Each officer would have responsibility for a specific client base and assist only with dissemination and re-dissemination of the most sensitive reporting. This aspect cannot be overstated since the most sensitive reporting is often also the most authoritative due to the placement and access of the source or method. For example, the five DCOs assigned to the FBI would come from the analytical organizations that utilize the bulk of the FBI's sensitive reporting. The resource implications for organizations providing officers to fill DCO joint IC billets would be minimal. Most organizations could spare five intelligence officers from their staffs of hundreds or thousands of personnel.

This alternative would be politically feasible within both the existing Intelligence Community bureaucracy and the Legislative Branch of the federal government. First, it would not require the DNI to lobby Congress for a fifth Deputy Director.

The Assistant Deputy Director for Dissemination would be subordinate to the Deputy Director for Requirements since dissemination is directly linked to his mission of "understanding the needs of the customers of national intelligence." Second, the Assistant Deputy Director for Dissemination would act as the "Dissemination Czar" within the Intelligence Community, a position that the House and Senate Intelligence Committees have longed for since the IRTPA was signed into law in 2004.

Since Dissemination Coordination Offices (DCOs) would be embedded within collection organizations, with universal access to all collected information, the phenomenon that intelligence consumers "don't know what they don't know" would be mitigated. The DCOs, having universal information access, would provide the necessary oversight within collection organizations to ensure that all available intelligence information was shared with their respective organizations. If a dissemination impasse were to develop between the DCO and the collection organization, the DCO could appeal directly to the Assistant Deputy Director for Dissemination to adjudicate the case.

***FINAL ANALYSIS***: After analyzing both alternatives, the Director of National Intelligence should establish Dissemination Coordination Offices (DCOs) within Intelligence Community collection organizations with an appeals process to a newly-appointed Assistant Deputy Director for Dissemination within the Office of the Deputy Director for Requirements. There are several reasons why this alternative is the best choice. First, it provides for a national-level "Dissemination Czar," something the Congressional Intelligence Oversight Committees have longed for since they passed the IRTPA in 2004. Second, this alternative provides for daily oversight of collection organizations at the source of collection, something the Intelligence Community has not seen since its inception in 1947. It also provides for an objective organization, the Office of the Assistant Deputy Director for Dissemination, to make the difficult dissemination decisions when the collection and analytical

bureaucracies are at an impasse. The collector culture has proven that it will dominate the analytical culture, as it has for the past 60 years. This alternative provides analysts with a voice in dissemination decisions and a direct appeals process to a national-level adjudicative body. Finally, for the first time analytical representatives would have universal access to all collected information within all collection organizations. This would preclude the "I don't know what I don't know" phenomenon that has continually plagued the Intelligence Community. As an Intelligence Community, we must have continual oversight of collection with an appeals process to an objective adjudication organization. This alternative will ensure that intelligence consumers receive all collected information to produce the most comprehensive intelligence product possible.

## Scott A. Boehm, Office of the Director of National Intelligence OIG

### Assistant Inspector General for Inspections

Scott Boehm attended the University of Notre Dame on a four-year Army ROTC scholarship, and graduated in 1986 with a degree in Philosophy.

Upon graduation, Scott received a Regular Army commission in the Army Aviation Branch and attended flight school at Ft. Rucker, Alabama, where he learned to fly the UH-60A Blackhawk helicopter.

In 1987, Scott was assigned to Germany. In 1988, he was named the Special Army Liaison Officer to the U.S. Ambassador, U.S. Embassy, Nicosia, Cyprus. Scott coordinated joint and multinational flight operations in support of the American Embassy in Beirut, Lebanon and regularly flew missions into Beirut.

In 1991, Scott was assigned to the 101st Airborne Division (Air Assault) at Ft. Campbell, Kentucky. He served in the Division for five years. In 1992, Scott joined the U.S. Army's Military Intelligence Corps and served as an Infantry Battalion, Infantry Brigade, and Aviation Brigade Intelligence Officer in the 101st. He also commanded an Infantry Battalion Headquarters Company of 215 soldiers for 18 months.

He has worked in the Pentagon for the Army Staff, the Defense Intelligence Agency as a Military Intelligence Analyst, and the Department of Defense Inspector General as a Project Manager leading intelligence evaluations.

Scott's current position is Assistant Inspector General for the Director of National Intelligence. He leads teams conducting intelligence evaluations and reviews to assist in transforming the national intelligence apparatus. Scott also holds a Master's Degree in Public Policy Management from Georgetown University.

# Invitation to Contribute Articles

# to

# The Journal of Public Inquiry

The Journal of Public Inquiry is a publication of the Inspectors General of the United States. We solicit articles from professionals and scholars on topics important to the Inspector General community.

Articles should be approximately
four to six pages (2,000-3,500 words),
single-spaced, and submitted to:

Jennifer Plozai
Department of Defense Office of the Inspector General,
400 Army Navy Drive, Room 1034
Arlington, VA 22202
(703) 604-8322

# Inspector General Act of 1978, as amended
# Title 5, U.S. Code, Appendix

**2. Purpose and establishment of Offices of Inspector General; departments and agencies involved**

In order to create independent and objective units--

(1) to conduct and supervise audits and investigations relating to the programs and operations of the establishments listed in section 11(2);

(2) to provide leadership and coordination and recommend policies for activities designed (A) to promote economy, efficiency, and effectiveness in the administration of, and (B) to prevent and detect fraud and abuse in, such programs and operations; and

(3) to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action;