

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

*The Journal of Public Inquiry*



FALL/WINTER

2008-2009

COUNCIL OF INSPECTORS GENERAL ON  
INTEGRITY AND EFFICIENCY

# Council of Inspectors General on Integrity and Efficiency

## Members of the Council

“The Inspector General Reform Act of 2008” created the Council of Inspectors General on Integrity and Efficiency. This statutory council supersedes the former President’s Council on Integrity and Efficiency and Executive Council on Integrity and Efficiency, established under Executive Order 12805.

The CIGIE mission is to address integrity, economy, and effectiveness issues that transcend individual government agencies; and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

The Chair of the CIGIE is the Honorable Phyllis K. Fong, US Department of Agriculture IG, and the Vice-Chair is Mr. Carl A. Clinefelter, Farm Credit Administration IG. The membership of the CIGIE includes the 67 statutory Inspectors General of the following agencies.

Agency for International Development  
Department of Agriculture  
Amtrak  
Appalachian Regional Commission  
Architect of the Capitol  
U.S. Capitol Police  
Central Intelligence Agency  
Department of Commerce  
Commodity Futures Trading Commission  
Consumer Product Safety Commission  
Corporation for National and Community Service  
Corporation for Public Broadcasting  
The Denali Commission  
Department of Defense  
Office of the Director of National Intelligence  
Department of Education  
Election Assistance Commission  
Department of Energy  
Environmental Protection Agency  
Equal Employment Opportunity Commission  
Export-Import Bank of the United States  
Farm Credit Administration  
Federal Communications Commission  
Federal Deposit Insurance Corporation  
Federal Election Commission  
Federal Housing Finance Board  
Federal Labor Relations Authority  
Federal Maritime Commission  
Federal Reserve Board  
Federal Trade Commission  
General Services Administration  
Government Accountability Office  
Government Printing Office  
Department of Health and Human Services  
Department of Homeland Security  
Department of Housing and Urban Development  
Department of Interior  
U.S. International Trade Commission  
Department of Justice  
Department of Labor  
Legal Services Corporation  
Library of Congress  
National Aeronautics and Space Administration  
National Archives  
National Credit Union Administration  
National Endowment for the Arts  
National Endowment for the Humanities  
National Labor Relations Board  
National Science Foundation  
Nuclear Regulatory Commission  
Office of Personnel Management  
Peace Corps  
Pension Benefit Guaranty Corporation  
Postal Regulatory Commission  
U.S. Postal Service  
Railroad Retirement Board  
Securities and Exchange Commission  
Small Business Administration  
Smithsonian Institution  
Social Security Administration  
Special Inspector General for Iraq Reconstruction  
Department of State  
Tennessee Valley Authority  
Department of Transportation  
Department of Treasury  
Treasury Inspector General for Tax Administration  
Department of Veterans Affairs

# LETTER FROM THE EDITOR-IN-CHIEF

**A**s I was reviewing the Fall/Winter 2008-2009 issue of the Journal of Public Inquiry, I was reminded about something the late President John F. Kennedy said: “Leadership and learning are indispensable to each other.”

The Journal is a learning tool and that is exactly why this publication – especially your contributions to it – play such a vital role in the Inspector General community. The Journal allows us to share our successes, lessons learned, and way forward – all in the hope we will not only become better leaders, but also better teachers.

I believe the value of the Journal is further enhanced by ensuring open and transparent communications with the public through its availability on the web and in print. It educates and informs the public with important insight into how we do business. In so doing, the Journal lays a foundation for building public trust – without which we can not be truly effective.

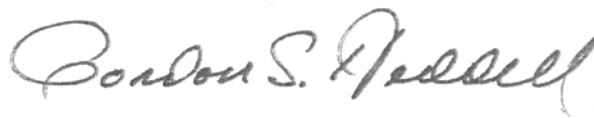
This particular issue of the Journal is special because of the many changes brought about by the formation of the Council of Inspectors General on Integrity and Efficiency, which is the subject of our feature article written by the Inspector General of the U.S. Department of Agriculture and CIGIE Chair, Phyllis Fong. The article, entitled “The IG Reform Act and the New IG Council: Dawn of a New Era,” is a comprehensive overview of the IG Reform Act of 2008 and the new goals that the CIGIE has adopted.

The Journal also features an excellent example of lessons learned in the testimony of Special Inspector General for Iraqi Reconstruction Stuart Bowen as he discusses the “Hard Lessons” of the early reconstruction effort in Iraq during his appearance before the Commission on Wartime Contracting.

Inspector General Patrick O’ Carroll of the Social Security Administration discusses how Social Security intersects with immigration enforcement in a speech delivered at a Federal Bar Association seminar. In addition, an article written by Inspector General Earl Devaney of the Department of Interior and James O’ Sullivan outlines the Honest Services Fraud Statute and its importance in dealing with public corruption cases.

Other articles address topics including tape recording of law enforcement-related interviews; the legal requirements of different business entities; and fraud awareness initiatives. These articles are relevant and timely to the issues facing our oversight community.

Finally, I would like to thank all of the authors for their submissions. It continues to be a difficult selection process for each and every edition of the Journal. The competition among the submissions continues to increase, which speaks well of the authors, their efforts, and the Inspectors General community as a whole. Your willingness to share your experiences in a transparent, open forum speaks volumes about your belief in what we do and your dedication to improving the process so we can better serve our country. In helping others to learn, we help ourselves become better leaders.



Gordon S. Heddell  
Acting Inspector General

# Journal

of Public Inquiry

DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL STAFF

EDITOR-IN-CHIEF  
Gordon S. Heddell

PUBLISHER  
John R. Crane

EDITOR  
Jennifer M. Plozai

GRAPHIC DESIGNER  
Jacob A. Brown

COPY EDITOR  
Bill McGloin

## JOURNAL EDITORIAL BOARD

Thomas C. Cross  
Acting Inspector General  
National Science Foundation

Mary Kendall  
Acting Inspector General  
Department of the Interior

Gregory H. Friedman  
Inspector General  
Department of Energy

J. Russell George  
Inspector General  
Treasury Inspector General for  
Tax Administration

Mary Mitchelson  
Acting Inspector General  
Department of Education

Patrick O'Carroll  
Inspector General  
Social Security Administration

## Feature Article

### 1 The IG Reform Act and the New IG Council-Dawn of a New Era

Phyllis Fong discusses the IG Reform Act, the new Council, and its effect on the future of government oversight.



## Oversight and Outreach

7 **Honest Services Fraud**  
Earl Devaney and James O'Sullivan examine honest services fraud and its effect on public corruption.

14 **Using Risk-Based Planning to Enhance Audit Impact**  
Gordon Milbourn, III and Mimi Sharkey look at a different approach to planning that could potentially enhance audit impact.

18 **How Legal Requirements Vary Depending on the Nature of the Business Entity Being Investigated**  
Thomas Coogan studies the different types of businesses and their relation to legal requirements.

24 **White Paper Tape Recording Interviews**  
Daniel Coney outlines the argument surrounding the tape recording of law-enforcement interviews.

30 **Postal Operations-Prelude to a Changing Audit Environment**  
Theodore Williams reviews a recent AFAA audit concerning postal operations in the Air Force.

34 **Managing Grants for Success**  
Elliot Lewis explores the challenges of managing grants designed for state and local governments.

39 **Department of Defense Fraud Awareness Initiatives**  
Frank Albright, Russel J. Geoffrey, and Lauren McLean summarize new fraud-related initiatives.

45 **Iraq's Inspectors General: A Work in Progress**  
Danny Athanasaw and Christopher M. Griffith provide insight into the struggles and improvements of the Iraqi Inspectors General.

50 **Hard Lessons: The Iraq Reconstruction Experience** Stuart W. Bowen, Jr. testifies before the Commission on Wartime Contracting on the lessons learned report from the Office of the Special Inspector General for Iraq Reconstruction.

58 **Immigration Enforcement and Social Security: The Inspector General Perspective**  
Patrick O'Carroll speaks regarding the connection between Social Security and immigration enforcement.

✂ Denotes the end of an article.



# The IG Reform Act and the New IG Council: Dawn of a New Era

Over the 30 year period the OIGs have been formally established by law, the community has evolved

**BY INSPECTOR GENERAL  
PHYLLIS K. FONG**

With the passage of the Inspector General Reform Act of 2008<sup>1</sup>, the inspector general community entered a new era in its 30-year existence. The new law has brought increased independence and concomitant levels of responsibility to the IGs, both individually and as a community. Since its birth in 1978, the community has evolved from an informal group of entities with similar missions into a formally-established organization with a mission that extends beyond the individual activities of its more than 67 Inspector General members. As a result of the Reform Act, the community is entering a period of organizational growth and maturity, with new opportunities to improve the effectiveness of federal programs.

This article will provide an overview of the Reform Act (legislative history and key provisions) and the creation of the new Council of Inspectors General on Integrity and Efficiency. As Chair of the Legislation Committee while the Reform Act was moving through Congress, and as the first elected Chairperson of CIGIE, I have had the privilege of working with the many people named in this article who have played a key role in bringing these efforts to fruition.

## LEGISLATIVE HISTORY

Until 2008, Congress had not made any significant revisions to the original Inspector General Act of 1978 since the 1988 Amendments were passed 20 years ago. IG Act reform initiatives, however, had been a matter of discussion and consideration since the mid-1990s, when Senator Susan Collins served as Chair of the Senate Governmental Affairs Committee (precursor to the current Homeland Security and Government Affairs Committee). During that time, Senator Collins introduced at least two bills to strengthen IG independence and authorities, but while these measures received some legislative attention they were never enacted. During that period, the IG community was organized to carry out its collective responsibilities through the two IG councils established by Executive Order, the President's Council on Integrity and Efficiency (composed of Presidentially Appointed, Senate confirmed IGs) and the Executive Council on Integrity and Efficiency (composed of



Designated Federal Entity IGs). The IG community recognized the need to participate actively and constructively in any efforts to amend and update the IG Act. The IG Reform Act of 2008 is the culmination of over seven years of effort by the IG community. Ken Mead (former Department of Transportation IG), during his tenure as PCIE Legislation Committee chair, started the process by surveying the community in 2000/2001 to determine the issues of highest concern/priority. Based on the survey results, the committee developed a package of proposals in anticipation of congressional interest in introducing legislation to mark the 25th anniversary of the original IG Act in 2003. During Russell George's (Treasury Inspector General for Tax Administration IG) tenure as chair of the Legislation Com-

Designated Federal Entity IGs).

The IG community recognized the need to participate actively and constructively in any efforts to amend and update the IG Act. The IG Reform Act of 2008 is the culmination of over seven years of effort by the IG community. Ken Mead (former Department of Transportation IG), during his tenure as PCIE Legislation Committee chair, started the process by surveying the community in 2000/2001 to determine the issues of highest concern/priority. Based on the survey results, the committee developed a package of proposals in anticipation of congressional interest in introducing legislation to mark the 25th anniversary of the original IG Act in 2003. During Russell George's (Treasury Inspector General for Tax Administration IG) tenure as chair of the Legislation Com-

mittee, Congress held hearings on IG community activities and actively considered some of the legislative proposals that had been developed, particularly by Rep. Jim Cooper. In subsequent years, Nikki Tinsley (former Environmental Protection Agency IG), while chair of the PCIE Human Resources Committee, took the lead in developing a strategy to address IG salary and bonus issues.

This preparatory work came to fruition when the 110th Congress convened in 2007. Changes in congressional leadership brought an increased emphasis on oversight and accountability, with more focus given to the activities of IGs individually and as a community.

Building on the work that had been done since 2000, Rep. Jim Cooper, Sen. Collins, and Sen. Claire McCaskill each introduced bills that addressed or included proposals developed by the IG community.

These members, working closely with Chairmen Henry Waxman (House Oversight and Government Reform Committee), Joe Lieberman (Senate HSGAC), and Edolphus Towns (House Government Management, Organization, and Procurement Subcommittee), championed the Reform Act proposals through the legislative process.

Hearings were held in both Houses, Administration concerns were addressed, and ultimately H.R. 928 was enacted by the Congress with no opposing votes in September 2008.<sup>2</sup> President Bush signed the Inspector General Reform Act of 2008 into law on October 14, 2008. (Public Law 110-409)

<sup>2</sup> H.R. 928, Improving Government Accountability Act, originally passed the House on Oct. 3, 2007, by a vote of 404-11. S. 2324, Inspector General Reform Act of 2007, passed the Senate on April 23, 2008 by unanimous consent. Both Houses of Congress worked together to reconcile the two bills into a final version of H.R. 928, renamed the Inspector General Reform Act of 2008. Final approval occurred in the Senate on September 24, 2008, by unanimous consent. This was followed by House action on September 27, 2008, by a vote of 414-0.

## DUTIES OF THE COUNCIL



- Reviewing areas of vulnerability to fraud, waste, and abuse in federal programs
- Developing coordinated government-wide activities to address these problems and promote effectiveness, including interagency projects to deal with problems that exceed the jurisdiction or capability of an individual agency
- Developing policies to maintain well-trained, highly skilled OIG staff
- Maintaining an internet website and other electronic systems to benefit all IGs
- Maintaining one or more professional training academies for IG personnel
- Submitting recommendations of individuals for vacant IG positions to the appointing authorities
- Making reports to Congress as necessary or appropriate
- Performing other duties within the Council's authority and jurisdiction

**KEY PROVISIONS OF THE LAW**  
The IG Reform Act contains a variety of provisions designed to enhance IG independence and accountability. Some highlights of H.R. 928 are:

IG Appointment and Qualifications requires that DFE IGs be appointed without regard to political affiliation, based on integrity and demonstrated professional ability.

Removal of IGs requires the President (for PAS IGs) or agency head (for DFE IGs) to give Congress 30 days advance notice before removing or transferring an IG. Notice must include the reason for the action.

IG Pay sets pay for PAS IGs (and SIGAR, SIGIR, CNCS, and CIA) at level three of the executive schedule, plus three percent. Requires that DFE IGs be classified at or above the majority of the DFE's senior level executives and their pay be not less than the average total compensation (including bonuses) of DFE senior level executives calculated on an annual basis.

Cash Bonus or Awards prohibits IGs from receiving cash awards or cash bonuses.

Separate Legal Counsel provides that each PAS IG shall obtain legal advice from a counsel reporting directly to an IG. Each DFE IG shall appoint a counsel, or obtain advice from a counsel reporting directly to an IG or from CIGIE staff.

Council of the Inspectors General on Integrity and Efficiency establishes a unified council of IGs, merging the two councils (PCIE and ECIE) previously established by executive order. CIGIE's mission is to address integrity, economy, and effectiveness issues that transcend individual government agencies; and to increase the professionalism and effectiveness of OIG personnel by developing approaches to establish a well-trained and highly skilled workforce. Membership includes PAS, DFE, and Legislative Branch IGs, as well as other officials.

The OMB Deputy Director for Management serves as Executive Chairperson, with a Chairperson elected from the IG members and an appointed Vice Chairperson.

Various funding mechanisms are au-

thorized for council activities, including interagency funding and use of a revolving fund. The Integrity Committee is now established by statute; its membership and jurisdiction are expanded to include being responsible for receiving, reviewing and reserving for investigation, allegations of wrongdoing against an IG and certain staff. It also must adopt new procedures and provide expanded information and reports to Congress.

## UNDER THE ACT

Changes to the IG budget request process under the Act:

- Each IG shall transmit a budget request to his/her agency head that specifies funds needed to operate, to meet all training needs (including IG certification that the request satisfies all training requirements), and to support CIGIE (these resources must be specifically identified and justified).
- Each agency head shall transmit a proposed budget to the President that includes an aggregate amount for the IG, amounts for IG training, amounts to support CIGIE, and any IG comments on the proposal.
- The President shall include in his budget request a separate statement of the budget estimate for each IG, the amount requested for each IG, the amount requested for training for IGs, the amount requested to support CIGIE, and any comments from an IG who believes that the president's request would substantially inhibit him/her from performing IG duties.

Subpoena Power clarifies that IG subpoena power extends to electronically stored information.

Program Fraud Civil Remedies Act adds DFE IGs to the list of entities that are covered by the PFCRA.

Law Enforcement Authority allows DFE IGs to apply for statutory law enforcement authority.

Semiannual Reporting Requirements makes IG inspection and evaluation reports subject to the requirements.

OIG Web sites requires that each agency homepage contain a direct link to the OIG Web site; each IG must post on its Web site, within three days, each publicly available report or audit; and each IG must maintain a direct link on its web site for individuals to report fraud, waste, and abuse.

Other Administrative Authorities provides IGs with additional expanded personnel authorities. Generally, each OIG is considered a separate agency and each IG is considered an agency head or appointing authority with respect to the following administrative authorities:

- *Voluntary Separation Incentive Payments:* IGs can now apply directly to OPM for the authority to offer voluntary separation incentive payments or "buyouts" within their own OIG.
- *Voluntary Early Retirement Authority:* IGs can now request directly from OPM the authority to offer early retirement to their employees.
- *Mandatory Retirement for Law Enforcement Officers:* Each IG now has authority to exempt a law enforcement officer from mandatory retirement up to the age of 60, if in his or her judgment the public interest so requires.
- *Reemployed Annuitants:* IGs can now go directly to OPM to request a waiver of the provision requiring that a retiree's pay be reduced by the amount of his/her annuity upon rehire by the government (for employees in positions for which there is exceptional difficulty in recruiting or retaining a qualified employee); and request authority to waive the pay reduction provisions for employees/retirees serving on a temporary basis (during the time an emergency involving a direct threat to life or property or other unusual circumstances exist).
- *SES Provisions.* Generally, IGs are considered to be agency heads and OIGs are considered to be agencies for purposes of applying the various provisions of Title 5 pertaining to

SES employees. This will have wide-ranging implications for many IGs, authorizing them to deal directly with OPM, rather than through their agencies, on such issues as requests for SES positions, establishing SES appraisal systems, and setting SES pay and performance awards.

- *SES Rank Awards.* CIGIE is now considered to be an agency head for purposes of making recommendations to OPM for OIG SES employees to receive rank awards.

Taken as a whole, the Reform Act successfully addresses many issues of importance to the IG community and lays a solid foundation for the future.<sup>3</sup> The community owes a debt of gratitude to all who worked so hard and persevered over the many years that this legislation was in the making.

## TRANSITION TO THE COUNCIL OF INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

One of the most significant changes brought about by the IG Reform Act is the creation of a unified council of federal inspectors general. This seemingly simple measure has profoundly affected the way the community addresses issues, makes decisions, and, ultimately, is perceived by external parties.

Over the 30-year period that OIGs have been formally established by law, the community has evolved from a loose confederation of offices with common interests, to two separate councils established by presidential executive order, to a single unified body established by statute responsible to both Congress and the president.

<sup>3</sup> Several issues were considered by one or both Houses but were not enacted in the final bill, due to the need for more time to thoroughly consider the proposal or member concerns. Examples include enhanced computer matching authority for OIGs, new authority for compelled interviews, expanded contracting authority, exemption of OIG activities from Paperwork Reduction Act requirements, and specific provisions affecting individual OIGs. To the extent that the IG community sees a continuing need for these measures, the opportunity exists to work productively with the Congress.



Leaders in the community recognized early on that significant advance planning would be necessary to ensure a smooth transition to a unified council should the reform legislation be enacted by Congress. The PCIE Executive Council appointed a Transition Planning Committee composed of four PCIE and four ECIE members and co-chaired by Earl Devaney and myself.<sup>4</sup> This committee began its work in January 2008 when it appeared that passage of some form of IG Act legislation would be likely during the 110th Congress.

Working through the spring and summer of 2008, the committee developed recommendations on such matters as elections, committee structure, voting, funding, and transition process. Members prepared a draft charter and organization chart, recognizing that revisions would be necessary to reflect the final version of enacted legislation. Throughout this process, the committee met frequently and considered a variety of perspectives on each issue before coming to consensus on its recommendations. A number of guiding principles were key to the committee's approach to its work:

- One IG, one vote – each IG would have an equal vote on CIGIE matters.
- The current PCIE/ECIE Executive Council would serve as the CIGIE governing body for 6 months after the law was enacted.
- The current committee chairs and committee structure would remain in place for six months after the law was enacted.
- CIGIE's first year budget and staff levels would remain consistent with the cost estimates developed by the Congressional Budget Office.

As a result of this Committee's work, the IG community was well prepared to handle the transition to a unified council upon enactment of the reform legislation in October 2008. Within a matter of

<sup>4</sup> Committee members are Jack Callendar (PRC), Carl Clinefelter (FCA), Claude Kicklighter (succeeded by Gordon Heddell) (DOD), Lynne McFarland (FEC), Richard Moore (TVA), and David Williams (USPS).

weeks, an election (fittingly overseen by Lynne McFarland, FEC IG) was held for the first CIGIE chairperson and the results were announced in mid-November. In November and December, the PCIE and ECIE held their last meetings as separate councils, recognized the leadership of their outgoing Chair and Vice-chairs, and briefed incoming CIGIE leaders and staff on continuing matters of interest.<sup>5</sup>

### CIGIE TODAY

January 2009 represented the start of a new era in the life of the IG community. It is a time of change in many arenas – a new Congress, a new presidential administration, a new council. Building on the successes and lessons learned over 30 years, the new council is moving forward rapidly.

The first CIGIE meeting was held in January 2009 under my leadership and that of Vice-Chairperson Carl Clinefelter (FCA).<sup>6</sup> The Executive Council presented the proposed Charter, the draft Strategic Business Plan, and the Transition Planning Committee's recommendations (many of which had already been addressed in the Charter and Business Plan); after discussion and comment, the Charter and Business Plan were formally adopted at CIGIE's February meeting.<sup>7</sup>

The Executive Council continues to work hard to implement the IG Reform Act's provisions and CIGIE's implementing initiatives. Executive Council members represent a broad spectrum of CIGIE's membership and include PAS IGs, DFE IGs, and a Legislative Branch IG.<sup>8</sup>

<sup>5</sup> The Councils have been well-served by the many contributions of their outgoing leaders: Clay Johnson, former OMB DDM and Chair of both the PCIE and ECIE; Gregory Friedman (DOE), PCIE Vice-Chair; and Tina Boesz (former NSF IG), ECIE Vice-Chair.

<sup>6</sup> By statute, OMB's DDM serves as Executive Chairperson of CIGIE. The Council looks forward to working closely with a new DDM upon his/her appointment and confirmation.

<sup>7</sup> Both of these documents are available on IGMET, the IG community's website.

<sup>8</sup> Executive Council members currently are Earl Devaney (DOI), Gregory Friedman (DOE), Gordon Heddell (DoD), Dan Levinson (HHS), Lynne McFarland (FEC), Patrick O'Carroll (SSA), Tony Ogden (GPO), and Jon Rymer



This is critical to ensuring that a variety of perspectives are considered whenever issues involving the community must be addressed.

The charter adopted by CIGIE addresses governance matters - how CIGIE will do its business. It incorporates provisions of the IG Reform Act and adds policies and procedures where necessary to enable CIGIE to carry out its activities. Key provisions address:

- Conduct of elections
- Preparation of strategic and business plans
- Developing meeting agendas and obtaining quorums
- Voting procedures
- Funding mechanisms
- Budget preparation and execution
- Committee structure, leadership, and membership
- Procedures to amend the charter

The strategic business plan sets forth the council's business goals, supporting objectives, and performance measures for the first two years of its operation. It builds on the strategic mission set forth in "A Strategic Framework 2005-2010," adopted by the IG community in 2004, as well as the more recent mission statement contained in the IG Reform Act. The plan established three goals aimed towards establishing CIGIE as a major contributor to government-wide integrity and efficiency.

(FDIC).





The plan includes objectives and timeframes designed to enable the community to accomplish these goals by December 2010. These three goals are:

1. Contribute to government-wide improvements in program integrity, efficiency, and cost-effectiveness by providing cross-agency analysis of OIG findings and recommendations in areas of vulnerability confronting multiple government programs.
2. Increase the professionalism and effectiveness of the IG community workforce.
3. Create an effectively functioning council able to meet its vision, mission, and goals.

The first goal recognizes that the council's success will be judged by administration and congressional stakeholders largely on the council's ability to contribute to improvements in federal operations. To accomplish this, the council will annually identify and perform at least two cross-cutting studies or combined meta analyses of work performed by OIGs in their individual agencies.

The second goal focuses on the continuing need to provide excellent professional development and training to OIG employees. To achieve this goal, the council will establish a community-wide academy(ies) to present high quality and cost-efficient training to audit, investigative, inspection/evaluation, management, and other professional staff.

Finally, and equally as important as the first two goals, the third goal recognizes the need to permanently establish an effective organization to enable CIGIE to carry out its statutory responsibilities. Activities under this goal include administrative operations (developing staffing, funding, and accountability plans; obtaining space, facilities, and equipment; and setting up a revolving fund and accounting procedures) and planning and organization activities (updating committee structure, membership, and charters; and revising strategic and planning documents).

In addition to these three overarching goals, CIGIE leaders and staff deal on a daily basis with the ongoing business of any federal entity: responding to congressional, media, and public requests; handling member IG inquiries; and coordinating council activities with other federal entities such as GAO, OMB, and OPM.

In this last arena, particularly noteworthy is the work being done by the IG Candidate Recommendation Panel, co-chaired by Glenn Fine (DOJ) and Lynne McFarland (FEC), to fulfill CIGIE's statutory responsibility to identify and provide qualified candidates for vacant IG positions.

## CONCLUSION

As this article goes to press, the IG community has had three months of active operation under the umbrella of a unified council. The transition has been smooth, due in large part to the vision and care of many dedicated IGs and the professionalism and expertise of leaders from the ranks of the career OIG staff.<sup>9</sup>

Perhaps the most noteworthy aspect of this transition has been the apparent

ease with which the community has begun to see itself as one entity, with a focus on the common challenges and types of work each individual IG experiences. We are a stronger community, close-knit and better situated to face the challenges ahead. It has become clear that we as IGs have much more in common with each other than we have differences.

Although we cannot predict the challenges to come, history tells us that there will indeed be opportunities for the IG community to play a key role in assuring government effectiveness. The current economic crisis has led to enactment of historic legislation intended to spur recovery in key sectors of the American economy.

The IG community's current challenge, then, is to oversee the stimulus spending provided under the American Recovery and Reinvestment Act of 2009.<sup>10</sup>

OIGs have been given a very visible role in providing oversight of funds under ARRA, both in terms of membership on the newly-created Recovery and Accountability Transparency Board,<sup>11</sup> and in terms of the funding given to 23 specified IGs to provide oversight in their own agencies. ARRA has brought new visibility and recognition to the IG community; it also shines a spotlight on our ability to devise proactive and effective ways to ensure that funds are spent well.

I am confident that, working together, the IG community will continue to do an outstanding job to better the delivery of government programs and improve the lives of our citizens. ✎

<sup>9</sup> The accomplishments discussed in this article would not have been possible without the professional expertise and assistance of so many dedicated OIG career employees. I regret that it is not possible to name them all here. I am personally indebted to USDA OIG's outstanding staff, particularly David Gray, Mark Jones, Kathleen Tighe, and Cheryl Viani, who have directly managed PCIE Legislation Committee and CIGIE activities.

<sup>10</sup> P.L. 111-5, signed by President Obama on February 17, 2009.

<sup>11</sup> The Board is chaired by Earl Devaney (former DOI IG) and is composed of 10 IGs named in the ARRA: Agriculture, Commerce, Justice, Energy, Homeland Security, Health and Human Services, Education, Transportation, Treasury, and Treasury IG for Tax Administration.



# Phyllis K. Fong

**Phyllis K. Fong** was sworn in as Inspector General for the U.S. Department of Agriculture on December 2, 2002. USDA is one of the largest and most diverse departments in the federal government. Its mission includes the management of traditional farm programs, private lands conservation, domestic food assistance, agriculture research and education, agricultural marketing, international trade, meat and poultry inspection, forestry, and rural development programs.

As Inspector General, Ms. Fong is the senior official responsible for audits, evaluations, investigations, and law enforcement efforts, relating to USDA's programs and operations. The Office of Inspector General provides leadership in promoting economy, efficiency, and effectiveness in USDA programs and addressing fraud, waste, and abuse.

Ms. Fong was recently elected as the first Chair of the Council of Inspectors General on Integrity and Efficiency, which was established by the Inspector General Reform Act of 2008, Public Law 110-409, to consolidate the former President's Council on Integrity and Efficiency and Executive Council on Integrity and Efficiency. CIGIE's members include 67 federal Inspectors General, and its mission is to promote economy and effectiveness in federal programs through coordinated governmentwide activities. Previously, Ms. Fong served as Chair of the PCIE Legislation Committee and was a member of the PCIE Audit Committee. She also served as PCIE representative to the Comptroller General's Advisory Council on Government Auditing Standards.

Prior to her appointment at USDA, Ms. Fong served as the Inspector General of the U.S. Small Business Administration from April 1999 until December 2002. A career member of the Senior Executive Service, she had also held several positions at SBA OIG, including Assistant Inspector General for Management and Legal Counsel (1994-1999) and Assistant Inspector General for Management and Policy (1988-1994). She also served as Assistant General Counsel for the Legal Services Corporation (1981-1983) and as an attorney with the U.S. Commission on Civil Rights (1978-1981).

Ms. Fong graduated from Pomona College with a B.A. degree in Asian studies and earned her J.D. degree from Vanderbilt University School of Law. Ms. Fong is a member of the Tennessee and District of Columbia bars.

[PUBLIC CORRUPTION]

# Honest Services Fraud

## A modern tool for dealing with federal public corruption cases

BY INSPECTOR GENERAL  
EARL DEVANEY AND JAMES  
P. O'SULLIVAN

The versatile “honest services” fraud statute makes it a crime to devise a “scheme or artifice to deprive another of the intangible right of honest services.”<sup>1</sup> A recent series of high-profile convictions illustrates the effectiveness of this statute as a modern tool for dealing with federal public corruption cases. For example, on September 29, 2008, former Central Intelligence Agency Executive Director Kyle “Dusty” Foggo pleaded guilty to honest services fraud for having fraudulently deprived the U.S. of its right to his honest services as a public official. The basis for the charge was that Mr. Foggo had abused his high-ranking position by devising and executing a scheme to induce the CIA into hiring “companies and individuals with whom he had concealed his personal relationships.”<sup>2</sup>

Another high-profile example of the use of the honest services fraud statute is that of former federal lobbyist Jack Abramoff. Mr. Abramoff pled guilty to



honest services fraud<sup>3</sup> and conspiracy to commit honest services fraud, stemming from his extensive efforts to induce public officials to take improper action on behalf of his clients.<sup>4</sup> As a result of the Abramoff investigation – and illustrating the substantial reach of the statute – a U.S. Congressman<sup>5</sup> and four former senior Congressional staff members<sup>6</sup>

subsequently pled guilty to conspiracy to commit this crime.

The honest services fraud statute has been useful not only in prosecuting public corruption cases of national significance, but also in dealing with more common corruption cases such as government procurement fraud. For example, in March 2007, a government contractor pleaded guilty to honest services fraud in connection with a scheme to steer government contracts at Walter Reed Army Medical

1 The Honorable Earl E. Devaney is the Inspector General of the Department of the Interior. James P. O’Sullivan is a former Associate General Counsel of the Office of Inspector General, Department of the Interior. The authors thank Chris Martinez, Attorney Advisor, Office of Inspector General, Department of the Interior, for his assistance in preparing this article. “The views of co-author James P. O’Sullivan reflect his personal views and do not necessarily reflect the views of the Department of Justice.”

2 DOJ press release, “Former CIA Executive Director Kyle ‘Dusty’ Foggo Pleads Guilty to Defrauding the United States” (Sept. 29, 2008) available at <http://sandiego.fbi.gov/dojpressrel/pressrel08/sd092908.htm>.

3 In January 2006, Jack A. Abramoff pleaded guilty to a number of charges including honest services fraud and conspiracy to commit honest services fraud.

4 Richard B. Schmitt, “Jack Abramoff Sentenced to 48 Months,” L.A. Times (Sept. 5, 2008), available at <http://articles.latimes.com/2008/sep/05/nation/na-abramoff5>.

5 In September 2006, Congressman Robert W. Ney, pleaded guilty to, among other things, conspiracy to commit honest services fraud.

6 Tony C. Rudy, a former member of the staff of Congressman Tom DeLay, pleaded guilty in March 2006 to conspiracy to defraud the citizens of the United States and the United States House of Representatives of the right to his honest ser-

vices. Neil G. Volz, a former member of the staff of Congressman Robert W. Ney, pleaded guilty in May 2006 to conspiracy to commit honest services fraud. William J. Heaton, a former member of the staff of Congressman Robert W. Ney, pleaded guilty in February 2007 to conspiracy to commit honest services fraud. Mark D. Zachares, a former senior staffer to the House Transportation and Infrastructure Committee, pleaded guilty in April 2007 to conspiracy to commit honest services fraud.



Center.<sup>7</sup> Moreover, the ongoing National Procurement Fraud Initiative, announced by the DoJ in October 2006,<sup>8</sup> has yielded convictions and indictments under the honest services fraud statute. In December 2006, a federal jury in U.S. District Court Western District of Virginia convicted a U.S. Army procurement official and the chief executive officer of a Defense contractor of two counts each of honest services wire fraud, and one count each of bribery.<sup>9</sup> In June 2007, DoJ announced the guilty plea of a former DoD civilian employee that included one count of honest services wire fraud related to a scheme to obtain unauthorized pay and entitlements.<sup>10</sup>

While these cases show that the honest services fraud statute is indeed an effective 21st century tool for dealing with public corruption, the statute's ancestry goes back to the 19th century when the original mail fraud statute was enacted to protect the federal mails. Over the course of the next 100 years, the theory of honest services fraud developed in case law interpreting the mail and wire fraud statutes and emerged as a powerful doctrine in the 1970s, supporting public corruption prosecutions of state, local and federal officials.<sup>11</sup>

In 1987, however, the U.S. Supreme Court's *McNally* decision held that the mail and wire fraud statutes applied only

to the defrauding of a property interest, and did not apply to defrauding the government and citizens of their intangible right to the honest services of public officials.<sup>12</sup> Congress responded swiftly to this decision, and in 1988 enacted 18 U.S.C. § 1346, a definitional provision of the mail and wire fraud statutes that expressly covers a scheme or artifice "to deprive another of the intangible right of honest services".<sup>13</sup> Since 1988, the honest services fraud statute has been applied in a wide variety of factual circumstances and has proven to be a flexible tool in dealing with public corruption.

### THEORY AND ELEMENTS OF HONEST SERVICES FRAUD

Although section 1346 is subtle in its application and can raise nuances of legal interpretation, the basic theory behind it is straightforward and intuitive, especially in cases involving federal government officials.<sup>14</sup> A federal government employee takes an oath to support and defend the Constitution and to faithfully discharge the duties of public office. The federal government, the employing agency and citizens in general have a right to the honest services of every federal employee who undertakes that public trust. The right to honest services includes the right to the conscientious,

12 *McNally v. U.S.*, 483 U.S. 350 (1987).

13 The full text of 18 U.S.C. § 1346 states: "For the purposes of this chapter, the term 'scheme or artifice to defraud' includes a scheme or artifice to deprive another of the intangible right of honest services." A scheme or artifice to defraud using the mail is proscribed by 18 U.S.C. § 1341. Wire fraud is proscribed by 18 U.S.C. § 1343.

14 The statute has a somewhat more controversial history when applied in an exclusively private sector scheme. Some cases involving only private parties have encountered resistance from courts and criticism from commentators who have expressed concerns that the statute may be criminalizing conduct that amounts to no more than a civil fraud or perhaps only a breach of contract. The statute has also generated criticism on federalism grounds when applied to corruption of state or local officials. Commentators have generally taken a more favorable view of the statute when a federal interest is at stake or the conduct involves a federal official, although some have nevertheless criticized the statute as inherently vague.

loyal, faithful, disinterested and impartial service of federal employees.<sup>15</sup>

Whenever a federal employee engages in deceit, fraud, bias, undue influence, conflict of interest, self-enrichment, self-dealing and concealment, he or she commits a serious breach of public trust and, depending on the facts, may become criminally liable under the honest services fraud statute. The statute also applies to other persons who are not federal employees who deprive the government and its citizens of the honest services of federal officials.

Four elements must be established in order to prove honest services fraud in a federal government context: the defendant must knowingly devise or participate in a scheme to defraud the government or the public of its right to honest services; the falsehood at the heart of the scheme must be material; there must be a specific intent to defraud; and there must be use of the mails or a transmission by wire, radio or television in interstate commerce.

As regards the first element, the government generally must prove that the scheme would likely compromise governmental objectivity and fairness.<sup>16</sup> This often means that the scheme centered on a particular, discretionary decision or set of decisions.<sup>17</sup> The courts, however, courts have held that there is no requirement that an official actually ren-

15 The statute does not define the term "honest services." A bill, S. 2559, introduced by Senator Leahy in the 109th Congress contained the following definition of the term: "The term 'honest services' includes the right to the conscientious, loyal, faithful, disinterested, and unbiased service, to be performed free of deceit, undue influence, conflict of interest, self-enrichment, self-dealing, concealment, bribery, fraud, and corruption."

16 E.g., *U.S. v. Hasner*, 340 F.3d 1261, 1271 (11th Cir. 2003) (discussing public officials' fiduciary duty to the public to be open and act in their best interests, and how the public's right to honest services is harmed when those duties are breached).

17 E.g., *id.* at 1265-68 (Chairman of county housing agency convicted of committing honest services mail fraud by voting on a government contract in order to directly benefit a private party with whom he had an agreement to share the resulting commission).



der any biased or impartial decisions; it is enough that an official failed to disclose information material to his or her duties, such as a conflict of interest.<sup>18</sup>

The second honest services fraud element is that the fraudulent scheme must involve a material deception by the accused official. Even though the word “materiality” appears nowhere in 18 U.S.C. §§ 1341, 1343, or 1346, the Supreme Court established that these and similar statutes inherently adopted the common law meaning of fraud, which had always “required a misrepresentation or concealment of material fact.”<sup>19</sup> In a nutshell, a material misrepresentation or concealment is one that has “a natural tendency to influence . . . the decision of the decision making body to which it was addressed.”<sup>20</sup>

The third element requires that the defendant have specific intent to defraud. This means not only that the official was aware of the scheme, but that he or she willfully intended for it to harm governmental honesty and fairness. Such intent may be proven by circumstantial evidence. No direct admission is required, but the facts must be such that could lead a reasonable jury to conclude that the defendant did not act in good faith, but specifically intended to harm governmental objectivity and honesty.

The fourth and final element in an honest services mail fraud case is, of course, that the mails be used or caused

to be used in furtherance of the fraud. The mailing, however, does not have to be essential to the scheme, and the defendant need not be the one responsible for it. Also, the definition of “the mails” has been extended by statute beyond the U.S. Postal Service to include private and commercial carriers involved in interstate commerce, such as FedEx.

For honest services wire fraud charges, the fourth element requires that the defendant, in furthering his or her scheme to defraud, transmitted or caused the transmission of any writing, signal, or sound by means of a wire, radio, or television communication in interstate commerce. Typically, this includes email, fax, and telephone/cell phone communications, although the statutory terms invite further definition as technology continues to change and evolve. Moreover, as is also the case with mail fraud, the communication itself need not contain a fraudulent representation; it merely needs to “further” the scheme in some way, such as by arranging a meeting place or providing other information helpful to executing the scheme.

Within the broad parameters of these elements lies a vast spectrum of misconduct that can be covered by the honest services fraud statute. A scheme or artifice to defraud citizens and the government of the right to the honest services of public officials can take many forms. Some of the most common types of honest services fraud cases involving public officials include bribery schemes, undisclosed financial interest schemes, and schemes involving misappropriation of confidential information. It is important to keep in mind; however, that the honest services fraud statute is flexible enough to embrace any scheme to defraud that comes within its limits.

In many cases, the honest services fraud statute is used in conjunction with other criminal statutes, such as those proscribing bribery, illegal gratuities or other conflicts of interest. Consequently, the facts that would support those violations will often also support an honest services fraud case. On the other hand, there

may be cases where the facts would not establish all the required elements of a conflict of interest crime but would be sufficient to establish an honest services fraud violation.

## BRIBERY SCHEMES

Many honest services fraud cases strongly resemble bribery or illegal gratuity cases. For example, in a number of the honest services fraud cases arising out of the Abramoff investigation, there was a scheme or artifice to defraud that consisted of the defendant accepting (as a public official) or providing (as a lobbyist) a “stream of things of value” (e.g., domestic and overseas trips, golf, entertainment, meals and drinks, employment opportunities, etc.) to influence or reward official action. In the case of the government officials, they agreed “to take a stream of favorable official action” (e.g., making certain contacts with executive branch officials, inserting legislative amendments, etc.).

Such cases, even when they do not include a bribery count, nevertheless have a strong bribery-like quality to them.<sup>21</sup> Unlike the bribery statute, however which requires an explicit quid pro quo or a showing that the giving of things of value was intended to induce a pattern of official actions (e.g., either “this for that” or “these for those”),<sup>22</sup> an honest services fraud case has no such requirement.

<sup>21</sup> The Information and Plea Agreement in the case of Congressman Robert W. Ney did not contain a bribery or illegal gratuity count.

<sup>22</sup> Section 201(b)(2) of Title 18, U.S. Code, states that whoever “being a public official . . . corruptly demands, seeks, receives, accepts . . . anything of value . . . in return for being influenced in the performance of any official act” shall be fined or imprisoned under the statute. (Emphasis added.) See also *U.S. v. Ganim*, 510 F.3d 134, 148-49 (2d Cir. 2007) (noting that “bribery can be accomplished through an ongoing course of conduct” if the gifts are being given in exchange for a course of official action); *U.S. v. Jennings*, 160 F.3d 1006, 1014 (4th Cir. 1998) (noting that “[t]he quid pro quo requirement is satisfied so long as the evidence shows a ‘course of conduct of favors and gifts flowing to a public official in exchange for a pattern of official actions favorable to the donor’”) (quoting *U.S. v. Arthur*, 544 F.2d 730, 734 (4th Cir. 1976)).

<sup>18</sup> See, e.g., *U.S. v. deVegter*, 198 F.3d 1324, 1328 (11th Cir. 1999) (noting that “[a] public official’s undisclosed conflict of interest . . . does by itself harm the constituents’ interest in the end for which the official serves—honest government in the public’s best interest”) (emphasis added); *U.S. v. Holzer*, 816 F.2d 304, 308 (7th Cir.) (holding that a judge’s receipt of bribes and “loans” to influence official actions constituted mail fraud irrespective of whether he ruled differently on any cases), vacated, 484 U.S. 807 (1987) (ordering reconsideration in light of *McNally*); *U.S. v. Sawyer*, 85 F.3d 713, 724 (1st Cir. 1996) (noting that “the public is deprived of its right . . . to disinterested decision making” when “an official fails to disclose a personal interest in a matter over which she has decision-making power”).

<sup>19</sup> *Neder v. U.S.*, 527 U.S. 1, 22 (1999).

<sup>20</sup> *Id.*

Nor, as is required under the illegal gratuity statute, is it necessary to show that a thing of value was given “for or because of an official act.”<sup>23</sup> Thus, instead of showing a specific link between a bribe or gratuity and some official action, in an honest services fraud case there is a showing of a “stream of things of value” and a corresponding “series of official acts.”

For this reason, it is useful to consider honest services fraud counts in cases that may initially be evaluated as a bribery or illegal gratuities case. Especially since the Supreme Court’s *Sun-Diamond*<sup>24</sup> decision which required a strong link to some official action in gratuities cases, the honest services fraud theory may provide a useful alternative to a bribery or illegal gratuity charge.

For example, in the *Woodward* case involving a Massachusetts state legislator, the Court held that an honest services violation may be established where there is a showing of a “generalized pattern of gratuities to coax favorable official action.”<sup>25</sup> As the Court further explained, “[a] person might not, however, give an unlawful gratuity with the intent to effect a specific quid pro quo. Rather, as the government contends here, a person with continuing and long-term interests before an official might engage in a pattern of repeated, intentional gratuity offenses in order to coax ongoing favorable official action in derogation of the pub-

lic’s right to impartial official services.”<sup>26</sup>

Kickback schemes, close relatives of bribery schemes, have also been prosecuted under the honest services fraud statute. One example of a kickback scheme is the arrangement engineered between Jack Abramoff and Michael Scanlon. Abramoff recommended to his Native American tribal clients that they use the grassroots and public relations services provided by Scanlon’s firm. Abramoff did not disclose to his clients that he had an arrangement with Scanlon to receive fifty percent of the net profits of the fees paid to Scanlon’s firm. In the words of the plea agreement, this scheme violated Abramoff’s “duty to disclose all relevant facts to his lobbying clients, including conflicts of interest and any financial interest in fees paid to others.”<sup>27</sup>

#### UNDISCLOSED FINANCIAL INTEREST SCHEMES

A second type of honest services fraud case involves schemes in which a public official has an undisclosed financial interest and takes some official action or uses public office to benefit a secret financial interest. Section 1346 has been regularly used to successfully prosecute state and local public officials in this type of case.<sup>28</sup>

Although the honest services fraud statute has been less frequently used to prosecute federal officials for undisclosed, conflicting financial interests, one notable federal case involved a scheme by two U.S. Department of the Treasury officials to use their access to the govern-

ment procurement process to channel money to themselves and their companies.<sup>29</sup> The scheme involved the use of no-bid contracts to a third-party contractor who provided financial benefits to the Treasury officials. The two officials were convicted of honest services wire fraud violations. They also were convicted of violations of 18 U.S.C. § 208 which bars an executive branch employee from taking action on a matter that could affect the employee’s financial interest.

Another federal case of this type involved an Assistant U.S. Attorney who engaged in a scheme to make favorable recommendations to the court and others on behalf of cooperating witnesses and defendants in exchange for money.<sup>30</sup> In one instance, the AUSA accepted \$98,000 from a cooperator. In return, the AUSA argued for leniency at a sentencing hearing. The AUSA pled guilty to two counts of honest services wire fraud and one felony conflict of interest count under 18 U.S.C. § 208.

There may be a number of reasons why the honest services fraud statute is not used more frequently in federal prosecutions involving conflicting financial interests on the part of federal officials. In some cases, there may not be any element of concealment and hence no “scheme or artifice” as required under the mail and wire fraud statutes. For example, in cases where federal employees have acted on matters that would affect a company with which they were negotiating for employment or had an arrangement for future employment, the employee may have made no attempt at concealment. In some cases of an inadvertent section 208 violation, the conflicting financial interest may even have been reported on a financial disclosure report. A more likely explanation for the paucity of federal cases of this type, however, is that

29 *U.S. v. Quinn*, 359 F.3d 666 (4th Cir. 2004). For additional facts in this case, see Case 1 in the 2002 Conflict of Interest Prosecution Survey, issued by the Office of Government Ethics on October 31, 2003.

30 See Case 3 in the 1997 Conflict of Interest Prosecution Survey, issued by the Office of Government Ethics on March 13, 1998.

23 For example, 18 U.S.C. § 201(c)(1)(B) states that whoever “being a public official . . . demands, seeks, receives, accepts . . . anything of value . . . for or because of any official act performed or to be performed by such official or person” shall be fined or imprisoned under the statute.

24 In *U.S. v. Sun-Diamond Growers*, 526 U.S. 398 (1999), the Supreme Court ruled that in an illegal gratuity case it was necessary to show that the gratuity was linked to some specific official act taken by the public official. One current legislative proposal seeks to expand the scope of the illegal gratuity statute by amending the statutory definition of “official act” to include “any decision or action within the range of official duty of a public official.” See H.R. 2438, “Clean Up Government Act of 2007,” 110th Cong., 1st Sess. (introduced May 22, 2007).

25 See *U.S. v. Woodward*, 149 F.3d 46, 55 (1st Cir. 1998), cert. denied, 525 U.S. 1138 (1999).

26 *Id.*

27 See Factual Basis for the Plea of Jack A. Abramoff at p. 3.

28 See *U.S. v. Mittelstaedt*, 31 F.3d 1208 (2d Cir. 1994), cert. denied, 513 U.S. 1084 (1995) (consultant employed by two towns to advise on zoning and planning matters had undisclosed interest in certain real estate projects); *U.S. v. Bissell*, 954 F. Supp. 841 (D.N.J. 1996), judgment aff’d. without opinion, 142 F.3d 429 (3d Cir. 1998) (local prosecutor shared a partnership interest in gasoline stations with attorney who represented adversaries of the prosecutor’s office); *U.S. v. Grandmaison*, 77 F.3d 555 (1st Cir. 1996) (part-time city alderman secretly influenced the award of a contract to a construction company that was his employer).

section 208 is itself an adequate tool for dealing with employees who act on matters that benefit their own financial interest, whether or not that interest is concealed.<sup>31</sup>

There are some situations, however, not covered by section 208, that may justify use of the honest services fraud statute. Section 208 covers the financial interests personally owned by the federal official; it also covers certain other so-called “imputed interests” that constitute a conflict for an official, such as the financial interests held by a spouse or a minor child. But section 208 does not cover the financial interests of other close relatives such as a sibling, a parent, or an uncle or aunt.<sup>32</sup> It also does not cover the financial interests of a “significant other” or “live-in partner.”

So, for example, if instead of a steering a contract to a company owned by a spouse (which would violate section 208), the official directed the contract to a company owned by a brother or a member of the official’s immediate household, section 208 would not apply. In these situations, the honest services fraud statute may be a useful alternative to a section 208 prosecution. The honest services fraud statute could apply if there was a scheme to steer the contract to a brother, an in-law or some other family member whose financial interests are not covered by section 208.

## MISAPPROPRIATION OF CONFIDENTIAL INFORMATION SCHEMES

A third type of honest services fraud case is one where the dominant facts involve a misappropriation of confidential information. It is well established that the misappropriation of confidential infor-

31 For those employees who are required to file either a public or confidential financial disclosure report, the failure to report a financial interest could violate both civil and criminal statutes.

32 The Standards of Conduct attempt to address this problem on an administrative level by requiring officials to consider recusal from matters that would affect the financial interest of other close relatives or members of their household. See 5 C.F.R. § 2635.502.

mation, whether it be government information or business information, can constitute a violation of the mail and wire fraud statutes. Even prior to the enactment of the honest services fraud statute, the Supreme Court in *Carpenter* upheld the conviction of a Wall Street Journal reporter who used nonpublic business information to make money trading in the stock market.<sup>33</sup>

Many honest services fraud cases involving public officials engaged in bribery or undisclosed financial interest schemes have elements that involve the misuse of nonpublic government information. One honest services fraud case in which misappropriation of government information was at the heart of the case was *United States v. Czubinski*.<sup>34</sup>

Richard Czubinski was employed by the Internal Revenue Service in the Boston office of the Taxpayers Services Division. In order to carry out his official duties, which included answering taxpayer questions regarding their returns, Czubinski was authorized to have access to the IRS’s Integrated Data Retrieval System. His authorization was limited to answering taxpayer inquiries, but Czubinski browsed the database and conducted searches that were outside the scope of his official duties.

The government indicted Czubinski on nine counts of honest services wire fraud and four counts of computer fraud. A jury convicted Czubinski on all counts. On appeal, the First Circuit reversed Czubinski’s conviction on all counts. With respect to the honest ser-

33 See *Carpenter v. U.S.*, 484 U.S. 19 (1987).

R. Foster Winans was a reporter for the Wall Street Journal who wrote a daily column called “Heard on the Street” which evaluated stock based on business information that he gathered in the course of his work for the newspaper. The column had an impact, although hard to calculate, on the stocks that it discussed. Winans conspired with Carpenter and others in a scheme to provide advance information that would later appear in the columns and to trade in stock on the basis of this advance information. In addition to various securities laws violations, Winans was convicted of honest services fraud.

34 See *U.S. v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997).

vices fraud counts, the Court held that the unauthorized browsing of confidential taxpayer information did not, standing alone, deprive the government of his honest services as a federal employee.

The Czubinski decision provides useful guidance as to what would be needed to successfully establish an honest services fraud case involving a scheme to misappropriate confidential government information. The First Circuit acknowledged that the government had established that the defendant engaged in unauthorized searches of taxpayer information using interstate wire transmissions (the database was in Martinsburg, West Virginia). The court, however found that the government did not establish that the defendant had received any tangible benefit from his misuse of his position. The court thus determined that the case “falls outside of the core of honest services fraud precedents”<sup>35</sup> in that it did not involve bribery, embezzlement of some other serious breach of public trust. In this regard, the First Circuit took special note of the fact that the defendant’s duties were ministerial (responding to taxpayer requests for information about their own returns) and did not involve a discretionary, decision-making role. Finally, the court said that the government failed to prove the intent to deprive the public of the defendant’s honest services, since it did not establish that Czubinski intended to use the files he browsed for some private purpose.

Thus, to be successful, an honest service fraud prosecution involving a misappropriation of confidential information should show that: there was a disclosure of the confidential information to some private party for private gain; if there was no such outside disclosure, that the government employee used the information for his or her own private purposes; the employee served in a position that involved a discretionary, decision-making role; the breach of public trust was sufficiently serious; and there was a failure to carry out official duties (such as granting exclusive, preferential treatment) that

35 *Id.* at 1077.

amounted to an intent to deprive the public of the official's honest services.

The misuse of the confidential information would not necessarily have to result in a financial gain to the official or to some private party. It could, for example, be the unauthorized release of sensitive nonpublic government information that significantly benefits the goals of some private organization, particularly where there is some demonstrable harm to the government or the public resulting from the release.

### MISUSE OF OFFICIAL POSITION SCHEMES

In one of the cases arising out of the Abramoff investigation, it was established that Abramoff had attempted to secure an appointment for Mark Zachares in the Department of the Interior Office of Insular Affairs.<sup>36</sup> The Office of Insular Affairs was responsible for U.S. island territories; Abramoff had lobbying interests in the Commonwealth of the Northern Mariana Islands. Abramoff was unsuccessful in this effort. Ultimately, Mark Zachares found a position on a Congressional staff.

Abramoff and Zachares had a so-called "two-year plan" in which Zachares would work on the Hill advancing Abramoff's interests and gain valuable contacts that would enhance his value as a future lobbyist working for Abramoff. The factual statement in the plea agreement set forth a bribery-like scheme in which Abramoff provided a "stream of things of value" in exchange for a "stream of official action." Zachares pleaded guilty to conspiracy to commit honest services fraud.

This case suggests the outlines of an innovative application of the honest services fraud statute to deal with a scheme that might be described as placing a "mole" in a government position. Such a case could be established even in the absence of a bribery-like exchange of favors for official action if the following elements were established: there was an express or implicit understanding of future private

sector employment between the official and an outside party; and an official engaged in a pattern of exclusive preferential treatment of the outside party, such as providing nonpublic information, arranging for special access, and speaking on behalf of the outside party's interests. This pattern of preferential treatment must be serious enough to amount to a deprivation of the public's right to the official's honest services.

Such a theory of an honest services fraud case would enable law enforcement to address serious misconduct that might not be covered by the conflict of interest law which deals with representation of private parties in matters in which the United States has an interest. That statute, 18 U.S.C. § 205, bars an employee of the executive branch from acting as an agent or attorney in a matter in which the U.S. is a party or has a direct and substantial interest. The statute serves two policy goals.

First, it protects government processes from the improper influence and advantage that a private party might obtain by being represented by a government employee. Second, it preserves the value of loyalty that an employee should have to his or her employer, the government. The statute, however, requires that a person act as an "agent or attorney." Thus it would not apply in a situation where a private party had not engaged the government employee as a representative. For extreme conduct in which the official acted as a "person on the inside" and bestowed preferential treatment that compromised the duty to provide honest services, the honest services fraud statute could apply instead.

### FEDERAL PROGRAM FRAUD SCHEMES

Finally, the honest services fraud statute can be used in cases involving federal program fraud. The federal program fraud statute proscribes bribery related to programs that receive federal funds when there is no bribery of a federal public official.<sup>37</sup> In a case involving a local gov-

ernment official, the mayor of Calumet City, Illinois, was convicted under both 18 U.S.C. § 666 (federal program fraud) and under the honest services fraud statute.<sup>38</sup> The honest services fraud conviction involved a kickback scheme in which a law firm that received "the lion's share" of the city's legal business kicked back thirty percent of the payments it received from the city to the mayor. The concurrent program fraud scheme involved the payment of comp time to city employees who had taken leave time to engage in political activity. In this case, the two counts involved different sets of facts. As required by the program fraud statute, Calumet City received more than \$10,000 annually in federal funds.

### THE FUTURE OF HONEST SERVICES FRAUD

The honest services fraud statute continues to be an effective tool for dealing with public corruption and is often viewed as a first-line defense for combating new and unusual fraud schemes until Congress provides a particular legislative response. The statute should be considered as an alternative charge where the facts might not support all the elements of a conflict of interest crime – for instance, bribery or illegal gratuity cases where there is no specific link between benefits and particular official acts, financial conflict cases where the concealed financial interest is that of a family member or other relationship not covered by the conflicts laws, and cases involving extreme disloyalty and violation of the duty of a public official to serve the public interest.✱

<sup>36</sup> See Factual Basis for the Plea of Mark Dennis Zachares at 1 (Mar. 14, 2007).

<sup>37</sup> See 18 U.S.C. § 666.

<sup>38</sup> *U.S. v. Genova*, 333 F.3d 750 (7th Cir. 2003).





# Earl E. Devaney

**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.

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.

---

**James P. O'Sullivan** is a senior attorney in the Departmental Ethics Office of the U.S. Department of Justice. From 2005 to 2008, he served as an Associate General Counsel in the Office of Inspector General of the U.S. Department of the Interior where he worked on public integrity investigations.

He was a member of the joint audit team of the Department of Defense and Department of the Interior that received an Award for Excellence from the former PCIE in 2008. Prior to his service at the Department of the Interior, he was the Special Assistant to the Director of the Office of Government Ethics from 2002 to 2005 and was an Associate General Counsel at the Office of Government Ethics from 1992 to 2002.

He is a member of the adjunct faculty of the Washington College of Law of the American University and a graduate of Georgetown University Law Center. Mr. O'Sullivan is admitted to practice in Maryland, the District of Columbia, and New York.

# James P. O'Sullivan



[AUDIT]

# Using Risk-Based Planning to Enhance Audit Impact

## How to confront the bigger risks to the programs that you audit

**BY GORDON MILBOURN AND MIMI SHARKEY**

The last few years, the U.S. Postal Service Office of Inspector General focused attention on the type of work we do, the quality of that work, and the contribution it makes to the Postal Service's success. While we have dramatically improved in many areas and introduced a number of innovative approaches to how we do our work, as our Inspector General David C. Williams says, "We are pleased, but not satisfied."

All OIGs make decisions as to what audit work will address the most significant issues facing their agency. One method is to use some form of risk assessment to make those determinations. This article discusses a new approach that the Postal Service OIG has embraced that builds upon previous efforts and successes in the audit planning process. Specifically, this article discusses our approach to risk-based planning and what we call "Risk Deployment" of audit resources, as well as what the Postal Service is doing as a result of our increased emphasis on risk.

### A CHALLENGE TO OUR MISSION

A key part of our mission is to help the Postal Service improve its bottom line and meet its universal mail delivery mandate efficiently and economically. While our mission stays the same and our resources are limited, the environment we work in changes, while customer, stakeholder, and legal expectations and man-

dates increase. For example, the *Postal Accountability and Enhancement Act of 2006* requires new work from us. Our challenge is to meet our mission by conducting audits that matter the most – and risk-based auditing helps us do that smarter.

**“Using this risk deployment strategy allows us to position our resources to address high-risk areas more efficiently.”**

### RISK DEFINED

What do we mean by risks? Simply, we mean events or things that could keep the Postal Service from accomplishing its goals and objectives. Risks can be quantified in terms of money, such as excessive costs or foregone revenue. They can be articulated in terms of loss of data (either to outside hackers or the crash of a system that obliterates much needed management information), damage to public goodwill or reputation, or damage to the ethical climate of the organization. Risks can also be foregone opportunities – such as not introducing a great new product or mission-critical system, thereby harming future revenue or mission delivery, respectively.

### RISK-BASED PLANNING

Historically, many OIG audit groups primarily focused attention on their specific program areas, and in previous years, we did as well. In addition, audit groups typically risk-assessed narrow topics or individual audits in their planning or audit surveys. While this approach was common practice, we were concerned that it did not help us identify or address the most critical, and in many cases global, issues facing the Postal Service. We became increasingly interested in those issues that crossed or fell between Postal Service Vice President programmatic areas. We also sought a way to tackle situations where the number and significance of the issues we found were greater than the audit resources we had organizationally dedicated to addressing them. As a result, we realized that we needed to be in the best possible position to know what the totality of the Postal Service's risks are, understand how they impact the Postal Service, and help find ways to address them more effectively. Therefore, in 2007 we developed a risk-based planning approach that examines risks Postal Service-wide, which is considered state-of-the-art in the internal auditing profession.

We began by doing a top-down risk assessment of the Postal Service. In preparation, we researched the concept of risk from a number of sources, such as the Institute of Internal Auditors and the Corporate Executive Board's Audit Director Roundtable. Additionally, we received

helpful advice from the Tennessee Valley Authority OIG, which had also increased its focus on risk.

### CATEGORIES OF RISK

Leaders from our Office of Audit with input from key Postal Service executives, our Office of Investigations and numerous stakeholders, examined the issues facing the Postal Service across the full spectrum of its mission and operations. We grouped Postal Service risks into three broad categories: strategic, financial, and operational, and included aspects of risk related to compliance and information technology within the three categories.

### RISK FACTORS

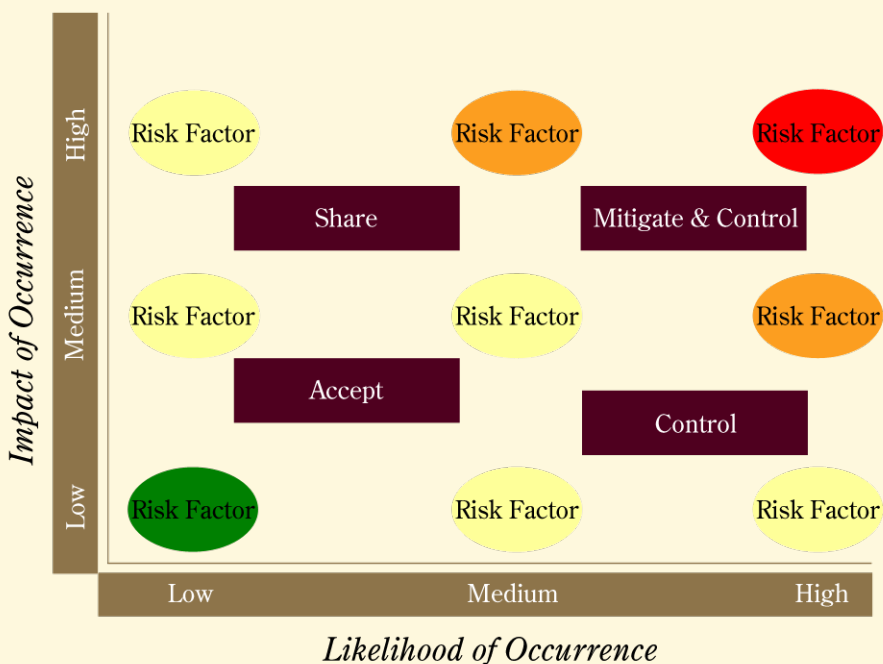
We then identified specific risk factors under each of the three overarching categories. The next step was to determine the level of risk for each risk factor by assessing the likelihood of its occurrence and the impact if it did occur. There are sophisticated quantitative methods to make these assessments; however, we elected, to use such factors as our knowledge of the Postal Service, the views of key Postal Service officials, and the results of our audits and those of the Government Accountability Office.

We learned continuously throughout our development process. For example, we quickly realized it was not reasonable or practical to plan audits to address every risk factor every year. We therefore made decisions on what audit work to perform based on our assessment of risk for each risk factor and on how that fit into the “big picture” for the Postal Service.

We also found that we may touch on more than one risk factor during an audit of any specific topic. For example, poorly managed relations with mailers might be an underlying problem found in a work sharing audit.

At a high level, we then arrayed the Postal Service’s risk factors visually for their associated risk category in a “spider diagram,” as shown in top right.

## Example of Risk Heat Map



### HEAT MAP

To pictorially present our detailed risk assessment results, we illustrated the risk factors overall, and individually, for each risk category on a “heat map” using red, orange, yellow, and green to present the levels of risk (see example below):

- Red means a risk factor has a high likelihood of occurrence and a high impact if it occurs; and
- Orange means it is either high likelihood and medium impact, or medium likelihood and high impact.
- Red or orange ratings mean that the risks are significant and need to be carefully managed to ensure day-to-day success.
- Using the same two descriptors of likelihood and impact, yellow means a risk factor is medium-medium, medium-low, low-medium, low-high, or high-low; and
- An assessment of green means that both the likelihood and the impact are low.

Generally speaking, the high likelihood-high impact and high likelihood-medium impact rated risk factors have the greatest potential impact at the Postal Service-wide level, and should be

of greatest interest and concern to top management, Postal Service Board of Governors, and to us. Anything ranked high to medium impact should be of particular interest to operational managers, although it can be important to both groups.

Using heat maps, we were able to take volumes of information about each risk factor under the three overarching categories and reduce it to a single picture for each category of risk. We also constructed a summary Postal Service-wide heat map, shown below. It was then easy to see that many risk factors were interrelated and certain ones stood out as being the most critical.

### HOW ORGANIZATIONS DEAL WITH RISK

In addition to showing how specific risk factors rate, the heat maps also depict how organizations typically deal with risks. Risks are handled differently, based on their rating, and differ from one heat map quadrant to another. In general, organizations:

- Accept risks that have a low likelihood of occurrence and a minor impact if they do;

- Share risks that have a low likelihood of occurrence but a high impact if they do;
- Implement controls for risks that have a high likelihood of occurrence, but a low impact; and
- Implement mitigation techniques (to prevent problems) or controls (to catch them) for risks that are both high likelihood and high impact.

## RISK DEPLOYMENT

It is up to the Postal Service and the board to address the risks that they face; however, we can add tremendous value by bringing the significant ones to their attention and identifying their ramifications. The objective of the risk-based planning approach is to increase our value to the Postal Service by focusing audit attention on the highest risk areas while still completing our mandatory audit workload.

Our audit directorates are structured with a focus on specific programmatic areas of the Postal Service. For example, our Delivery Directorate focuses on the operations of, and issues confronting, the Delivery Vice President. A designated structure, with specific resources assigned to each directorate, lends stability to our organization and helps our auditors over time, gain expertise in the Postal Service programs they audit. It presents difficulties when we find that the issues confronting a specific Postal Service program have become so significant and widespread that a single directorate cannot effectively address them.

In introducing a risk-based approach to our work, from a process standpoint we continued with the specific structure and programmatic focus of each directorate. This was strongly preferred to reorganizing or permanently reassigning resources each time bodies of needed work overwhelmed the available resources in a directorate. To allow us to quickly address new or changing risks, however, we moved to a proactive Risk Deployment approach to become more agile and better able to quickly address significant issues.

Risk Deployment allows us to regularly evaluate where our resources are most needed and to shift personnel or work to address those needs. When situations demand organizational flexibility, we reassign a few individuals, entire teams, or entire directorates into new areas of work for a period of time, or reassign specific work from one directorate to another. Risk Deployment does not mean bureaucratic restructuring to address the changing Postal Service environment. Instead, staff either volunteer to participate in Risk Deployment projects, or are delegated by management based on what is deemed best for the organization, with consideration to personal needs.

Using this Risk Deployment strategy allows us to position our resources to address high-risk areas more efficiently, as opposed to delaying critical audits when the directorate that routinely handles the topic is already fully engaged.

Another benefit of the Risk Deployment strategy is that it provides an opportunity to broaden individuals' or audit teams' knowledge of postal operations and to strengthen their auditing skills. This broader knowledge of and experience with postal operations will lead to more robust audits and greater contributions and value to the Postal Service.

## IMPACT ON INDIVIDUAL AUDITS

As a result of our risk-based planning initiative, our audit staff includes an increased focus on risk in their audit objectives. Thinking in these terms helps them see the big picture in their audit projects and compels them to consider how individual projects tackle the most significant Postal Service concerns. Explicitly, audit staffs contemplate the bigger risks confronting the program they audit, as well as how their proposed audit project addresses those risks.

## POSTAL SERVICE INSTITUTES ENTERPRISE RISK MANAGEMENT

After performing our top-down risk as-

essment, we briefed the Postmaster General, Deputy PMG, and the Board's Audit and Finance Committee regarding our efforts and results. They expressed a commitment to develop a complementary instrument with interdependent roles.

The Postal Service Chief Financial Officer formed an Enterprise Risk Management Committee made up of the Deputy PMG, Senior Vice Presidents, Counsel, himself, and others (including the Inspector General as an adjunct, non-voting member), to further address risks and institutionalize risk management in the Postal Service. Under the committee's leadership, a broad-based working group and individual Postal Service components have begun identifying – and in some cases developing – techniques to mitigate, control, or share their risks.

## NEXT STEPS

We continue to use a risk-based focus and consider Risk Deployment in our annual planning process. The Office of Audit executives and directors regularly assess the risks facing the Postal Service, and, recently, OA executives completed a thorough update of last year's top-down risk assessment to kick off our 2009 annual audit planning effort. Our audit directors will use this information to plan specific audits to address what we determined to be the greatest risks facing the Postal Service in 2009.

In this manner, we are truly, on an OA-wide basis, identifying the most important bodies of work that need to be done, and then positioning ourselves to do that work without restructuring our organization every year. This more agile approach enhances our value to the Postal Service. Further, it operationally places us in a future-oriented position. It is a new and exciting direction for us to move in, both in the IG community and in the broader world of internal auditing. ❁





# Gordon C. Milbourn

**Gordon C. Milbourn III** was named Assistant Inspector General for Audit of the U.S. Postal Service Office of Inspector General in February 2005. He is responsible for all audits in the Postal Service areas of core operations, financial management, technology, and headquarters operations. His staff of approximately 350 employees — located in major offices nationwide — conducts independent audits for the largest civilian federal agency, with over \$70 billion in annual revenues, a workforce of over 700,000 employees, and nearly 38,000 facilities.

Milbourn began his federal civil service career in 1974 as an internal auditor with the IRS Inspection Service. He left the IRS in 1986 to work for the Naval Audit Service, and in 1987, moved to the Environmental Protection Agency, Office of Inspector General. During his over 12 years at EPA OIG, he held positions as a Supervisory Auditor, Audit Manager, Headquarters Staff Director, and Divisional Inspector General for Audit. In 1999, he was selected as the Assistant Inspector General for Audit (Small Business and Corporate Programs) for the Treasury Inspector General for Tax Administration, and from November 2002 to February 2005 served as TIGTA's Acting Deputy Inspector General for Audit.

Milbourn is a graduate of the University of Virginia, and attended the Defense Systems Management College. He has received numerous awards during his career, including four EPA Bronze Medals.

---

**Mimi A. Sharkey** is a Program and Policy Specialist for the Office of Audit at the U.S. Postal Service Office of Inspector General. She reports directly to the Assistant Inspector General for Audit and serves as an authoritative resource in the area of planning, budgeting, and accountability. Her responsibilities include solving significant problems between and among programs, systems, functions, policies, and other critical issues.

In 1997, Ms. Sharkey was hired by the Social Security Administration as a Presidential Management Intern (now known as the Presidential Management Fellows Program). In this capacity, she began working for SSA in their Seattle Regional Office, and then came to headquarters and worked in the Office of the Principal Deputy Commissioner, the Office of Budget, and the Office of Communications. Subsequently, in December 1999, Ms. Sharkey accepted a position with the SSA OIG in their Office of Executive Operations where she worked on strategic planning efforts, public affairs issues (internal and external), media and congressional issues, semiannual reports to Congress, and wrote and reviewed speeches, articles, letters, reports, and brochures. In February 2002, Ms. Sharkey began working for the USPS OIG in Strategic Planning, and held a series of progressively more responsible positions.

Ms. Sharkey has earned numerous awards and other recognition throughout her career, and has a Bachelor of Arts degree in Psychology, a Master of Arts degree in Social Work with a minor in Public Administration, and is currently a doctoral candidate at the University of Baltimore in the Doctor of Public Administration program.

# Mimi A. Sharkey



[INVESTIGATIONS]

# How Legal Requirements May Vary Depending on the Nature of the Business Entity Being Investigated

Identifying these entities will dictate what substantive laws can be applied

BY THOMAS COOGAN

The President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency, now Council of Inspectors General on Integrity and Efficiency require all investigators to possess:

"A knowledge of applicable laws, rules, and regulations, including the U.S. Constitution, the U.S. Criminal Code (including elements of crimes, the federal Rules of Evidence, the federal Rules of Criminal Procedure, and other pertinent statutes, such as the Privacy, Freedom of Information, and Whistleblower Protection Acts."

"Quality Standards for Investigations" (December 2003), p. 3. Further, the CIGIE states:

**"Legal Requirements**—Investigations should be initiated, conducted, and reported in accordance with all applicable laws, rules, and regulations; guidelines from the Department of Justice and other prosecutive authorities; and internal agency policies and procedures. Investigations should be conducted with due respect for the rights and privacy of those involved."

"Quality Standards for Investigations" (December 2003), p. 7. The goal of this article is to inform readers how legal requirements vary depending on the nature of the business entity being investigated, whether corporation or partnership or sole proprietorship, and how to identify



what type of business entity is being investigated.

## INTRODUCTION

Identifying what type of business entity is being investigated will dictate what substantive laws can be applied to the entity and what procedural laws must be followed by the investigator. There are many types of business entities, including corporation, partnerships, and sole proprietorships. Some substantive laws will apply only to certain types of entities. Other substantive laws might appear not to apply to business entities, but actually do apply. At the outset of an investigation the applicable substantive law must be identified in order to determine

what evidence needs to be gathered.

Identifying what kind of business entity is being investigated also will dictate what procedural laws need to be followed by the investigator. These procedural rules will impose a duty on the investigator and a right on the subject of the investigation. Some procedural laws will apply only to individuals and not to business entities. Some laws, however, will provide rights to some types of business entities. In order to gather information appropriately, the investigator must identify the type of business entity that is the subject of investigation in order to know what procedural laws are applicable regarding the gathering and reporting of information.

There are many types of business entities, including corporations, partnerships, and sole proprietorships. The most commonly mentioned business entity is probably the corporation. Corporations generally have more obligations and fewer rights than other types of business entities. By far, however, the most common type of business entity in America is not the corporation but the small, unincorporated businesses, often a sole proprietorship. Sole proprietorships usually do not register with State authorities and have few if any record-keeping requirements. Sole proprietorships generally have fewer obligations and more rights than other types of business entities. In addition to corporations and sole proprietorships, there are other types of business entities such as partnerships. Partnerships generally have obligations and rights that fall between those of corporations and sole proprietorships.

#### **IDENTIFYING SUBSTANTIVE LAWS THAT APPLY TO BUSINESS ENTITIES**

Identifying what type of business entity is being investigated will dictate what substantive laws can be applied to the entity. At the outset of an investigation, the applicable substantive law must be identified in order to determine what evidence needs to be gathered.

#### ***SUBSTANTIVE LAWS THAT APPLY TO ONLY CERTAIN TYPES OF ENTITIES***

Some substantive laws apply only to certain types of entities. Corporations will be subject to laws covering corporations; partnerships will be subject to laws covering partnerships, etc. In addition, some laws will not apply to business entities unless they employ a certain number of employees. Some laws enforced by the Equal Employment Opportunity Commission will be applicable only if the entity employs 15 or more individuals.

#### ***SUBSTANTIVE LAWS THAT APPEAR NOT TO APPLY TO BUSINESS ENTITIES BUT DO***

Some laws may appear not to apply to a business entity but in fact do apply. For example, 26 U.S.C. §7206 states that any “person” who falsifies tax information is guilty of a felony. On its face, the statute would seem to only apply to individuals. However, the legal definition of “person” in the Internal Revenue Code, 26 U.S.C. §7701(a)(1), includes not only individuals (i.e. “natural persons”) but also partnerships and corporations as well as other entities. An important step in dealing with business entities is to understand that laws and regulations affecting “persons” might also apply to corporations and similar organizations that typically would not be considered “persons.”

#### **IDENTIFYING PROCEDURAL LAWS THAT APPLY TO BUSINESS ENTITIES**

Identifying what kind of business entity is being investigated also will dictate what procedural laws need to be followed by the investigator. These procedural rules will impose a duty on the investigator and a right on the subject of the investigation.

#### ***LAWS APPLYING TO GATHERING INFORMATION FROM BUSINESS ENTITIES***

Investigators need to be able to identify the type of business entities involved in the inquiry to determine if various laws, such as the Right to Financial Privacy Act or Fifth Amendment, apply to their inquiry. The type of entity, and other identifying characteristics, such as the number of partners, will determine what procedures need to be followed in gathering information.

#### ***CORPORATIONS***

It can be easy to obtain information from a corporation, regardless of its size, whether it is public or private, for-profit or nonprofit. The U.S. Supreme Court

has determined that unlike “natural persons,” corporations have no privilege against self-incrimination within the meaning of the Fifth Amendment. See *Bellis v. United States*, 417 U.S. 85 (1974); *United States v. Kordel*, 397 U.S. 1, 7 (1970). Corporations are also not entitled to notice and right to challenge a subpoena issued for financial records under the Right to Financial Privacy Act.

#### ***PARTNERSHIPS***

Like corporations, the U.S. Supreme Court has determined that partnerships have no privilege against self-incrimination within the meaning of the Fifth Amendment. See *Bellis v. United States*, 417 U.S. 85 (1974); *United States v. Kordel*, 397 U.S. 1, 7 (1970). However, under the Right to Financial Privacy Act, partnerships of five individuals or fewer are entitled to notice and a right to challenge a subpoena for the partnership’s financial records.

#### ***SOLE PROPRIETORSHIPS***

The Supreme Court has interpreted the Fifth Amendment privilege against self-incrimination to include the act of producing business records of a sole proprietorship. *United States v. Doe*, 465 U.S. 605 (1984). The act of producing records concedes the existence and possession of the records called for by the subpoena as well as the respondent’s belief that such records are those described in the subpoena.

#### **LAWS APPLYING TO DISCLOSING INFORMATION FROM BUSINESS ENTITIES**

The type of entity, such as corporation, partnership, or sole proprietorship, will determine what procedures need to be followed in disclosing information.

Determinations on disclosing information obtained during a government investigation will be subject to various information laws, including FOIA, 5 U.S.C. §552, and the *Privacy Act*, 5 U.S.C. §552a. FOIA generally encour-



ages disclosure unless there is an exemption, including an exemption for personal privacy protection. That protection, however, cannot be invoked to protect the interests of a corporation or association. See, e.g., *Sims v. CIA*, 642 F.2d 562, 572 n.47 (D.C. Cir. 1980); *National Parks & Conservation Ass'n v. Kleppe*, 547 F.2d 673, 685 n.44 (D.C. Cir. 1976). According to the DoJ, however, information about a closely-held corporation or small business when the individual and corporation are identical could be withheld from disclosure. *Providence Journal Co. v. FBI*, 460 F. Supp. 778, 785 (D.R.I. 1978), rev'd on other grounds, 602 F.2d 1010 (1st Cir. 1979), cert. denied, 444 U.S. 1071 (1980). See also *National Parks, supra*, 547 F.2d at 686; cf. *Zeller v. United States*, 467 F. Supp. 487, 496-99 (E.D.N.Y. 1979).

The *Privacy Act*, 5 U.S.C. §552a, protects the rights of individuals. Corporations and organizations clearly do not have any *Privacy Act* rights. Guidelines from the Office of Management and Budget, responsible for administering the *Privacy Act*, also suggest that an individual has no *Privacy Act* rights when the records of that person pertain to him solely in his "entrepreneurial" capacity. Some courts, however, do not agree and have applied the *Privacy Act* to such records.

### BASIC TYPES OF BUSINESS ENTITIES AND THEIR CHARACTERISTICS

There are a variety of business entities. The most common, however, are corporations, partnerships, and sole proprietorships.

Publicly traded corporations will have a wealth of publicly available information. A publicly-traded corporation is one that has its stock traded. Private corporations, also known as close or closely held corporations, do not publicly trade stock and information about these non-public companies will also be more difficult to track down than for public corporations.

### CORPORATIONS

Corporations are created by state law. One of their main purposes is to encourage investors to become shareholders in a business in order to provide capital investment and earn a return on their investment without being liable for anything beyond their personal investment in the company. Because they are created by law, they can be, and are more closely regulated than other business entities that can be created without any particular legal authority, such as a sole proprietorship or general partnership. While there are various types of corporations, including Subchapter C and Subchapter S (the former paying corporate tax, the latter passing tax liability to the shareholders), and for-profit and non-profit corporations, they all will file with their State to be incorporated. State filing agencies will be a valuable source of information. In addition, corporations will be required to maintain certain records, including articles of incorporation, by-laws, and minutes of meetings. Finally, as with any other business, corporations will maintain financial records to account for their business and to file tax returns.

Professional corporations are a special type of corporate entity used by certain professionals, such as physicians, accountants, and attorneys.

### LIMITED LIABILITY COMPANIES

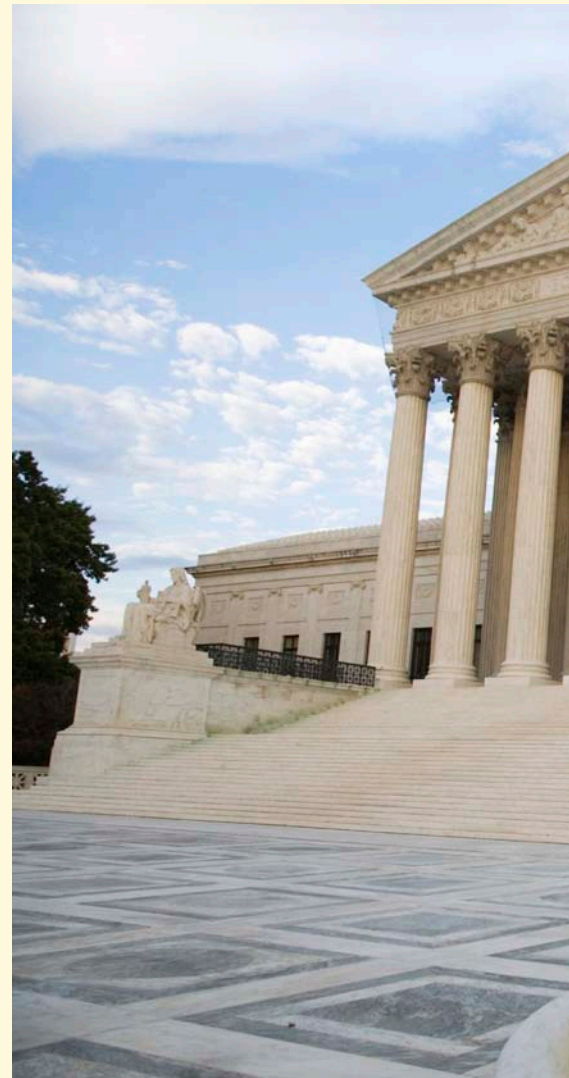
Limited liability companies are not corporations; however, like corporations they are intended to shield investors from personal liability for the acts of the business. They are designated by abbreviations such as LLC, LC, and Ltd. Co. Limited liability companies, like corporations, will typically have filing requirements with their State. Their recordkeeping requirements may not be as formal. For example, rather than articles of incorporation and by-laws there could be a membership agreement. Tax liability is supposed to pass to the members.

Some states prohibit certain professionals, such as physicians, accountants, and attorneys, from forming limited li-

ability companies to limit their liability for their professional services. These states may allow such professionals to form "professional" limited liability companies, which enable members to limit their liability for company business, such as contracts with vendors, but not for the member's professional services, such as advice to clients. A professional limited liability company, abbreviated PLC, should otherwise operate the same as a limited liability company.

### DESIGNATIONS SIGNIFYING WHETHER AN ENTITY IS INCORPORATED

State law will require corporations to use certain designations to signify that they are incorporated. Delaware, a state well-known for being friendly to corporations and, therefore, a



home to many of them, has a long list of designations that can be used: “association,” “company,” “corporation,” “club,” “foundation,” “fund,” “incorporated,” “institute,” “society,” “union,” “syndicate,” or “limited,” (or abbreviations thereof, with or without punctuation), or words (or abbreviations thereof, with or without punctuation) of like import of foreign countries or jurisdictions (provided they are written in Roman characters or letters). Title 8, §102, Delaware Code. One of those words or abbreviations used for corporations in foreign corporations presumably could be “Societa per Azioni” or the abbreviation “S.p.A.” used by Italian corporations and expressly allowed by the State of Con-

necticut. §33-655 General Statutes of Connecticut. The District of Columbia, home to most federal agencies, has perhaps the most simple and straightforward requirement for required designations: “corporation,” “company,” “incorporated,” or “limited,” or shall contain an abbreviation of 1 of such words. § 29-101.08 District of Columbia Code. When the above words are seen, or related abbreviations such as “Inc.,” “Corp.,” “Co.,” “Ltd.,” and others, the investigator can be fairly sure that the business entity is incorporated.

Not every business entity that looks like a corporation is a corporation, and some designations can be misleading. For example, in most

states “Company” or “Co.” will be a designation for a corporation; however, some states that allow the use of “Company” prohibit the use of “and Company”, “and Co.,” “& Company” or “& Co.” and those designations are used by unincorporated entities, such as partnerships. See, e.g., §273.177 Kentucky Revised Statutes if the word “company” or the abbreviation “Co.”; but if the word “company” or the abbreviation “Co.” is used, it may not be immediately preceded by the word “and” or the abbreviation “&.”

In some states individuals and partnerships may register a fictitious name with the word “Company” in it. Designations therefore can be helpful but not necessarily accurate in helping to identify the type of entity being investigated.

## PARTNERSHIPS

Unlike corporations that are created by statutory law, partnerships typically are not governed by statutes, but by common law and practice applied and interpreted by courts when legal questions arise.

Typical business partnerships, sometimes called general partnerships, are formed when two or more persons join together for a common business purpose. Ordinarily there is no filing requirement, although some states will allow partnerships to file.

The partnership, like other business entities, also will ordinarily need to register for tax purposes. The partnership is usually formed when the partners sign a written partnership agreement.

Unlike shareholders whose liability is limited, general partners are “wholly and severally” liable unless the agreement says something else.

That means if one partner creates a liability for the partnership, every partner is liable for the whole amount, not just their individual proportional share.





## LIMITED PARTNERSHIPS

Some partnerships allow for limited liability for some partners and unlimited liability for others. These are known as “limited partnerships” abbreviated “L.P.” There also can be partnerships where all partners are liable for the partnership except for professional services rendered by a partner. These entities are known as “limited liability partnerships” abbreviated “L.L.P.”

## SOLE PROPRIETORSHIPS

By far, however, the most common type of business entity in America is not the corporation but the small, unincorporated businesses, often a sole proprietorship. Sole proprietorships hold themselves out as businesses but mostly operate because of the efforts of one person. These “mom-and-pop” operations account for up to 70 percent of all business activity. Sole proprietorships usually do not register with State authorities and have few if any recordkeeping requirements.

A sole proprietorship will be run by one person, sometimes with the help of family members or close associates. States typically will not require any filing, except perhaps to register for paying sales tax. Sole proprietorships are popular because there are no start-up requirements, no documentation, and no costs, such as legal fees. Because unlike corporations sole proprietorships are not created by statute, state agencies will typically not have much if any information. That will require the investigator to obtain information from the sole proprietorship.

It is not unusual for a sole proprietorship to do business under a name other than the same of the sole proprietor. For example, Mary Smith, a sole practitioner accountant, might do business as “ABC Accounting,” a “fictitious” business name, and her business records might identify the sole proprietorship as “Mary Smith d/b/a ABC Accounting.” (In some jurisdictions they will use “trading as” or “t/a” instead of “doing business as” or d/b/a.) Some States will require that the fictitious business name be registered. In addition, when a business

uses a fictitious business name instead of the same of the sole proprietor, it may not be entitled to all of the same legal protections that the individual would be entitled to receive.

## INFORMATION TO IDENTIFY CORPORATIONS

Corporations are required to register with their State of incorporation. States will maintain information about corporations and some states will have information available online. For example, Pennsylvania corporations can be researched at <http://www.corporations.state.pa.us/corp/soskb/csearch.asp>. Local business journals contain corporate information. For publicly traded corporations, information is publicly available online from “EDGAR,” the SEC Filings & Forms database at <http://www.sec.gov/edgar.shtml>. All publicly traded companies, foreign and domestic, are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Anyone can access and download this information for free. EDGAR will contain extensive information about the corporation, including the names of Board members and corporate officers. Some corporate tax return is publicly available. For example, Forms 990, which are filed with the Internal Revenue Service by non-profit corporations and other entities, are available online through Guidestar, a privately funded database of nonprofit organizations at <http://www.guidestar.org/>.

The Government Accountability Office’s “Investigators’ Guide to Sources of Information” (GAO/OSI-97-2) at <http://www.gao.gov/archive/1997/os97002.pdf> lists the following additional sources of information about corporations:

- America’s Corporate Families (Annual Dun & Bradstreet directory listing approximately 11,000 parent companies and over 79,000 subsidiary companies and divisions owned by the parent companies)
- Best Insurance Reports (Annual editions of the Best Insurance Reports [Life-Health and Property-Casualty]

present detailed information on U.S. and international insurance companies.)

- Directory of Companies Filing Annual Reports with the Securities and Exchange Commission Under the Securities Exchange Act of 1934 (Published by Government Printing Office, this directory lists companies that sell stock on the national exchanges or over the counter and that file annual reports with SEC.)
- Directory of Corporate Affiliations—Who Owns Whom (Annual directory provides information on almost 150,000 public and private parent, subsidiary, and associate companies in the United States and overseas.)
- Dun & Bradstreet’s Million Dollar Directory (Annual Dun & Bradstreet directory contains information on over 20,000 public and 140,000 private utilities, transportation companies, banks, trust companies, mutual and stock insurance companies, wholesalers, and retailers, including corporate officers, locations, phone numbers, type of business, and number of employees.)
- Financial Yellow Book (Directory lists over 41,000 top executives at leading financial institutions from chief executives to subject-area officers and over 8,500 board members and their affiliations.)
- Foreign Representatives in the U.S. Yellow Book (Directory includes officials’ titles, addresses, and telephone and fax numbers for personnel who represent foreign corporations in the United States.)
- Moody’s International Manual (Manual contains background and financial information on over 3,000 foreign firms.)
- Moody’s Investors Services (Moody’s broad business-sector manuals cover companies whose stock is traded on stock exchanges and contains history and background; names and titles of officers and directors; location of plants and properties; the headquarters phone number and address; and

financial statements.)

- Predicasts Funk and Scott Index, United States (Directory indexes articles on products, companies, and industries that appear in most business periodicals and newspapers.)
- Standard & Poor's Corporation Records (Directory cover over 12,000 publicly traded companies and 34,000 subsidiaries, affiliates, and privately held firms, including company's brief history, financial statements, capital structure, lines of business, subsidiaries, and officers and directors. Information on 70,000 executives is also available.)
- Standard & Poor's Register of Corporations, Directors and Executives (Annual directory lists about 56,000 public and private companies and the names and titles of over 400,000 officials.)

#### INFORMATION TO IDENTIFY PARTNERSHIPS AND SOLE PROPRIETORSHIPS

Finding out about partnerships and sole proprietorships, however, will ordinarily

not be so straightforward. Partnerships and sole proprietorships typically are not required to register with the state or federal government. Unless they do for some reason, such as registering under a fictitious name, public agencies will not maintain information about partnerships or sole proprietorships. In the absence of official information that identifies a business entity, investigators should consult with legal counsel to ensure that proper substantive and procedural laws are identified. Because partnerships and sole proprietorships will have certain rights not afforded to corporations, investigators should not assume that an entity is a corporation.

#### CONCLUSION

Identifying what type of business entity is being investigated will dictate what substantive laws can be applied to the entity and what procedural laws must be followed by the investigator. At the outset of an investigation the applicable substantive law must be identified in order to determine what evidence needs to be gathered.

There are many types of business entities, including corporations, partnerships, and sole proprietorships. Corporations generally have more obligations and fewer rights than other types of business entities. In contrast, sole proprietorships generally have fewer obligations and more rights than other types of business entities. Partnerships generally have obligations and rights that fall between those of corporations and sole proprietorships. Investigators must understand what type of business entity is being investigated because different substantive and procedural laws will apply to different entities. Obtaining information to identify corporations will be easier than for partnerships and sole proprietorships. When doing investigations of this type, knowing more about the nature of the business is essential to the investigator's success. ❁

**Thomas Coogan** is the Assistant Inspector General for Investigations at the Legal Services Corporation Office of Inspector General, which, unlike most other OIGs, not only investigates fraud but also has specific statutory authority to investigate regulatory compliance.

He came to LSC after retiring from the Postal Service OIG where he served in various executive capacities, including Deputy Inspector General and General Counsel and was Chair of the Council of Counsels to the Inspectors General. He also worked at the FDIC, USDA, DOJ and the Secret Service.

Mr. Coogan is also a faculty member and program coordinator of the Master's degree program in forensic studies at Stevenson University in Maryland, a fully-accredited graduate program in forensic accounting, computer forensics, investigations and law that is offered on campus as well as on-line. He is an appointed member of the Higher Education Committee for the Association of Certified Fraud Examiners and past contributor to the Journal of Public Inquiry.

He has received many honors, including awards from the President's and Executive Councils on Integrity and Efficiency. Mr. Coogan received a Bachelor's degree from Hamilton College, a Master's degree in forensic science from Antioch College, a law degree from the Antioch School of Law, and has been admitted to practice law in New Hampshire, where he served as a federal judicial law clerk; Maryland, where he worked in private practice; and the District of Columbia.

# Thomas Coogan





## [INVESTIGATIONS]

# White Paper Tape Recording Interviews

*In my survey, of the relatively few in law enforcement who opposed the idea of tape recording interviews, the arguments were remarkably consistent and one-dimensional*

**BY DANIEL CONEY**

This white paper discusses tape-recording law enforcement related interviews, and identifies the positive and negative aspects of the practice. In researching this paper, I surveyed law enforcement officers and agents, primarily drawn from the ranks of the Rocky Mountain Inspectors General Council, prosecutors and judges. I also discussed this topic with Federal Law Enforcement Training Center legal staff, and researched professional writings. In presenting assessments of both sides of the issue in this paper, I hope to open a constructive dialogue resulting in improved understanding of the practices OIG law enforcement employs, and whether changes to those practices are necessary.

## THE DRIVERS FOR CHANGE

The changing face of law enforcement must result in professional law enforcement agencies adapting to technology changes, as well as changes in the political and social climate we operate in. Today, federal law enforcement needs to implement a flexible and realistic policy of capturing the results of our interviews in a more effective way.

The dynamics of today's legal practice in defense of criminal or civil defendants is all too familiar to those who have been in court over the last decade. Given the stringent requirements to obtain a federal indictment, defense attorneys have resorted to an intentional practice of putting witnesses on trial rather than confronting the facts of the case. OIG agents are routinely castigated in court and administrative proceedings, their intentions painted as corrupt. Well-known interviewing expert Don Rabon



pointed out, “Now, often, the defense has only to raise the specter of the *possibility* that inappropriate steps were taken within the “communication event”. One Special Agent in Charge related how his agency went to tape recording interviews following a case where the jury refused to believe a confession because the perception was law enforcement was hiding something by not taping the interview.

The key driver for change is the fact that law enforcement is not held in high esteem, and the agent's testimony bears no greater influence or credibility than any other witness, and sometimes less. The public and the courts both seem to believe agents have a stake in the outcome of the proceedings – a belief perhaps founded since some agencies rate performance and grant awards based on the outcomes of those proceedings. The respect and presumption of truthfulness once enjoyed by law enforcement simply does not exist in the culture anymore, in

part due to the parade of law enforcement officers who have been indicted for their own crimes and the rampant corruption of the past in some departments. Just recently, Federal Bureau of Investigation agent John Connally was convicted of helping the Boston mafia arrange hits, while two OIG agents from the U.S. Department of Health & Human Services were indicted for separate fraud schemes. In recent years, some 18 Federal Air Marshals have been charged with felonies. The *Giglio* and *Henthorn* court decisions reflect the court's displeasure with law enforcement ethics and their attempt to be sure such ethical concerns are known by defense. The FBI laboratory failures still linger in the public memory, and routine news stories about DNA freeing another wrongly convicted person are abound.

In this environment, we have seen more and more courts and prosecutors preferring evidence that does not rely on

the testimony of law enforcement officers. Because of cost restraints, decisions on which cases to pursue are based in part on the level of litigation the prosecutor will face, particularly suppression hearings where witness or defendant statements are at issue. Effective law enforcement is not simply about proving facts; sophisticated agents actively seek to eliminate or at least mitigate possible defenses before ever bringing the case to prosecution.

When it comes to interviewing, instead of asking the question, “Why should we tape?”, the better question is, “Why aren’t we taping?” Are there legitimate grounds for not taping interviews, or in only taping in limited circumstances? If our interest is to serve the public, why would we not want to be as transparent and up-front about our practices as possible? If our interest is conveying the facts as truthfully as possible, why would we not resort to the best evidence we could possibly obtain? If our interest is in protecting the rights of citizens, why aren’t we bending over backwards to insure what they say is not taken out of context?

I would submit that while there is historically no precedent for tape recording, and thus a resistance from some in law enforcement to something “new”, the reason why this has been so is two-fold: in the past, the technology was not acceptable and the costs for an adequate ability to record were infeasible. Since those two questions were answered in the negative, there was never a need to ask further questions.

However, today’s technology and cost feasibility is well within any agency’s reach. Furthermore, the culture and accountability of the times we live mandates we progress to a point where we at least ask the more in-depth questions about why we do not take advantage of the cost effective technology that now exists. This article is intended to do just that – to look at fourteen of the most common arguments or concerns about tape recording interviews.

## HISTORICAL ARGUMENT

In my survey, of the relatively few in law enforcement who opposed the idea of tape recording interviews, the arguments were remarkably consistent and one-dimensional. Essentially, the best argument presented was one of history – an “if it ain’t broke don’t fix it” concept in which the overriding theme is that over the many years they have done investigations and secured convictions, they had never needed to use recordings.

This is an obviously flawed argument. While the past informs the present and is the basis for setting precedent, it should not make us so inflexible that we do not take advantage of new and better ways to accomplish the mission before us. Such an emotional response appeals to our sense of tradition more than anything else, but holds little logic.

## RESTRICTING THE ABILITY TO “GET THE INTERVIEW”

One argument is that having a tape recording device in the room puts people on the defensive, and more likely to refuse an interview. I have found no empirical studies on this topic, but my personal experience using a tape recorder has found no resistance at all, particularly when it is explained in the context that the recording is intended to protect them from misquoting their statements. In fact, it is apparent the interviewee forgets entirely about the tape recorder as the interview progresses. It also allows a more natural “conversation” to take place, with an agent not necessarily having to take furious notes to capture everything said in an interview.

An appropriate parallel is the *Miranda* decision in 1966. In the immediate aftermath, law enforcement as a whole predicted widespread impacts on interview success that never materialized. Professional law enforcement officers adapted quite well and today few would argue that *Miranda* amounts to much more than a slight bump in the road. One SAC commented that his OIG recorded

about 65 percent of their interviews last year, representing 450 to 500 interviews, and only had one lawyer refuse to consent. Other SACs who regularly record interviews reported no problems stemming from refusals to consent, thus, it appears this is not a material problem. Where someone does not consent to a recording, the interview can still take place, memorializing the fact that a recording opportunity was offered which the interviewee declined, which still has the effect of protecting the appearance of propriety before a jury.

## INTEGRITY AND ETHICS

By necessity, law enforcement as a profession, and individually as officers and agents, must be one in which we are above reproach. Even the appearance of impropriety or underhandedness reflects poorly on all of us. The fact that we are not recording interviews fuels conspiracy theories and fears of a public that often worries about such things as “big brother” and an over-reaching government.

There is nothing we do in our interviews that should not be open to the utmost public scrutiny. After all, we are usually talking about depriving a citizen of their liberty, seizing their assets and other serious intrusions. We are not the KGB, nor the Gestapo – we proudly bear the banner of public servant. As such, establishing and following a policy of routinely recording interviews of suspects and key witnesses puts us under the microscope as much as the person interviewed. It equals the scales so to speak, and it disables defense attorneys from being able to make inane arguments that impugn the integrity of the agents. At the same time, it installs an element of professionalism and self-policing. The dashboard cameras in patrol cars have been a boon to demonstrate how professional an officer acted, or in cases when an officer abused his authority, it had the effect of being able to weed out those officers. While embarrassing for the department, it is much

better to remove from service those who cannot handle their position.

### OPERATIONAL SECURITY

A concern for law enforcement involves revealing techniques or strategies employed by a professional investigator. I would suggest it is rather the plan for implementing law enforcement tactics in any given situation that is critical, not the elements of the tactics themselves, which are more “like plays in professional football – everyone pretty much has access to the same game plans and plays. It isn’t so much who has the most plays as who can best execute the plays that they all have.”

This is really the point of public distrust in law enforcement, and therefore jury bias, is we by nature are very secretive of what we do and how we do it. We cannot expect jurors to trust our testimony if they do not understand how we go about obtaining confessions any more than we can expect them to trust physical evidence if they don’t understand how it was collected at a scene. Some people point to particular tactics the public may see as distasteful, such as excessive use of profanity when dealing with certain segments of society. This perhaps is an issue for certain agencies in some contexts, but for the vast majority of the OIG community, there is no excuse for the unprofessionalism of profane, abusive or out-of-control speech. The public can see such speech as intimidating and coercive because it is, and we should not be lowering our standards to allow such conduct. If we cannot support a practice when exposed to the light of day, then it should not be a practice in our repertoire at all, despite results we may sometimes achieve. The means and ends must both be pure in American law enforcement. Law enforcement needs to realize their customer is really the jury, whether that be an actual jury, a decision-making judge, a tribunal or administrative board that makes final decisions. We need to be accountable and transparent to our customer so they can be comfortable with the facts presented to

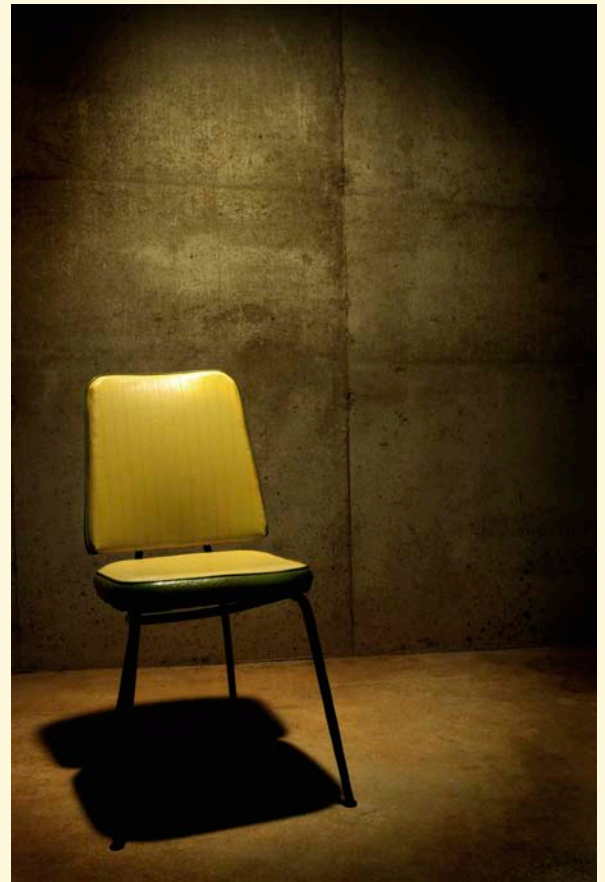
them. Every reasonable effort should be employed to make the facts speak for themselves – and tape recordings do that in a literal way.

### HIGHLIGHTING MISTAKES

Another issue concerns a myriad of problems that fall generally under a fear that memorializing the encounter on tape captures mistakes that could affect the case. It may be that it captures the flaws of an inexperienced or inept interviewer. It may capture procedural mistakes or faux pas’ involving speech that is unbecoming. Of those surveyed, the overwhelming majority cited the fact that an agent knowing an interview was going to be recorded resulted in more thorough and professional interviews. One SAC stated it has “made my agents better interviewers – no one wants to go into an interview unprepared, and then sound foolish on the tape. An agent will only do that once.”

Interviewing is one of the integral components of the job, and enhancing that skill is possible through using mistakes made, as well as very good techniques, to train others to avoid future mistakes. Furthermore, from a supervisory standpoint, SACs are able to much more effectively monitor individual agent performance and deal with allegations if they can review the interview. Presently, it is rare for a SAC to actually see an agent “in action” and be able to judge performance based on what an agent does rather than the status quo, which is judge an agent based on the ability of a prosecutor to resolve a case appropriately.

Yet another issue that is more fundamental to this argument is the ethical basis for why we would not want a mistake exposed in the first place. The underlying assumption is we don’t want to have a recording in case there are mistakes.



That presupposes first that your agents will make mistakes, and second that we don’t want those mistakes exposed. This is fundamentally unethical, and from Watergate to Martha Stewart, is the basis from which worse lapses in judgment occur. Where we make mistakes, we ought to own up to them, regardless of the consequences. We must not also assume that all mistakes are fatal; judges and juries do not expect human beings to be perfect, and minor lapses should not be expected to result in exclusion of the statement.

### TRAINING & POLICY NEEDS

Headquarters management and field managers must have realistic expectations about the learning curves and the time it will take for agents to comfortably integrate this practice into their routine. There are some differences interviewing on tape, such as setting protocols for preambles on tapes, what to do if you have to stop a tape mid-way through an interview, how much talk occurs before or after a recording is turned on, or introducing documents during an interview.



There needs to be training provided for these kinds of procedural issues, and the agent needs to be completely aware of the technical functioning of the recording device they are using.

One SAC said some otherwise competent agents “freeze” when they record the interview – much like a “stage fright” kind of reaction. This is a training need that all the people I spoke with said was overcome by becoming comfortable with doing interviews with a recorder on, even if such recordings are in mock interviews. The feedback they get from seeing or hearing themselves on tape will make them better interviewers.

There also needs to be a protocol for how one saves the recording for evidentiary purposes, and as the technology progresses, agencies need to keep abreast of what is on the horizon for electronic recording, such as authentication of digital recordings to defeat any defense claim of tampering. Another issue at the forefront is designing and equipping interview rooms wired for audio and video, which aids in the quality of both forms of recordings.

### CONSENT OR NOTICE

One important consideration is whether to seek consent before recording. FLETC advised there is no legal requirement to obtain consent to record an interview or give notice that a law enforcement officer is taping an interview, barring some union requirements.

Another complication for consideration is whether to obtain consent before or after activating a recording device. It is obviously much better to have as part of the recorded conversation the notices and explanations given to the interviewee on tape. There are at least two solutions. The first possibility is to not ask for consent, but rather simply give notice that a recording is taking place. This practice is consistent with federal law, and helps eliminate interviewee resistance by not giving them an opportunity to say no to a consent. If the person does not wish for the interview to be taped, then the

agent can have discretion to continue the interview without the tape, but the tape up to that point has captured the declination by the interviewee and the interview report should articulate such a rejection. Secondly, the agent may ask for verbal consent to record the interview before turning on the recorder, then upon turning the recorder on, make a preamble including a statement such as, “John Doe has consented to the recording of this interview, is that right Mr. Doe?” The elicited response then captures the consent on tape.

### ACCURACY & COMPLETENESS

One of the major benefits cited by respondents to the survey was the improved accuracy and completeness of their reports. The more complex a case, the more help recording seems to be, particularly when you have initial complaints or qui-tam complainant interviews of subject matter experts who will use technical jargon and mention names, events, dates, and places that the investigator is unfamiliar with. As the investigation progresses and the agent understands the issues and acronyms better, having the ability to go back to a tape and listen again has aided a more timely completion of investigative steps. This is particularly useful in procurement, health care, and scientific or engineering related cases where there are many technical issues. Some agencies merely do a brief cover memo to a transcript, in which case they cite the timesavings involved over typing an interview report, while other agencies cite extra time given to agents for report completion results in a much better and more thorough product, but not necessarily a timesaving.

### TRANSCRIPTION

A major issue that has both pros and cons involves the time and cost of transcription. One SAC, laboring this point, said headquarters must not expect agents to transcribe tapes unless they want a case to come to a screeching halt. Agents are not equipped to handle

transcribing tapes - they need to focus on keeping an investigation moving.

There is also the issue of authenticating a transcript by the same person doing the interview. One of the benefits of using a transcription service is the independent third party verification and authentication of what is on the tape. Transcription services are cost-effective, though they can be costly, which is why one SAC pointed out there needs to be discretion first on when to record an interview, and second, on which interviews need to be transcribed. A secondary issue involves confidentiality and security clearance needs for the contracted transcription service, as well as securing any email transactions of digital voice files.

My personal practice has been to use the interview tapes to prepare a comprehensive summary statement in the form of an interview report. I place in the body of the report a statement that the interview was recorded and the recording is available in evidence. I provide a copy of the recorded interview to the prosecutor, but I never seek to produce a transcript since transcripts are useful more at trial than for investigations. In my view, if a transcript is needed, this should be a litigation expense bore by the prosecutive authority rather than the investigative agency.

### LIABILITY INSURANCE

“One of the biggest issues faced by law enforcement officials – and the reason an increasing number of agencies are recording interrogations in their entirety – relates to allegations that mistreatment of a suspect by officers resulted in a coerced confession. A recently as October 2006, a United States District Court awarded \$9 million in damages to Alejandro Dominguez, who spent four years in prison for a crime he did not commit.” In the litigious society we all know we live in, it has reached a point where it is necessary to defend ourselves against claims of wrongdoing, and to do so proactively. Tape recording the interview process is the most reasonable



and efficient method of providing what amounts to low-cost liability insurance for both the agent and agency. Such not only protects from monetary damages, but also serves to, little by little, begin to build trust back in the public's mind concerning police conduct.

### TECHNICAL COMPETENCE OF THE PUBLIC

Another issue mentioned as weighing in on the issue of juries is the fact that the vast majority of the public has become technologically savvy. As such, they are more skeptical of law enforcement's resistance to using the technology. Juries want to make judgments of guilt or innocence themselves, and they want to hear straight from the defendant's mouth to make that judgment. Our job is to service that need by providing a product our customer can confidently use.

### OVER-RELIANCE ON WRITTEN STATEMENTS

Obtaining written statements can be a tricky business. If the defendant writes his own confession, which is preferred, it is human nature to minimize the criminal conduct. It is common that a person will make valid and even strong admissions during the course of a verbal interview, but when reduced to writing, amount to nothing more than excuses. I have actually had a subject write himself entirely out of a confession after verbally making admissions. On the other hand, if the agent writes the confession, the invariable defense claim is we put words in the defendant's mouth, or he felt coerced into signing words not his own – the claims are endless.

Furthermore, most OIG's have requirements for employees to cooperate in investigations. Such cooperation clearly would include answering questions in an interview, but it is quite possible a claim could be made that an employee has met his or her obligation to cooperate by submitting to an interview, but not in providing a written statement. Tape-recording interviews precludes any such contingencies.

### OVER-RELIANCE ON TECHNICAL EQUIPMENT

One of the more practical considerations in tape recording interviews involves reliance on a tape recording that fails. This perhaps illustrates two problems – one being mechanical failure, the other being the agent relying too heavily on technical equipment. One agent related an experience in which a confession was gained, but when the tape recording was played, the critical point of the confession was missing. Defense counsel was able to make hay with this at first, but fortunately, the agents had two backups. Both agents had taken written notes contemporaneously with the interview and the confession was in both sets of notes, and they were using an interview room with a video recording. Though the video recording did not have sound, it showed that during the critical moment, the tape had to be flipped over. Today, digital recording devices that fit in the palm of your hand are available at low cost, and have recording capacities of over 8 hours without having to switch a tape. The lessons learned here are: agent notes are still helpful, perhaps even necessary; redundant systems are a good idea on important interviews; pictures (video) are better than mere audio; and agents are still going to have to testify about and justify their procedures to a skeptical audience.

### LITIGATION RISK

Some of the most time-consuming litigation work has to do with procedural rather than factual issues. Suppression hearings are all about excluding facts because of what is typically a procedural error, mistake, or intentional act on the part of law enforcement. Central to this proposition is law enforcement's procedures with respect to interviewing witnesses and suspects, and how the results of those interviews are memorialized. Interestingly, this is the area that perhaps has the greatest contrast between the views expressed by survey respondents. The conventional wisdom expressed among those in favor of tape recording

interviews is that recording will reduce the time and expense involved with litigation, and yield more plea bargains.

One very successful prosecutor had a very different opinion, saying tape recording will likely not reduce pleading practice at all. First, even if we have a client "dead to rights" in a taped interview, defense counsel will still move to suppress it because that is their job. The existence of solid evidence against a defendant says nothing about how vigorously defense counsel will fight to exclude it. Furthermore, tape recordings are Jencks and/or Brady material that must be turned over to defense counsel. In many long-term, complicated cases, an interview of a witness might look very different in year one of an investigation than in year three or five. Early statements may include erroneous assumptions and a lack of a fully developed understanding of the fraud scheme. Clearly, these are explainable differences, but that is the point – a defense attorney will take any difference and try to raise doubt in a jury's mind. The preference from a prosecutor's point of view is to only have to deal with testimony at trial. The prosecutor also said videotape is the better taping method, because body language communicates so much and demeanor can be interpreted by a jury in a video, where it cannot in an audio tape.

### CONCLUSION

Overall, the evidence in support of tape recording interviews is clear and convincing. The concerns voiced primarily in the area of litigation risk are the most troublesome aspects militating against recording, and should lead us toward a robust policy that tries as much as possible to account for these concerns. For instance, though it may be helpful to have a tape recording of witness interviews early in a complicated case, the fact that conflicts between those recordings and later statements may cause more harm than good when we reach the litigation phase perhaps ought to point us to a general policy against recording interviews of witnesses early in an in-

investigation. Presently, it is common to make serial requests for information and continue to ask questions of these kinds of witnesses as our understanding of the case develops and there is no reason that cannot continue.

At the end of the day, we must ask ourselves two questions: Who is/are our customer(s), and what is the best product we can provide? Ultimately, juries or administrative boards are the end user of the product we produce, but in between there are a host of others we have to be responsive to as well. Based on recent jury responses, court decisions, and input from prosecutors and judges, there can be no dispute that tape recording interviews goes a long way toward providing the best product we can.

Additionally, we are to serve the public interest and do so in the most economical way we can. Investigations can be costly affairs. Because a tape recording tends to make a case more airtight if done right, it provides better assurance of a return on investment – that return being enhancement of public safety, protection of taxpayer money, making our programs whole, and carrying out the mission that we have been charged with.

It is my judgment that though the practice of tape recording may actually

increase some facets of litigation, this likely will be a function first of the novelty of the practice. The more routine and accepted the practice becomes, the fewer issues will arise with it, so long as there is a consistent policy and adherence to the policy about how to appropriately conduct taped interviews. Secondly, though the initial foray into this area will produce lessons learned, the benefit in the professionalism of law enforcement and responding to cultural demands needed to be successful will produce greater dividends than refusing to adapt. Just like the worries associated with Miranda in the 60's, this new challenge we will look back on in a few years and wonder what we were so worried about. While there is a transitional process that will involve a learning curve, if we are serious about serving the public and being successful, we must adapt to the changing environment or find that we are producing buttons when the demand is for zippers.

U.S. Attorney's Offices across the country are being responsive to the courts, who more and more demand the accountability of taped interviews. Even the FBI has recently decided to change course and start allowing the taping of their agent's interviews. Director Mueller said in his confirmation hearings in

2001 that he would consider making this change, and slowly the prohibition is being lifted.

Finally, in 2003, the State of Illinois passed legislation requiring law enforcement at the state and local levels to record all subject interviews in homicide cases. Maine and New Mexico have followed suit. President Barack Obama was a junior state senator in Illinois at the time, and was the driving force behind the bill. Though "prosecutors resisted it, he argued persuasively that it would ensure convictions in the large majority of cases." It is safe to assume this could be an issue we must face in the immediate future. Rather than be compelled by law or executive order, why not do what is right in the first place? This is an idea where its time, like it or not, has come.✿

---

**Daniel H. Coney** has served in the law enforcement profession for nearly 25 years, including as a police officer and a Special Agent. He works in the Denver office of the Office of the Inspector General for the U.S. Department of Commerce. His experience has been primarily in financial fraud investigations in the health care, contracting, grant, and non-profit arenas, netting nearly 100 indictments and \$65 million in monetary recoveries over the past 15 years.

Dan has continually held certifications as a Certified Fraud Examiner and Certified Financial Investigator since 1995, and the certification of Certified Business Manager since 2001. He has been awarded the Distinguished Achievement Award by the Board of Regents of the Association of Certified Fraud Examiners, as well as been presented the prestigious Guardian of Justice Award from the United States Attorney's Office for the District of Kansas.

# Daniel H. Coney



[AUDIT]

# Postal Operations: Prelude to a Changing Audit Environment



## BY THEODORE J. WILLIAMS

Like most federal agencies, our Air Force audit environment is complex and dynamic, with missions constantly changing to meet new requirements and warfighter needs. Our mission—to provide all levels of Air Force management with independent, objective audit evaluations across the full spectrum of Air Force operations—poses challenges for how we employ our audit staff effectively to provide world class audit service. Increasingly, new technologies, growing numbers of DoD joint service organizations and automated information systems present new challenges for how we go about accomplishing our audit mission. To continue adding value for our customers, we can no longer audit strictly within the confines of Air Force operations, but must increasingly cross organizational lines to interact with other DoD and government agencies to obtain information needed for evaluations.

As an example, Chief Financial Officers Act audits of Air Force financial statements and line items rely extensively on Defense Finance and Accounting Service financial information, as well as from information provided by non-Air

Force systems such as Army munitions systems and Naval Facilities Command military construction systems. Moreover, information technology audits generally must be coordinated with Defense Information Services Agency officials, and several recent projects such as Hurricane Katrina support and pharmacy operations required interaction with US Northern Command, the Federal Emergency Management Agency, and DoD joint medical organizations. Clearly, our Air Force audit environment is changing dramatically and we must refine our processes to ensure continued value-added audit results for our clients.

A recent Air Force Audit Agency audit of Air Force Postal Operations provides an excellent example of the need for Air Force and all government auditors to work in a changing audit environment to achieve audit objectives. This audit required our Air Force audit team to interact with DoD and other federal agencies such as the U.S. State Department and the U.S. Postal Service to fully evaluate postal operations and obtain information needed to accomplish our audit objectives. This article will illustrate why interaction with other non-Air

Force government activities was essential for meeting our customer needs.

## DOD POSTAL RESPONSIBILITIES

Under the “single manager” concept for military mail, the Secretary of the Army is the Executive Agent for the Military Postal Service and relies on the Military Postal Service Agency to validate USPS bills, provide technical assistance, and monitor overseas postal operations. Day-to-day Air Force postal operations fall under the purview of the Office of Warfighting Integration and Chief Information Officer (SAF/XC), which provides oversight and management of day-to-day Air Force postal operations such as planning, programming, and budgeting for overseas military mail transportation requirements.

## POSTAL AUDIT TEAM

The Administrative Assistant to the Secretary (SAF/AA) is responsible for overseeing HQ Air Force Secretariat funding, to include SAF/XC, and expressed concern about rising Air Force postal costs. Specifically, SAF/AA requested an AFAA review of all aspects of postal operations,



to include postal billings, cost sharing, and policies in effect that impacted all DoD military departments. To meet SAF/AA's request, we formed an audit team comprised of a Program Manager, three Audit Managers, and, as with most centrally-directed Air Force audits, our statisticians. To complement and assist in researching, planning, and applying the audit were ten installation auditors located at stateside and overseas European and Pacific locations. Working together, the Program Manager and each Audit Manager contributed their own unique knowledge, expertise, and ability to this complex tasking, ensuring a successful, comprehensive review of postal operations. Working in geographically separated offices, the audit team effectively communicated and coordinated audit work and report writing to streamline the audit process, providing senior AFAA and Air Force management with specific, hard-hitting, value-added audit results. Most critical to this success was our thorough understanding of the key roles DoD and government agencies played in overall military postal operations.

The Military Postal Service is the primary organization that Air Force and other services use to transport official and personal mail, priority supply items, publications, and other materials to overseas areas in peacetime and contingencies. The DoD pays for mail transportation between the U.S. gateways such as New York (John F. Kennedy) and San Francisco airports and overseas and inter- and intra-theater locations, with the three military departments sharing the transportation costs. To accomplish the fairly complicated billing process, DoD and USPS use three primary postal systems to measure, monitor, and bill military mail movement as described below.

- Automated Military Postal System  
The AMPS is a DoD system used to dispatch mail from all overseas military mail terminals except the Narita and Okinawa (Japan) and

Inchon (Korea) mail terminals.

- Surface and Air Support System  
The SASS is a USPS system that uses zip code information to determine which military department to charge for mail movement.
- Global Enterprise Mail System  
The GEMS is a USPS system used to dispatch military mail from the United States and the Narita, Okinawa, and Inchon mail terminals. Together, AMPS and GEMS systems generate manifests for mail from overseas mail terminals to stateside terminals (retrograde), and from stateside terminals to overseas terminals (prograde) that are transmitted to SASS for billing.

### AUDIT RESEARCH, PLANNING, AND DESIGN

The team interacted with USPS, State Department, Military Postal Service Agency, Army, and Navy officials to identify organizational responsibilities as well as the pertinent management information systems used to collect, analyze, and summarize billing data. Audit planning began with preliminary SAF/XC and SAF/AA meetings to discuss management concerns regarding the annual \$100 million Air Force postal costs that were rising each year.

Based on our initial planning meetings, several other Air Force, DoD, and government officials expressed great interest in the audit, having a collective desire to reduce over all postal costs and thoroughly evaluate the following areas:

- Billing processes;
- Billing system interfaces;
- Postal policies that determine which service or activity pays for postal service;
- Personal and official mail;
- Potential use of postal services for personal reasons;
- Types of mail sent between overseas installations;
- Authorized customers at overseas locations using postal services;
- Second destination charges; and

- Potential for sending letters and parcels using higher class priority when 'lower class' rates could apply.

An overriding customer concern was related to DoD postal policies governing military mail movement and costs that had not been revised since implementation (some 30 years or older); Services have never been able to reassess policies and procedures. With that in mind, we believed the audit could identify opportunities to affect policy and law to save money. In addition, SAF/AA questioned whether the Air Force postal practices were consistent with other services, and asked that we crossflow information with all interested DoD postal officials.

### CROSSFLOW WITH OTHER DOD SERVICES

To facilitate the review and maximize results, the audit team provided frequent interim briefings to Air Force officials and Military Postal Service Agency, Army, and Navy mail officials of conditions that appeared to impact DoD mail operations. Based on this positive interaction and cooperation, the Military Postal Service Agency director invited the lead Audit Manager to present an open-forum discussion during the annual Atlantic Mail Conference in Garmisch, Germany. The lead Audit Manager provided a presentation addressing current DoD mail policies and obtained valuable feedback from all DoD postal representatives attending the conference. This cooperative forum helped the audit team obtain buy-in for the audit approach, and develop realistic and practical recommendations for revising DoD mail policies and providing more efficient mail service to military members and families.

### AUDIT SITE VISITS

The audit team site visits included Joint Military Postal Service Agency-Atlantic (Newark and JFK terminals), JMPSA-Pacific (San Francisco), Air Mobility Command and US Transportation

Command (Scott AFB), and the Frankfurt Mail Terminal to become familiar with stateside and overseas terminal processes during the research phase. Faced with the challenge to assess and evaluate virtually all aspects of Air Force postal operations to include funding, billing, mail movement, automated systems, and policy, the team scoped the audit and designed the audit program for application at multiple high-volume postal sites. The following provides background on each area evaluated as well as results.

### **INTRA-THEATRE MAIL MOVEMENT**

Under the Intra-theatre Delivery Service concept, the Military Postal Service provides postage-free delivery of official, personal, organizational, and commercial correspondence and parcels that do not enter the USPS network within the United States, its territories, or possessions. To use IDS, both the sender and addressee must be authorized Military Postal Service users and, in lieu of postage, the block letters “MPS” must be marked on the envelope or parcel. Air Force post office personnel must ensure all IDS letters, envelopes, and parcels are sent as space available mail rather than pay higher costs for priority mail.

- *Condition.* Air Force postmasters sent IDS mail using priority rather than space available rates.
- *Coverage.* We determined whether intra-theater mail was shipped priority versus space available mail by working with Military Postal Service Agency personnel to obtain AMPS reports of zip codes and intra-theater mail movement; pulling AMPS AV-7, Report by Mail Class, for all APO zip codes manifesting mail to other APO zip codes in FY06; using Excel to quantify mail sent priority versus space available; and comparing the priority and space available Department of Transportation rate.

### **BULK BUSINESS MAIL MOVEMENT**

Bulk Business Mail is comprised of stan-

dard third and fourth class mail and includes vendor printed matter, catalogs, brochures, pamphlets, and circulars. The stateside gateways should separate BBM and send it space available (surface container) rather than intermingle BBM with other class mail and send it priority (commercial air).

- *Condition.* Personnel located at the stateside mail gateways sent BBM as priority rather than space available mail.
- *Coverage.* Auditors interacted with USPS personnel and Joint Military Postal Agency – Atlantic and Pacific gateways to review gateway warehouse processes and obtain mail volumes of overseas BBM. We reviewed and documented the weights of all incoming BBM during the period 16 through 29 September. Specifically, we documented the amount of BBM received at eight selected overseas installations that was mixed with priority mail.

### **SYSTEM INTERFACE BILLINGS**

Mail transactions originating in AMPS identify dispatching office zip codes whereas mail transactions originating in GEMS identify destination zip codes. The Military Postal Service Agency uses SASS billing information to charge each Service a proportionate amount of the USPS military mail bill.

- *Condition.* The GEMS and SASS interface did not provide assurance that GEMS transactions originating at retrograde dispatch locations were properly processed.
- *Coverage.* Auditors discussed system capabilities and requested data downloads from Military Postal Service Agency personnel supporting mail transactions and manifests. We determined whether Air Force mail billings were properly processed by obtaining Army, Air Force, and Navy transactions from the DoD AMPS and the USPS GEMS and SASS systems. We matched AMPS transactions to SASS transactions, GEMS transactions to SASS trans-

actions, and SASS transactions to GEMS and AMPS transactions to identify transactions from each system that could not be traced from input to output.

### **BULK BUSINESS MAIL POLICY**

The DoD Postal Manual outlines delivery and non-delivery policies for BBM. When destination postal personnel receive BBM, they attempt to make delivery. If undeliverable, postal personnel remove the BBM address and discard the mail. The DoD manual does not address controls required to reduce undeliverable BBM volume.

- *Condition.* DoD and Air Force bulk business mail policy allowed undeliverable BBM to be sent overseas. The audit manager discussed policy with Military Postal Service Agency, Army, and Navy mail managers and identified common issues with the other DoD services.
- *Coverage.* We evaluated the adequacy of DoD and Air Force postal policies and reviewed and documented weights of all incoming and outgoing mail at eight selected overseas installations. We also documented weights of BBM and the amount of undeliverable BBM.

### **INTRA-THEATRE DELIVERY SERVICE POLICY**

The DoD – USPS Postal Agreement, negotiated in February 1980, specified that personal first-class letters, post cards, and audio cassettes weighing 12 ounces or less within the Atlantic, Latin America, and Pacific theaters sent IDS would be at “no cost.” Current DoD Postal Manual IDS policy was not specific as to what items can be sent IDS, but did disallow using IDS for advertising, commercial purposes, and shipment of household goods.

- *Condition.* DoD and Air Force IDS policy needed revision to reduce perceptions of waste and abuse. The audit manager discussed current policy with Military Postal Service Agency, Army, and Navy mail managers and

identified common issues with the other DoD services.

- *Coverage.* We evaluated the adequacy of DoD and Air Force postal policies and reviewed and documented weights of all incoming and outgoing intra-theatre mail at eight selected overseas installations. We reviewed all IDS packages received and documented potential IDS abuse at these locations.

### AUDIT BENEFITS

Since current DoD postal operations and policies are not Air Force-specific, postal deficiencies applied to all DoD departments. The audit work performed and associated recommendations will result in Air Force savings of \$34.6 million, but also DoD savings of at least \$100 million over the Future Years Defense Program. And, because we performed the audit at only ten judgmentally selected Air Force installations, Air Force officials believed the savings could actually be much greater. We recommended the Air Force:

- Set proper Major Command intra-theatre distribution policies (\$17 million savings over the Future Year's Defense Plan);
- Revise Air Force, DoD, and USPS bulk business mail policies (\$7.5 million savings over FYDP);

- Revise DoD intra-theatre policy to reduce perceptions of waste and abuse and ensure only appropriate shipments were mailed (\$2.7 million savings over FYDP);
- Establish procedures to segregate and bill the Army and Air Force based on actual, rather than estimated, shipment weights;
- Recoup Air Force contract container shipment over-billing valued at \$2.2 million;
- Implement USPS system controls to provide assurance that the USPS properly bills DoD for retrograde mail;
- Automate Germany-Air Mail Terminal operations to ensure Army and Air Force pays accurate amounts for their respective retrograde mail service; and
- Deobligate unneeded obligations and establish procedures to ensure unneeded obligations are deobligated in the future, resulting in making \$4.5 million available for other Air Force mission needs.

### PRELUDE TO FUTURE AUDITS

As this audit example clearly indicates, the audit environment is changing and the need to work with other DoD and government agencies to accomplish comprehensive audit objectives is in-

creasing dramatically. This postal effort provides an excellent example of the positive benefits of collaboration and innovative approaches to audit, working closely with all interested stakeholders, can positively impact a joint program or activity. Because of the tremendous interest in the audit from all stakeholders, the audit team briefed results to the very senior levels of DoD and Air Force postal management. The presentation persuaded senior officials that postal policies were outdated and inefficient, and could easily be used to promote fraud, waste, and abuse. Senior Air Force leadership (SAF/XC, SAF/AA) fully concurred with all recommendations in the report, and sent a personal email to the Auditor General noting the significance of the report since it will have immeasurable positive impact on future overseas postal operations, save money, and improve DoD postal service to our warfighters. As a team, the AFAA auditors professionally represented our organization at its best and set the stage for future audits of programs that may overlap DoD and other government agencies. ✎

*Contributor: Mr. Michael Rollyson, Audit Manager, AFAA/FSC, March ARB CA*

**Theodore J. Williams**, a member of the Senior Executive Service, is Auditor General of the Air Force, Office of the Secretary of the Air Force, Washington, D.C. He also serves as head of the Air Force Audit Agency, which is responsible for all internal auditing in the Air Force. He exercises full administrative and technical supervision over a worldwide organization composed of more than 800 members assigned to 50 locations.

Mr. Williams served in the Air Force more than 26 years before retiring in the rank of colonel in 1999. While on active duty, he worked for the Air Force Audit Agency more than 11 years as an acquisition auditor, audit manager, branch chief, acting office chief, program manager and executive officer to the Air Force Auditor General. He was also an AC-130, KC-135, and EC-135 navigator, instructor and evaluator for more than 10 years.

# Theodore J. Williams





## [PROGRAM GRANTS]

# Managing Grants for Success

The core of any entity or operation is its people and the environment in which they operate

BY ELLIOT P. LEWIS

Much of what the federal government is charged with achieving is not done directly by the government and its employees, but rather through grants to state and local governments, educational institutions, and nonprofit entities. The federal government relies extensively on grants to deliver services to the public. For example, one of the Department of Labor's core responsibilities is to improve citizens' capabilities and opportunities for profitable employment. Many of Labor's programs to achieve these goals are administered through grants.

The Employment and Training Administration is the largest grantor agency within the Department of Labor with an FY 2008 appropriation of \$44 billion. Of this amount, grants comprise \$11 billion. Through its grants, ETA administers programs to improve the employment prospects of adults, youth, and dislocated workers.

As unemployment climbs, businesses outsource or close, technology advances, and the types of employment opportunities change, Department of Labor employment and training programs can be a critical link for someone obtaining a new job or acquiring the necessary skills and re-training that will make them employable in a new industry. The current economic climate, coupled with the ever-changing employment landscape, means that programs must be ready to respond to the needs of our workers and to ensure that the taxpayers' interest is protected.

The need for effective grants management is now amplified by The American Recovery and Reinvestment Act of 2009, which adds billions of dollars to ETA's grant programs. Ensuring that these



funds are spent wisely, reach recipients quickly, and attain desired results will represent an enormous challenge for the Department of Labor, and an added oversight responsibility for the OIG.

Delivering services through grants presents unique vulnerabilities as management, costs and ultimately, successful performance are not under the direct control of the agency. For this reason, it is imperative that the agency remain vigilant throughout the life of the grant—from pre-award through grant closeout to ensure that grant programs are effective, reach intended recipients, and achieve intended results.

Based on issues that I have seen in nearly 30 years of auditing grants from many different federal agencies, this article outlines the internal control framework needed to manage grants for success, and key control activities that should be performed during the grant life cycle.

## FRAMEWORK TO ENSURE EFFECTIVE GRANT MANAGEMENT

Successful grants management involves nothing more than good internal control. Many people think of financial management when they hear the words internal control. Internal control, however, has much broader applications. Internal control is a process, effected by management and employees, designed to provide reasonable assurance of achieving a specified objective. Therefore, the internal control framework is critical to managing grants for success. Internal control consists of five interrelated components:

- *Control Environment;*
- *Risk Assessment;*
- *Control Activities;*
- *Information and Communication;*  
*and*
- *Monitoring.*

## CONTROL ENVIRONMENT

The core of any entity or operation is its people and the environment in which they operate. The same is true for a grant program and its individual grantees. The success of any grant program is dependent first and foremost on the commitment of those running the program and the tone they set throughout the organization. This includes not only the grantor agency, but the grantee as well. People at all levels of both organizations must possess the right knowledge, the adequate skills and they must be expected to carry out their duties with the integrity that expending taxpayer dollars demands. The control environment permeates all the other components of the internal control framework.

Effective grants management begins with strong, consistent commitment by officials responsible for the program. The success of every grant program is greatly impacted by the commitment of the person at the highest level of the grant-making agency (and the highest level of the grantee). What is important to that individual permeates through the organization and drives what the organization focuses its time and attention on. If a grant program's success is viewed as important and a priority, that will drive performance. I believe that you get what you focus on. If the agency is clearly focused on achieving results through its grant programs, it is much more likely that those results will be achieved. This focus is not something that is occasionally done, or is only done at the kick-off of a new program or new round of grants. The focus must be continuous. The agency must define what success looks like and constantly assess its progress in achieving that success.

The head of the organization also sets the tone for the organization, or the manner in which things are accomplished. If the head of the organization sets and enforces an expectation of integrity and ethical behavior, that will drive the culture of the organization. Sound decisions demand a com-

mitment to ethics and integrity. This is especially critical when deciding which grantees to select and which grants to award. If proper procurement procedures are not followed, grantees may be selected that are not the best choices to provide needed services or did not offer the best grant proposal. Program officials must make sure that the people with procurement expertise are involved in the selection process, and that they have the necessary authority and independence to carry out their duty. Subject matter experts must be involved of course and make decisions on questions pertaining to their area of expertise, but procurement experts must be allowed to make the decisions on purely procurement matters. It is ultimately up to the leadership of the grantor agency to ensure this happens.

Program officials must demonstrate integrity, commitment to competence, and a willingness to assign authority and responsibility to have positive impact on grant management. Conversely, lack of such commitment will have an adverse impact on grant management and consequently on grant performance and results.

## RISK ASSESSMENT

An entity must be aware of and address the risks it faces. In the case of grants, this includes the risk that the grant will not achieve its intended purpose or that it will not be done in the fair and ethical manner required of programs financed with public funds. As with many endeavors, when spending public dollars, results are important, but the end does not justify the means. Taxpayers expect that the government's business be conducted in an appropriate manner. The grant-making agency must clearly identify what it wants to achieve with its grant program, what is acceptable in accomplishing that goal, and then systematically assess what could prevent such achievement.

Grants have inherent risks because of their nature. That is, unlike the manage-

ment of other government expenditures, the grantee has the primary responsibility for performance and management of the grant. As a result, risks should be considered for the grant program, the grantor agency, and the grantees.

## GRANT RISKS

Is the grant program new or significantly revised? This poses greater risk than a well-established program where people have had time to learn and understand the grant program and implement appropriate controls. Similarly, are the grants themselves regularly made, such as formula grants or are the grants unique, such as demonstration grants? Unique or one-time grants have increased risk, because you are trying something new that does not have a track record. Has there been a significant increase in funding the grant program or are funding levels consistent from period to period? A significant ramp up of spending for a program increases the risk that funds will not be used as intended or as effectively as possible. As noted previously, the unprecedented funding increases in the economic stimulus package, combined with the need to award those funds quickly, will increase the risk to successful performance. Other risk factors to consider include the complexity of the program, how challenging the program goals are, and whether Congress has clearly defined what the program is intended to deliver.

## GRANTOR AGENCY RISK

Does the grantor have sufficient resources to administer and oversee the grant program? Are staff sufficiently knowledgeable about the grant program? Is the grantor properly organized so that the responsibilities are assigned to the right people and they have the necessary authority to carry out their responsibility? The organizational structure of a grantor agency is critical. People need access to the information to perform their jobs, and they also need the appropriate level of authority to carry



out their responsibilities. I have seen organizational structures where an office responsible for establishing grant policy and procedures did not have the authority to require grant officers to adhere to the policies because the grant officers were under a different line of authority.

### GRANTEE RISKS

Is the grantee experienced in managing the particular grant program, does it have experience with other federal grant programs, or is it new to managing federal grants? New grantees which lack experience in managing federal funds present a special risk as they are often unaware of all of the rules and regulations that go with spending taxpayer dollars versus other funding. A grantee with experience in managing federal grants may require additional guidance and oversight when it becomes involved in a program with which it has had no prior experience. Even for an existing grantee, risk assessment should include an evaluation of the grantee's past performance, financial management, and significant management or staffing changes that have occurred. You must also consider whether the grantee is receiving a significant increase in funding. The grantee may be adept at operating the grant program, but may not have the capacity to administer a significantly larger program.

It is important for agencies to develop, use, and continue to improve and strengthen their methods for assessing risk.

### CONTROL ACTIVITIES

For each risk identified, control activities should be developed to address or mitigate those risks. The type and degree of control activities should be commensurate with the level of risk identified. The level of risk can be measured in two ways: the probability that the risk will occur and the impact it will have. Those risks that are most likely to occur and would have the greatest impact should be addressed with the greatest level of control. Control activities are defined by the policies and procedures of an organization.

Written policies and procedures must be established and executed to help ensure that actions identified by management (or by law) as necessary to address risks are effectively carried out.

To ensure successful performance, control activities must be implemented that cover all phases of the grant life cycle. I divide the life cycle of a grant into four phases: pre-award, award, performance, and post-performance.

Pre-Award. There are a number of actions program officials should consider at the beginning of the grant cycle (pre-award phase) to help ensure effective grants management. A competitive process should be used to the greatest extent possible. Clear and objective criteria should be established to evaluate proposals and prospective grantees. The entire selection process and the rationale for decisions should be documented. Following proper procurement procedures in awarding grants is paramount. For example, program officials should make sure that proposal evaluation panels include appropriate technical experts; they may wish to make pre-award site visits to prospective grantees; and may consider steps to expand outreach to have the broadest range of organizations compete to offer services. When the grantor agency has the ability to select grantees (i.e., the grant is not a formula grant or other directed grant), it is imperative that the best, most capable grantees are selected.

Award. Once the decision is made to award a grant, a comprehensive, clear, and specific grant agreement is critical. The grant agreement is the principal means by which the grantor agency communicates to the grantee what is expected and how it is to be done. If program officials do not clearly spell out what is required, then they can not expect the grantee to deliver. Grant agreements must delineate clear, measurable objectives; specify all products to be delivered, if any, and incorporate all expectations and requirements. Grant objectives and resulting outcomes must be clearly linked to agency program goals. Grant proposals may be a good starting point for the



grant agreement, but a proposal may not be sufficiently clear or organized in the manner required by a good grant agreement. Modify the proposal as necessary. Finally, make sure that the grantee understands what is required by their grant agreement. Consider using post-award conferences or meetings to explain the grant.

Taking these steps in the early stage of the grant process is important in seeing that clear expectations are built into the grant from the beginning.

Performance. The performance phase is particularly impacted by the quality of controls at the grantee. The grantor agency must ensure that the grantee has the necessary people and systems to effectively achieve the desired grant results and manage the federal dollars. One of the biggest problems I have noted with costs claimed for grants is a lack of documentation that the funds have been spent correctly—in particular, documentation of personnel time spent on grant activities. Grantees need to document what they do and how it benefits the grant.





Grantees need to understand the cost principles and any additional requirements that affect what they can claim for reimbursement. Grantor agencies can require grantees to explain how they will go about determining allowable costs. This will help ensure that the grantee has properly focused on this and developed effective systems. Timely reporting by the grantee will help the grantor identify progress or detect problems. However, meaningful information has to be reported and the grantor agency needs to know that the grantee has good systems to produce accurate reports. Good reporting can help target monitoring and oversight to greater effect. A common trap is to only focus on those grantees who report problems or less than expected results. Sometimes you need to follow up on those results that look good (or too good) as they might not be as good as they appear. If they are as good as they look, the grantor agency may discover some best practices that can be replicated in other grants and programs.

**Post-Performance.** Once a grant has ended, the need for good controls continues. It is during this period that the grantor agency needs to ensure that all deliverables have been met. All grant funds need to be accounted for. Grant performance needs to be evaluated. Evaluating grant performance is necessary for making decisions about future funding of a grantee, but also to determine how effective the grant program was in achieving its goals.

### INFORMATION AND COMMUNICATION

All of the other components of the internal control structure need information and communication in order to function. Information and communications systems enable the grantor agency and grantees to capture and exchange the information needed to manage the grant program. In order to determine if a grant is achieving what is intended, those responsible for the grant program must have the right information, at the right time, and it must be reliable. This communication is two-way. The grantor agency requires information in order to determine if the grantee is doing what was intended. The grantee needs to know what is expected, how it is expected to be done, what limitations there are, and what deliverables there are. Without clear information about goals, the grantee may not provide the expected product and/or service. Finally, the public needs certain information so that there is transparency and accountability for the program and public dollars entrusted to the agency.

Grant recipients are required to maintain systems capable of recording and reporting accurate and timely financial, participant and performance information. Such information is critical to the government's ability to determine whether grantees are delivering the required services and to hold them accountable for federal funds. Reporting inaccurate financial and performance information is a common problem. Obviously, a grantee has an incentive

to overstate program success. If not detected, poor performing entities receive additional funding as the government "throws good money after bad."

Don't assume that just because critical information has been identified or communicated that it has reached the people that need to know and that they understand it. Regular follow up is needed to ensure grantees understand all the requirements and limitations for operating their grant. This includes what costs are allowable and what is unallowable.

I am reminded of a lesson I learned very early in my career. While auditing a federal grantee. I had spent weeks at the grantee's office testing claimed costs. I was surprised at how many items of costs were clearly not allowable under the cost principles. At the conclusion of fieldwork and before leaving the grantee's offices, there was an exit conference to go over the findings. The grantee officials listened intently at each finding that was presented. They took copious amounts of notes as each item was it terms of unallowable costs and on which section of the cost principles that was being applied. At the conclusion of the presentation, I asked the grantee officials if they had any questions. The first question they asked was what that cost principle document I kept referring to was and where could they get a copy. I told them they already had it—attached to their grant agreement. I then proceeded to walk them through their grant agreement. When they said they never realized it was there, I asked how they determined what types of costs were allowable under the grant. The consensus was that if an expense would be a legitimate business expense for their organization, then it would be a legitimate expense under the grant.

The lesson learned was to ask obvious questions and not assume. I learned not to assume that just because the requirements of the grant had been included as part of the written grant agreement that the people receiving it knew it was there, had read it, and understood it.

For the next grant audit, I asked at the beginning who determines what costs are charged to the grant and how do they determine it. Likewise, a grantor agency should not assume that just because they have included every requirement in a grant agreement that the grantee will realize the requirements are there and understand how to apply them.

Program officials need to take proactive steps to ensure that grantees know what is included in their grant and that they understand it. This can be done with post-award conferences and through monitoring visits. It can also be accomplished by the manner in which information is communicated—for example, use transmittal letters to highlight key requirements and expectations.

## MONITORING

Once risks have been assessed, controls have been put in place to address those risks, and information is flowing, the grantor agency must monitor the entire process to determine if the controls are working as intended. Monitoring allows the system to work dynamically, adjusting as necessary to changing con-

ditions, including changing risks. Since grant funds are spent by entities outside the federal government, appropriate and clear agency guidance, monitoring, and oversight of grantees are key to providing both financial and performance accountability.

The first steps toward ensuring adequate monitoring are to make sure that the agency's monitoring plan evaluates the items that comprise the essential framework for grant management as outlined above: control environment, risk assessment, control activities, information and communication. Monitoring is critical to identifying what is not working so that the same mistakes are not repeated in future grants. It is equally important to identify what is working so that best practices can be replicated in future grants.

Monitoring is generally thought of as the grantor agency monitoring its grantees. This is true; however, monitoring in the sense of sound internal controls also includes monitoring the grantor agency's operations as well. Monitoring should encompass the entire grant program—at the federal level, the grantee level, and

the ultimate recipient or beneficiary of the program. Monitoring should be designed to determine that the program as a whole is working as intended and achieving the desired results, not just an individual grantee.

Monitoring should also be a continuous process, not a one-time event. Monitoring and oversight, along with the other elements described in this article, must be consistent and frequent.

## CONCLUSION

Effective grants management requires picking the best service providers, making expectations clear to grantees, ensuring that success can be objectively measured, providing active oversight, evaluating outcomes, and using the successes and failures to improve the program. It is imperative that federal agencies exercise the most stringent level of oversight at all phases of the grant process to ensure that federal dollars are spent effectively and that citizens receive the services and results they deserve. As agencies will be spending billions of dollars under the Recovery Act, stringent oversight is all the more critical. ❁

---

**Elliot P. Lewis** is the Assistant Inspector General for Audit of the Office of Inspector General, U.S. Department of Labor. As the Assistant Inspector General for Audit, Elliot is responsible for and provides overall leadership to the Office of Audit. He is responsible for all audits within the Department of Labor including all financial and performance audits covering employment and training services, unemployment compensation, workers' compensation, workplace safety standards and oversight, mine safety standards and oversight, as well as many other services to protect the American workers. Prior to his appointment as AIGA, he served as the Deputy Assistant Inspector General for Audit.

Mr. Lewis joined the U.S. Department of Labor in 1991 as an Assistant Director of the Office of Financial Management Audits. He was promoted to the position of Director, Office of Financial Management Audits in 1996. In 2000, Mr. Lewis became the Director, Office of Audit Operations.

# Elliot P. Lewis



[OUTREACH]

# Department of Defense Fraud Awareness Initiatives

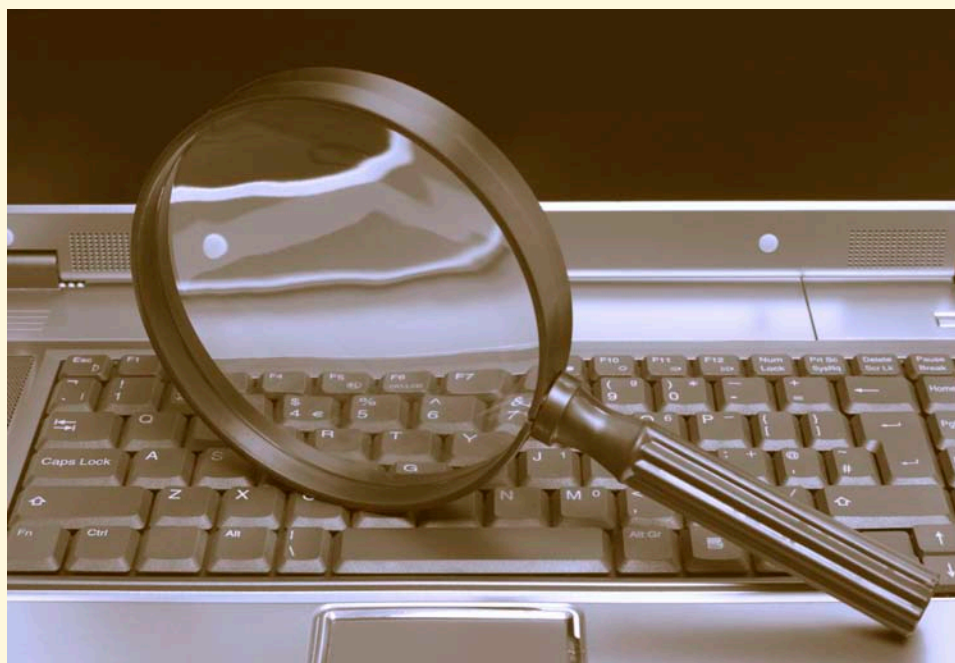
Increased procurement spending has unfortunately resulted in a new generation of fraudsters

BY FRANK ALBRIGHT, RUSSEL GEOFFREY, LAUREN MCLEAN

Within the federal inspector general community, fraud schemes, especially in the area of procurement fraud, have risen steadily in recent years. Defense budgets and procurement activity have risen dramatically, increasing from \$304 billion in fiscal year 2000 to almost \$700 billion in fiscal year 2008. This increased procurement spending has had the unfortunate result of producing new fraud schemes and a new generation of fraudsters. With so much at stake, it is critical that the Inspector General community remain vigilant in combating fraud, waste, and abuse in procurement as well as other high risk areas. And at the U.S. Department of Defense Office of Inspector General we are taking this fight to the next level.

First, we've set goals focused on punishing and detecting fraud, waste and abuse include:

- Realizing savings in defense contracting;
- Reducing corruption and cost overruns;
- Reforming acquisition management;
- Reducing fraudulent acquisition practices;
- Increasing oversight of procurement practices in the warfighting environment;
- Rebuilding the acquisition workforce; and
- Prioritizing prosecution to deter fraud, waste, and abuse.



Second, DoD IG, in partnership with the National Procurement Fraud Task Force, Panel on Contracting Integrity,<sup>1</sup> DoD Procurement Fraud Working Group, and DoD component organizations have several new initiatives aimed at educating the Inspector General and

<sup>1</sup> Section 813 of the John Warner National Defense Authorization Act for fiscal year 2007, Public Law 109-364, directed DoD to establish a Panel on Contracting Integrity that is responsible for conducting a department-wide review of progress made by DoD to eliminate areas of vulnerability in its contracting system. The Panel established 10 subcommittees that include the Procurement Fraud Indicators Subcommittee, chaired by the DoD Assistant Inspector General for Acquisition and Contract Management. The subcommittee members include representatives from Army Audit Agency, Air Force Office of Special Investigations and the Navy Acquisition Integrity Office.

DoD communities on methods to detect, prevent, and investigate fraud, waste, and abuse in procurement and other high risk areas such as health care and workers' compensation. The various DoD initiatives include training classes, conferences, and on-line resources for contracting professionals, attorneys, investigators, and auditors.

## HIGHLIGHTS OF NEW DOD TRAINING OPPORTUNITIES AND FRAUD RESOURCES... MORE THAN ONE TO CHOOSE FROM

DoD IG, in partnership with the Panel on Contracting Integrity, Procurement Fraud Indicators Subcommittee, has developed several new initiatives to educate auditors, attorneys, investigators, and



contracting professionals about fraud. The new initiatives include:

- The October 2008 launching of the “Fraud Indicators in Procurement and Other Defense Activities” Web page;
- Partnering with the Defense Acquisition University to develop online training for contracting professionals, and
- Hosting its initial fraud conference at DAU, Fort Belvoir, Virginia.

We are also sponsoring a special training session at the DoD Procurement Fraud Working Group’s Annual Training Conference.

### DOD IG RESOURCES FOR CONTRACTORS

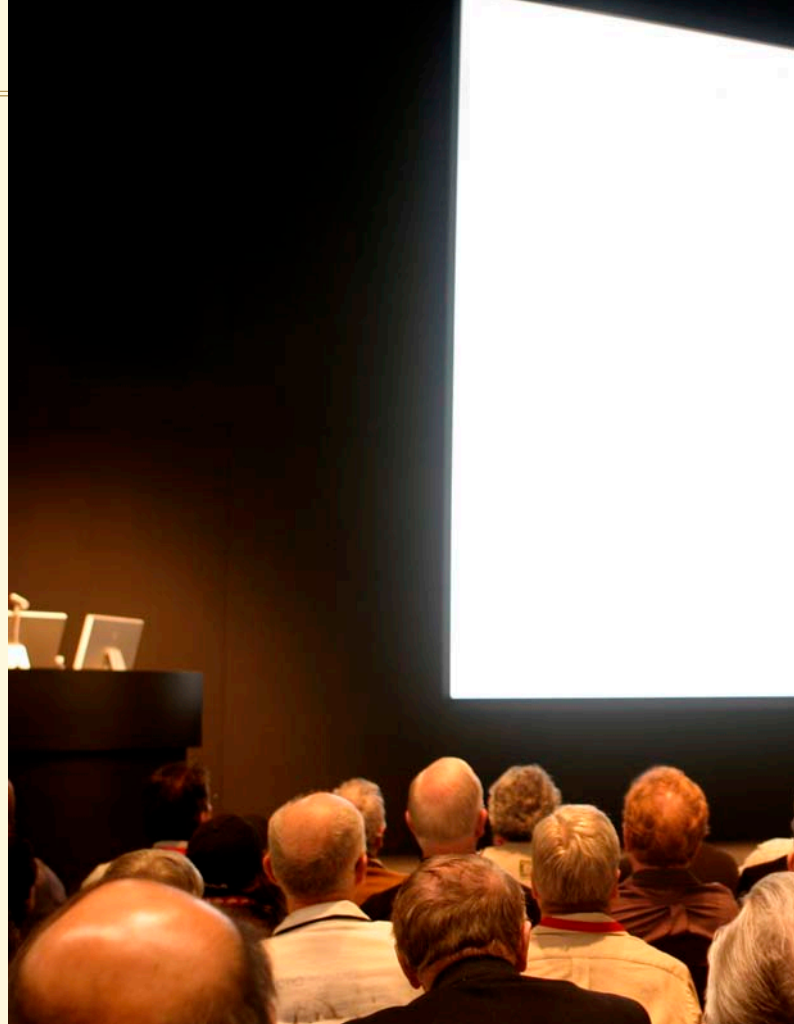
Other new DoD IG fraud resources include the Office of Investigative Policy and Oversight’s new Contractor Disclosure Program, which was developed to ensure compliance with recent changes to the Federal Acquisition Regulation (FAR Case 2007-006). The purpose of the Contractor Disclosure Program is to:

- Afford contractors a means of reporting certain violations of criminal law, violations of the civil False Claims Act, or significant overpayments discovered during self-policing activities; provide a framework for government verification of the matters disclosed; and
- Provide an additional means for a coordinated evaluation of administrative, civil, and criminal actions appropriate to the situation.

IPO created a link on the DoD IG, Web site ([www.dodig.mil](http://www.dodig.mil), click on the icon bearing the program’s name) which includes information about the new reporting requirements, a sample DoD Contractor Disclosure Submission Form, and contact information for contractors wanting to make a disclosure or obtain additional information about the program. IPO has also initiated several outreach efforts to assist with educating the DoD community and other organizations about the new reporting requirements.

### NEW FRAUD WEB PAGE

The “Fraud Indicators in Procurement and Other Defense Activities” Web page ([www.dodig.mil/inspections/apof/fraud/index.htm](http://www.dodig.mil/inspections/apof/fraud/index.htm)) has a variety of useful tools for the inspector general community and anyone that would like to learn more about fraud, waste, and abuse. The Web page was developed by the DoD IG’s Audit Policy and Oversight group and the Subcommittee with the assistance of more than 35 DoD agencies and components, as well as the American Institute of Certified Public Accountants. Other federal agencies that participated



# Department of Defense Tr

in this endeavor included the Government Accountability Office, U.S. Agency for International Development Office of Inspector General, and the Special Inspector General for Iraq Reconstruction. During the project, interviews were conducted with a variety of technical experts such as auditors, investigators, attorneys, and contracting professionals which resulted in 40 fraud scenarios and related indicators in 10 different areas. The fraud scenarios and indicators cover a variety of topics such as contracting, in-theater and retail operations, health care, and workers’ compensation.

Additional resources located on the web page include fraud guidance for auditors, fraud handbooks developed by DoD and other federal agencies, information on upcoming fraud training opportunities, and useful links. An interactive “Test Your Fraud IQ” link was recently added for those interested in getting feedback on their knowledge of fraud, waste, and abuse. The web page will be updated periodically with new “Fraud IQ” tests, fraud scenarios, and indicators. The DoD IG is currently developing a fraud dictionary for the web page which will include information on common fraud terms and schemes. Web site visitors are encouraged to submit comments, provide feedback, or submit a fraud scenario.



# Training in Fraud Awareness

## ON-LINE FRAUD TRAINING FOR CONTRACTING PROFESSIONALS

Another DoD IG/Subcommittee initiative is the development of online training for contracting professionals. The training will be available to anyone that would like to learn more about ways to prevent, detect, and identify acquisition fraud. The training is especially useful for persons working in the acquisition field such as contracting officers and program managers; however auditors, investigators and attorneys are encouraged to take part in the training which will take one or two hours to complete. The training is presented through a series of modules that address a variety of acquisition-related fraud topics and will be available at the DAU Web site ([www.dau.mil](http://www.dau.mil)) starting in April 2009. Additionally, the DoD IG's Audit Policy and Oversight group is working with DAU to prepare a series of short video clips that will be available for viewing at the beginning of each training module.

Highlights of topics included in the training are:

- More than 15 acquisition fraud scenarios covering topics such as defective testing, false invoices and false claims
- Information on common fraud schemes and related indicators

- Overview of criminal, civil, and administrative penalties and remedies
- Information on investigative agencies that should be contacted if fraudulent activity is suspected
- Links to fraud handbooks and other fraud resources developed by DoD agencies
- Opportunities for participants to test their knowledge of fraud schemes and indicators.

Persons completing the training will qualify for continuing professional education credits depending on the requirements of their field or license.

## UPCOMING DOD SPONSORED FRAUD CONFERENCES

### *DoD Procurement Fraud Working Group Annual Training Conference*

Recognizing that procurement fraud is of national significance and poses a threat not only to personnel safety, but also places at risk enormous taxpayer dollars, the DoD Procurement Fraud Working Group was established to develop a closer working relationship among the relevant DoD activities and agencies involved in the identification, investigation, and prosecution of contractor fraud. Its mission is to bring together experienced supervisory fraud agents, attorneys and auditors within the DoD enforcement community in a forum of information

exchange, legislative/policy development, and continuing education in regard to current issues, future national trends, investigative strategies, appropriate remedies,

and enforcement problems in the procurement fraud arena. It is intended not only to provide a real exchange of information and ideas among the various DoD agencies, but to also to provide enhanced interagency coordination, communication and cooperation with the U.S. Department of Justice and other government agencies combating procurement fraud.

The group, which was formed about five years ago, has hundreds of members, and a Steering Committee of approximately 20 members meets monthly. Members include lawyers, investigators, auditors and policy personnel from Army, Navy, Air Force, the Defense Logistics Agency, the Defense Contract Management Agency, the Defense Contract Audit Agency, National Aeronautics and Space Administration, the Criminal and Civil Divisions of the DoJ, the National Reconnaissance Office, and the Office of the Secretary of Defense.

This year's conference will be held during spring 2009, and attendance will be capped at 150. A link will soon be up on the DCMA web site, [www.dcmamail.com](http://www.dcmamail.com), to register. This year, as a change from past years, there will be fewer "talking head" presentations and more smaller-group discussions looking at the entire fraud investigation process from referral to comple-



tion, with a view towards identifying problems in the coordination of fraud remedies. Represented in these groups will be agency fraud counsel, auditors, procuring contracting officers/program managers, administrative contracting officers, DoJ criminal and civil lawyers, and debarment officials. On the last day there will be a panel comprised of legal counsel of major Defense contractors.

### ***Defense Acquisition University Hosts Fraud Conference***

The DoD IG, in partnership with the Subcommittee, will sponsor its initial fraud conference at DAU during the summer 2009. The conference will provide information on emerging issues and trends in the areas of fraud, waste, and abuse. Separate learning tracks will be available for auditors, investigators, attorneys and contracting professionals. The event will include interactive break out sessions, opportunities to obtain information on fraud from a variety of subject matter experts, and networking opportunities. Sample conference topics include:

- Information on the new mandatory disclosure requirement for contractors;
- Methods to identify fraud in the procurement process;
- Highlights of recent DoD procurement fraud cases;
- Fraud and corruption in the combat environment: highlights of fraudulent activity in Iraq and Afghanistan;
- An interactive “Solve the Scenario” session;
- Tips for auditors on making referrals to investigative agencies;
- Fraud risk assessment techniques for auditors

Information on this conference will be available on the “Fraud Indicators” web page. A sample conference agenda and speaker biographies will be posted for viewing during conference planning. An on-line registration form will also be available on the web page in early spring 2009. The conference is free to attend

and continuing professional education credits may be earned depending on the requirements of each specific field and/or professional license. The conference has space for 350 attendees so early registration is encouraged. Approximately 50 spaces will be reserved for contracting professionals and all registrations will be processed on a first-come, first-serve basis. If you are interested in suggesting a conference topic or would like more information about the event, please visit the following link: ([www.dodig.mil/inspections/apo/fraud/index.htm](http://www.dodig.mil/inspections/apo/fraud/index.htm))

### **DOD IG’S NEW CONTRACTOR DISCLOSURE PROGRAM**

With prompting from the Department of Justice and direction from legislation known as the “Close the Contractor Loophole Act,” the Federal Acquisition Regulation was revised on December 12, 2008 (*see*, 73 F.R. 67064). Stemming from FAR Case 2007-006, contractors are now required to strengthen their internal controls and codes of business ethics. The rule provides for the suspension or debarment of a contractor for knowing failure by a principal to disclose, in writing, to the government, credible evidence of fraud or criminal activity related to procurement fraud laws including the civil *False Claims Act*, or significant overpayments.

From 1986 until now, contractors wishing to disclose potential fraud to the DoD have been encouraged to make voluntarily disclosures to participate in the Voluntary Disclosure Program, which is managed by the DoD IG. While that program has resulted in recoveries of nearly \$500 million to date, participation in recent years has dwindled to approximately 10 disclosures per year, down

significantly from a high of nearly 60 disclosures in 1988. Feedback from major DoD contractors indicated that many disclosures were being made to contracting officers instead. Based on feedback from the DoD IG, the DoD and others, the DoJ was moved to recommend to the FAR Council that disclosures of fraud be made mandatory.

IPO has responded to the new requirement by transforming its once-voluntary program into a new mandatory one, simply titled the “Contractor Disclosure Program.” As was done previously, the program will receive disclosures of potential fraud and ensure they are fully coordinated with all affected DoD components: the Defense Contract Audit Agency; the Defense Contract Management Agency, the suspension and debarment authorities of the Defense Logistics Agency and the military departments, the defense criminal investigative organizations<sup>2</sup>, the criminal and civil divisions of the DoJ, and the individually affected contracting officers. With input from

<sup>2</sup> Includes the Defense Criminal Investigative Service, the Army Criminal Investigation Command, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.







and the Congress.

IPO has collaborated with many groups in the formulation of the Contractor Disclosure Program and in its “marketing.” IPO represented the Principal Deputy Inspector General of the DoD in cochairing the Contractor Integrity Reporting Committee of the National Procurement Fraud Task Force, along with the Inspector General of the National Reconnaissance Office. That committee, with strong representation from the DoJ, General Services Administration, and the NASA, was instrumental in coordinating the federal government response to the new FAR requirement.

those offices, IPO will refer the matter to the appropriate organizations to ensure action is taken that best fits the circumstances of the individual disclosure and the best interests of the DoD and DoJ. IPO will also provide program reporting internally within DoD, and to the DoJ

Since the new regulation was promulgated, IPO has been busy participation on panels and providing briefings to the American Bar Association, the American Conference Institute, the Defense Industry Initiative, and DLA attorneys. Upcoming presentations include DCMA

attorneys and the National Defense Industrial Association.

### DOD FRAUD INITIATIVES... OPPORTUNITIES TO INCREASE YOUR FRAUD AWARENESS

The various DoD fraud initiatives described in this article highlight the DoD’s ongoing commitment to combating fraud, waste, and abuse in procurement and other high-risk areas. The Department encourages the Inspector General and procurement communities to participate in any or all of the training venues and conferences offered during 2009. The DoD IG encourages challenge all attorneys, investigators, auditors, and contracting professionals to:

- Visit the “Fraud Indicators in Procurement and Other Defense Activities” Web page and take time to review the available resources and take the “Test Your Fraud IQ” quiz
- Learn more about procurement fraud indicators and schemes by participating in the DAU online fraud training
- Attend DoD sponsored conferences: DoD Procurement Fraud Working Group Conference or the DAU Hosted Fraud Conference
- Visit the DoD IG web page to learn more about the new Contractor Disclosure Program; and
- Visit the Defense Contract Management Agency, Contract Integrity Center’s webpage (<http://home.dcmac-y/index.htm>) to review fraud indicators, DOD newsletters and various tools used to fight fraud and help in fraud investigations.

We look forward to working with you to help prevent and detect fraud and abuse within the DoD, and to collaborate with other fraud-fighting professionals outside DoD, as we collectively advance the cause of ethics and accountability. It is a collective responsibility that will require the continued collaboration of fraud fighting professionals both within and outside DoD.





# Frank Albright

**Frank Albright** is the Director of Policy and Programs, within the Office of Investigative Policy and Oversight of the Office of Inspector General or the Department of Defense. In that capacity, Special Agent Albright directs the establishment of policy affecting the Defense Criminal Investigative Organizations including the Defense Criminal Investigative Service, the Army Criminal Investigation Command, the Naval Criminal Investigative Service, and the Air

Force Office of Special Investigations as well as other investigative and law enforcement organizations in the Defense agencies and the Military Departments. Programs under Special Agent Albright's cognizance include the OIG Subpoena Program, responsible for oversight of between 300-400 subpoenas issued annually in support of Defense investigations; and the DoD Contractor Disclosure Program, which provides a formal mechanism for the intake and coordination of disclosures of potential fraud made by Defense contractors either voluntarily, or as required by law or regulation. Special Agent Albright accepted his position with the OIG following a distinguished career as an Air Force officer and special agent/criminal investigator with the AFOSI.

---

**Russel Geoffrey** has been a member of DLA/DCMC/DCMA since 1991, and has held his position as Director of the Defense Contract Management Agency's Contract Integrity Center since its inception in May of 2000. In this position he manages a staff of six other attorneys and support personnel that have the agency-wide mission of coordinating fraud remedies and assisting in the prevention, detection, investigation and prosecution of fraud and other irregularities.

# Russel Geoffrey



**Lauren McLean** is an Auditor Technical Specialist in the Policy and Oversight component of the Department of Defense Inspector General. Prior to Audit Policy and Oversight, Ms. McLean was an audit team leader within the Defense Financial Auditing Service of the Office of the Inspector General DoD beginning in April 2005. From December 2002 to April 2005, she was a lead auditor at the United States Agency for International Development OIG where she worked in the Financial Audits Division on segments of the annual Government Management Reform Act audit during FY 2003 and FY 2004. Ms. McLean's diverse background also includes experience as an auditor at Madole Wagner, PLLC and Kerry J. Patton, CPA. She also worked for several years as a staff auditor with the City of Tulsa, Internal Auditing Department.



# Lauren McLean



[OUTREACH]

# Iraq's Inspectors General: A Work in Progress

## Public Corruption is endemic in Iraq

BY DANNY ATHANASAW AND  
CHRISTOPHER GRIFFITH

*No one at the ministry seems to know why I'm there or what I am supposed to do.*

*Everyone assumes we're just spies for the Americans... if we're too active, our minister will fire us. If I do my job, they'll kill me.*

-Concerns related by some Iraqi Inspector Generals and their staffs to U.S. Embassy – Baghdad officials, 2007.

### INTRODUCTION

Birthed in war, without precedent in peace, the Iraqi Inspector General system has struggled to find its place in post-Saddam Iraq. This article provides an overview of the system and assesses its chances for long-term survival.

### CPA ORDER 57

Coalition Provisional Authority Order 57, signed by Ambassador Paul Bremer on February 10, 2004, “established within each Iraqi ministry an Office of Inspector General . . . headed by an Inspector General.”

The IGs were initially appointed by Ambassador Bremer to serve a five-year term, which could be renewed for an additional five-year period. Upon the June 2004 restoration of full Iraqi sovereignty, the power to appoint IGs shifted to the Prime Minister's Office.

Under CPA Order 57, IGs “report directly to the relevant minister” and may be removed “only for cause.” CPA Order 57 remains the law of the land, although an Iraqi-drafted proposed replacement law is currently winding its way through the national legislature.



The duties of Iraqi IGs are strikingly similar to those of their American counterparts.

These include, but are not limited to: auditing the ministry's records and activities; conducting administrative investigations; receiving and assessing allegations concerning waste, fraud, and abuse that affect the ministry's interests; recommending corrective actions to the minister; and cooperating with investigative agencies and the judiciary in matters requiring their attention.

To accomplish these broad objectives, the IGs are supposed to be accorded “full and unrestricted access to all [ministerial] offices.” Further, Order 57 provides IGs with the power to subpoena witnesses and documents. Ultimately, the IGs are supposed to report their findings to their minister and issue an annual report to the Iraqi public.

### IRAQI ANTICORRUPTION INSTITUTIONS: A “THREE-LEGGED STOOL”

The CPA envisioned Iraq's IGs as one of that newly liberated country's three main anticorruption institutions. The other two are the Commission on Integrity, which has a limited law enforcement capacity, and the Board of Supreme Audit, which is roughly analogous to the U.S. Government Accountability Office. Importantly, BSA and COI are independent commissions under the Iraqi Constitution -- the IGs are not. This fact accords BSA and COI an additional layer of legal protection that the IGs do not possess.

CPA Order 55 established COI as Iraq's lead anticorruption agency. Under Order 55, COI possesses the statutory authority to investigate all allegations of public corruption and forward those cases which merit judicial action to the Central Criminal Court of Iraq. Addi-



tionally, COI is charged with educating the Iraqi populace about the dangers of corruption and drafting and administering financial disclosure regulations for all Government of Iraq employees.

CPA Order 77 outlines BSA's duties as Iraq's primary audit institution. BSA conducts regular financial audits of the GOI's ministries and reports its findings to COI and to the relevant IG. Unlike COI and the IGs, however, BSA was not created by the Coalition in 2004. Instead, it was founded during the British occupation of Iraq in the 1920s. BSA's longevity sets it apart from its brother institutions and leads it to guard jealously what it perceives as its prerogatives.

In this tripartite system, personnel from the ministerial OIGs are the only ones who have regular, daily involvement with the ministries. Therefore, they are often the first to uncover potential abuses or crimes. Thus, when an IG determines that a matter may involve corruption, fraud, embezzlement, or outright theft on the part of a ministerial employee, Order 57 requires the IG to refer this information to COI, along with whatever evidence the IG has gathered to date. COI then conducts further inquiries and determines whether the case should be forwarded to the CCCI for adjudication.

In practice, there are many problems with the flow of information among the anticorruption institutions. First, there is no established evidentiary threshold that triggers a case referral from an IG to COI. This has created substantial confusion. On occasion, COI thinks that certain IGs are being uncooperative because they forward little or any case data to COI while the IGs are often unsure how much evidence they need to gather before they send a case file to COI. Second, COI does not have the investigatory capacity to deploy its agents to the ministries to gather evidence and take testimony. COI usually just receives a file from an IG and then sends back a written list of questions for the IG to

answer, if he can. This exchange of paper – and all they use is paper – can drag on for years. Naturally, the OIGs often resent being asked to do COI's job. Third, institutional distrust often limits cooperation. In the post-Saddam era, acute political rivalries have seriously hampered the relationship between some IGs and COI's Commissioner. Fourth, BSA's has been somewhat reluctant participant in the U.S.-imposed anticorruption structure. BSA is often reluctant to provide its audit findings to the other two anticorruption agencies. Finally, no formal information sharing process exists. Data requests are usually handled in person and at the highest levels.

### IRAQI INSPECTOR GENERAL OFFICES - SOME CHARACTERISTICS

There are 35 IGs in Iraqi government. Most are housed within the GOI's ministries, with the remainder working at quasi-ministerial government entities, such as the Shia'a, Sunni, and Christian Endowments. OIGs range in size from the very small (the Ministry of Foreign Affairs OIG has approximately 20 employees) to the very large (the Ministry of Defense OIG is authorized a staff of several thousand, on paper). The budget to fund staff and other expenses comes from the ministry through the Ministry of Finance.

Little cross-office uniformity of internal structure exists among the various IGs. For example, some offices have relatively strict separation among administrative workers, auditors, and inspectors. Others rely more on *ad hoc* staffing arrangements. In these offices there usually is the IG, a principal aide or two, and an amorphous pool of "staff," which includes everyone from bodyguards, to drivers, to auditors. Additionally, since the Iraqi IG community is just over four years old, all IGs face the problem of finding qualified subordinates to accomplish their missions. OIG employees are drawn from

throughout the GOI. As elsewhere, nepotism often trumps qualifications leading to unqualified persons holding sensitive posts.

However, certain traits are common to all OIGs. For instance:

- Hotlines. All Inspectors General are required to operate an anonymous tip hotline that is accessible to all citizens. Often, this is little more than an irregularly-manned cell phone or a desk phone in the IG's office;
- The IG Council. This informal body has been in existence for several years. It provides all IGs with the opportunity to discuss and resolve issues common to the community; and
- Training requirements. The IG system needs basic training to achieve greater efficiencies and expertise in the areas of auditing, inspections, and investigations. Specifically, the IGs' auditors must receive training in general auditing skills so that they can actually perform audits on a regular basis. At the moment, most auditors have very little knowledge of performance auditing.

### UNITED STATES INVOLVEMENT

Since 2004, the U.S. government has supported a variety of efforts aimed at building the capacity of Iraq's IG system. Early on, the DoD led the way. DoD OIG deployed its first representative to Iraq in March 2004. In 2005, a team from DoD OIG's Investigations and Evaluations Directorate traveled to Baghdad to train and advise the OIGs from the GOI's two largest ministries, the Ministry of Interior, which controls all police forces, and the Ministry of Defense.

To this day, DoD, through the Multi-National Security Transition Command – Iraq, continues to train, mentor, and advise the MOI and MOD OIGs. On a relatively regular basis, personnel assigned to MNSTC-I provide several

weeks or months of classroom training on basic investigative topics to a class of mid-level employees from the two security ministries' OIGs. Certain Iraqi OIG personnel also receive a significant degree of "hands-on" mentoring from these U.S. advisors. Unfortunately, there are not enough advisors to mentor all those who would benefit from it, nor enough instructors qualified to train all those in need of training.

DoD's involvement with the Iraqi IG system has always been limited to two (MOI and MOD) of the 35 OIGs. From 2004 through early 2007, scant formal U.S. assistance was provided to any of the other OIGs. Meanwhile, the U.S. Department of State was pouring millions of dollars and dozens of personnel into capacity building efforts at COI. From 2004 through 2007 well over 40 American advisors – DoS, military, and contractor – worked with COI on a daily basis.

Finally, in early 2007, DoS appointed a Senior Consultant to Iraq's Inspectors General. He was responsible for training, mentoring, and advising all non-security ministry OIGs. Over the course of 2007, the Senior Consultant implemented several courses that covered the basics of what it meant to be an Inspector General and forged partnerships with various agencies and contractors (such as USAID and MNSTC-I) to deliver additional educational products to the Iraqi IG community. What he could accomplish was necessarily limited by the fact that he was one man responsible for more than 30 separate OIGs scattered throughout Baghdad.

## **MAIN ISSUES CONFRONTED BY IRAQ'S IGS**

One area where many OIGs have endeavored to make their presence felt is in the government contracting process. In Iraq, regulations governing procurement and contracting are byzantine and ever-evolving. There are many steps along the way where corrupt mid-level officials can arrange for kickbacks or broker sweet-

heart deals with firms owned by their friends and relatives. The sheer complexity of the rules often makes it difficult to track where the money even goes. Iraq's IG community recognizes these issues and seems committed to working with the ministries in order to enhance transparency and accountability in the contracting process. Many IGs are taking a more proactive role in reviewing contracts to ensure that procurement regulations are obeyed and that the money is actually spent on public goods.

A related issue of concern to the IGs is whether the goods delivered under the contract are, in fact, the actual deliverables specified in the contract. For instance, MOI and MOD frequently enter into arms contracts with outside vendors for the purchase of weapons and vehicles. In years past, the weapons and vehicles actually delivered to the GOI have often been so out-of-date or dilapidated that they were unusable. The IGs from MOI and MOD have begun to conduct inspections of such goods on a more regular basis in order to ensure that the weapons and material delivered to the armed forces are actually in working condition.

Similarly, Iraq's prisons are often in shockingly poor condition. Overcrowding and lack of food are but two of the issues faced by Iraqi correctional institutions. In an attempt to remedy these problems, the IG for the Ministry of Justice is now aggressively inspecting and reporting upon conditions in these facilities. The MOJ IG's actions reflect the concern for human rights that U.S. advisors have attempted to inculcate across the board among all Iraqi IGs.

## **COORDINATION EFFORTS**

Public corruption is endemic in Iraq. The SIGIR has referred to it as a "second insurgency." Consequently, the IGs are forced to dedicate significant amounts of their time to anticorruption initiatives. But if these efforts are to yield sustainable results, coordination among the three anticorruption agencies, while perhaps not sufficient, is most certainly necessary.

As a new institution, the IGs need to integrate more deeply with other, more established GOI agencies. Cognizant of this problem, the IGs established formal mechanisms to facilitate this desired coordination. In 2007, the GOI formed the Joint Anticorruption Council in 2007. Its members include the COI Commissioner, the BSA President, representatives from the IG community, and representatives from the Prime Minister's Office. The JACC is a coordinating body and does not have the power to set policy or allocate funds. Initially beset by political infighting, the JACC seems to be slowly evolving into a forum where the interested stakeholders can engage in a free and open exchange of ideas and opinions.

Another venue where this integration is occurring is in the Council of Representatives' Integrity Committee. The 275 member COR is Iraq's national legislature. Its Integrity Committee has oversight responsibility for the three anticorruption agencies. Recently, the Committee has begun to engage more closely with the anticorruption institutions in an effort to define common priorities and resolve any differences in the most amicable manner possible.

In 2008, the United Nations began to take a more hands-on approach to dealing with Iraq's anticorruption institutions. The UN is currently assisting the IGs, COI, and the BSA with training their personnel and drafting new anticorruption laws. Thanks to the improved security situation in Iraq, most of this training now occurs in Baghdad as opposed to Amman, Jordan or elsewhere overseas.

## **SUCCESSSES AND CHALLENGES**

Iraq's IGs struggle with a unique set of problems. In addition to the universal concerns voiced by government workers throughout the world, such as not having a large enough budget or a sufficient number trained staff, Iraq's IGs are still struggling to learn what it means to be an Inspector General. As Iraqi IGs go

about defining their roles within the GOI, they face opposition from powerful stakeholders who do not enjoy the thought of non-partisan oversight.

The security environment in Iraq – though improving – has adversely impacted the IGs' ability to do their jobs. A number of OIG staffers have died in the violence and countless more have seen their family members kidnapped, wounded, or killed. Additionally, innumerable man-hours have been lost to checkpoints, car bombs, blackouts, curfews, and the very human hesitation that one confronts when deciding whether to commute down highways colloquially referred to as "IED alleys." Progress, and the lack thereof, must always be judged in light of these facts.

Today, an OIG is functional in every Iraqi ministry. Considering that the entire concept of Inspectors General was only introduced to the Iraq in 2003-04, this is a significant achievement in and of itself. But moving beyond this threshold accomplishment, how successful has the introduction of an IG system to Iraq actually been? And what are the most severe challenges the IGs face during this period of transition to greater Iraqi control of all domestic institutions?

- **Coordination with COI and BSA:** This would include clarifying, preferably through a formal memorandum of understanding, audit responsibilities between BSA and the IGs. Right now, it is unclear which institution audits which programs. Such coordination could be accomplished through the JACC, but since the governing statutes (the CPA Orders and their eventual Iraqi-authored replacements) would be impacted, the COR's Integrity Committee should also play an active role.
- **Planning:** The individual IGs have only recently begun to grapple with planning for the future. To date, outside of MOI and MOD, little long-range strategic planning has been done. Budgets, hiring plans, and audit programs all need to be refined and set down on paper.

- **Training:** The Coalition has provided very basic training to the IGs and their staffs, but these initiatives are now winding down. The GOI has also funded various training programs, but needs to arrange for more advanced and in-depth instruction. Without competent subordinates, no IG can be expected to function effectively.

- **Budget Security:** Currently, the various OIGs receive their budget from their ministry. This impinges on their independence and hampers their ability to plan for the future. Improvements in this area will require the cooperation from the Ministry of Finance and the COR.

- **Pensions and Retirement:** The pension of an IG who retires today would be based on the salary he drew at his previous government job. This is usually significantly lower than his pay as an Inspector General. This makes it difficult to attract skilled recruits from other GOI agencies. This issue will become more and more of a problem as new IGs are named over the coming 12 months.

- **Continuity and Succession:** The five-year terms of the initial batch of IGs will expire in 2009.

The Prime Minister's Office will then renew or replace IGs' whose terms have expired.

Finally, Iraq's IGs are at risk of hyper-politicization. Elements within the GOI recognize the potential of the IG system and are trying to seize control of it in furtherance of their own political goals and objectives. It is imperative the Inspectors General retain their individual independence and that no single IG comes to dominate his peers. It would be especially damaging if the IGs were to fall under the control of a person or entity with close ties to the head of government. Such a situation with approximate the state of affairs under Saddam Hussein and undercut the central philosophical principle behind the entire concept of Inspectors General - independence.

## OUTLOOK

Right now, the COR is discussing a draft law that would replace CPA Order 57. This bill attempts to delineate clearly the IGs' roles as they relate to COI and BSA. It also clarifies the IGs' powers and some aspects of their internal office operations. When this bill will ultimately become law, and what it will look like when it does are, is uncertain.

Overall, the Iraqi Inspectors General have come a long way since 2004. The most progress has been made in the security ministries, where the U.S. advisory effort has been concentrated. The GOI must commit itself to sustaining these gains as U.S. support inevitably decreases. Other IGs, such as the IG for the Ministry of Justice, have also accomplished a great deal under challenging circumstances.

Recent improvements in the security environment have afforded the IG community with the breathing room it needs to focus on hiring and training qualified staff, engaging with the COR on crucial legal reform issues, and broadening and deepening its relationships with COI and BSA. Under Saddam, the ruling clique had a veritable license to steal. And while corruption still plagues Iraq, the IGs have taken the first modest steps toward revoking that license and safeguarding the riches of Iraq for future generations. ❧

*- Dr. Danny L. Athanasaw and Mr. Christopher M. Griffith. The authors served with the U.S. Department of State in Embassy Baghdad's anticorruption office, where their portfolio included advising Iraq's Inspectors General. Dr. Athanasaw spent approximately thirteen months in Iraq (2007-08) and Mr. Griffith spent more than two years there. Both authors currently work with the Special Inspector General for Iraq Reconstruction in Virginia. This article is based on their personal observations made during their time with the Department of State in Baghdad.*





# Danny Athanasaw

**Danny L. Athanasaw** joined SIGIR as its Chief of Staff in March 2008. He advises the Inspector General on a broad range of managerial and technical issues related to SIGIR's mission. His responsibilities also include strategic planning and the formulation of all internal policies.

Previously, Dr. Athanasaw served in Baghdad as the Department of State's Senior Consultant to the Iraqi Inspectors General. In that capacity, he counseled, trained, and mentored more than two dozen Iraqi IGs on ethics, transparency, investigations, inspections, and audits. As the Senior Consultant, Dr. Athanasaw built relationships between Iraq's IGs and a wide array of U.S. and international institutions, including: the President's Council on Integrity and Efficiency, the United Nations, and the European Union. In the spring of 2007, the Department of State honored Dr. Athanasaw for his work in Iraq by presenting him with its Meritorious Honor Award.

Prior to joining the Department of State, Dr. Athanasaw held a variety of senior positions within the Department of Treasury's Office of Inspector General. There, he regularly conducted detailed reviews of the Department's finances and operations. He also managed the Inspectors General Auditor Training Institute where he supervised the training of up to 1,500 auditors and evaluators from federal and local governments. In all, Dr. Athanasaw has over 35 years of experience in the federal government.

Dr. Athanasaw received his B.A. from the University of Tampa, his M.S. in Administration from Central Michigan University, and his Doctorate in Public Administration from Nova Southeastern University. He also taught undergraduate and graduate courses in accounting before deploying to Iraq in 2007.



**Christopher M. Griffith** currently serves as SIGIR's Senior Program and Policy Manager. Prior to joining SIGIR, Mr. Griffith spent more than two years in Iraq with the U.S. Department of State. There, he served as a Senior Advisor to the Embassy's anticorruption and rule of law offices. Earlier in his career, Mr. Griffith spent several years working as a litigation attorney in New York City. He graduated with honors from Harvard and received his J.D. from Cornell Law School.

# Christopher Griffith



[TESTIMONY]

# Hard Lessons: The Iraq Reconstruction Experience

*Congressional testimony before the Commission on Wartime Contracting in Iraq and Afghanistan, Washington, D.C., February 2, 2009*

**BY INSPECTOR GENERAL  
STUART W. BOWEN, JR.**

Chairman Thibault and members of the Commission on Wartime Contracting in Iraq and Afghanistan, thank you for inviting me to testify on the latest lessons learned report from the Office of the Special Inspector General for Iraq Reconstruction entitled *Hard Lessons: The Iraq Reconstruction Experience*.

## INTRODUCTION AND BACKGROUND

SIGIR is the successor organization to the Coalition Provisional Authority Inspector-General, which was established by Congress in November 2003 at the same time that it provided \$18.4 billion for the Iraq Relief and Reconstruction Fund. The agency's mandate, which has been expanded several times by Congress, is to oversee more than \$50 billion dollars appropriated for the relief and reconstruction of Iraq. More than 90 percent of this money has gone into four principal funding accounts: The Iraq Relief and Reconstruction Fund, the Iraq Security Forces Fund, the Commander's Emergency Response Program, and the Economic Support Fund.

To fulfill its Congressional mandate, SIGIR conducts audits, inspections, and investigations. Our office also initiated a series of lessons learned studies to identify problems and propose solutions in human resources, contracting, and program management in Iraq. Today, SIGIR is releasing *Hard Lessons: The Iraq Reconstruction Experience*, a detailed account of the U.S. effort to rebuild Iraq from prewar planning in mid-2002 through the fall of



2008. Like SIGIR's three previous lessons learned reports, *Hard Lessons* is not an audit. Rather, it seeks to meet our congressional mandate to provide "advice and recommendations on policies to promote economy, efficiency, and effectiveness" in programs created for Iraq's relief and reconstruction.

The research for *Hard Lessons* comprised hundreds of interviews with key participants in the reconstruction effort and the review of thousands of documents. SIGIR reached out to every senior U.S. official involved in rebuilding Iraq and almost all agreed to be interviewed or provide useful responses to questions. In addition, SIGIR staff interviewed rank and file members of the military and civilian agencies as well as private contractors who carried out the work of Iraq's reconstruction. We talked with many Iraqi leaders, including Prime

Ministers Allawi and Ja'afari, to ensure that we understood the Iraqi perspective on the reconstruction program. *Hard Lessons* also drew on the body of SIGIR's audits, inspections, and investigations, as well as reports from other oversight agencies and investigative bodies.

At the outset of the reconstruction effort in 2003, Lieutenant General Jay Garner, who headed the Office of Reconstruction and Humanitarian Affairs, said that history would "judge the war against Iraq not by the brilliance of its military execution, but by the effectiveness of the post-hostility activities." *Hard Lessons* chronicles that postwar reconstruction and, as the title suggests, it has been very difficult. The United States government was unprepared and ill-equipped to mount a major contingency relief and reconstruction program in Iraq in 2003. For the last six years we have been on a

steep learning curve.

The U.S. taxpayer has paid for a wide array of programs and projects in Iraq, ranging from training the Iraqi army and police to building and repairing the country's infrastructure in the oil, electricity, water, justice, transportation, and health sectors. Appropriated funds have supported programs to build democracy, enhance the rule of law, and improve the ability of Iraq's national, provincial and local governments to execute their budgets. Some of these projects have succeeded, but, as *Hard Lessons* documents, many did not.

## CENTRAL QUESTIONS AND ANSWERS

The central questions addressed by this report are: why did the U.S. reconstruction effort so often fail to achieve its goals? And, what can our government do to ensure that it has the capacity to manage future contingency operations?

*Hard Lessons* answers the first question by reviewing the chronology of the reconstruction effort and examining the challenges our government faced as the rebuilding program expanded from the \$2.4 billion envisioned by prewar planners to twenty-five times that much. The report answers the second question by identifying 13 hard lessons we must learn from the Iraq reconstruction experience.

Former Secretary of Defense Donald Rumsfeld and former Secretary of State Condoleezza Rice have both said that United States government did not have the right structure for conducting contingency relief and reconstruction operations. Consequently, as Rumsfeld told SIGIR, "The U.S. government has had to rely on quickly assembled ad hoc efforts such as ORHA to coordinate reconstruction." Nearly everyone SIGIR has spoken with agrees that the United States must reform the way it manages relief and reconstruction.

The U.S. Congress has already passed an important reform measure with "The Reconstruction and Stabilization Civil-

ian Management Act of 2008". This act, which incorporates a number of recommendations made by SIGIR in our previous lessons learned reports, creates a structure to address the planning, personnel, and program management needs of contingency relief and reconstruction operations. *Hard Lessons* concludes with some recommendations to ensure that RSCMA fulfills its purpose.

Divided in five parts, *Hard Lessons* begins with the blinkered and disjointed prewar planning that occurred between September 2001 and April 2003 when ORHA deployed to Baghdad. Part Two covers the 14-month period during which the Coalition Provisional Authority governed Iraq. The CPA's ambitious vision, which focused on improving Iraq's infrastructure, became the foundation for a greatly expanded reconstruction program. The United States struggled over the next four years to develop and implement a strategy for reconstructing Iraq as a stable and democratic nation on the path to prosperity. Deteriorating security both informed and complicated every decision. Part Three, examines the repeated realignment of U.S. funding to address the grave security threats posed by an exploding insurgency. Employing a variety of tactics to address the growing violence the United States poured money and – finally – more troops into the country, all the while trying to rebuild Iraq's physical infrastructure, its security forces, and its capacity to govern. Part IV chronicles the strongly-resourced surge, and the rise of Iraq's role in its own reconstruction.

Part V lays out SIGIR's 13 major findings – the hard lessons of the Iraq reconstruction experience. These findings are grouped in three categories which cover the principles, organization and mechanics of contingency relief and reconstruction operations.

## FIRST PRINCIPLES FOR CONTINGENCY RELIEF

## AND RECONSTRUCTION OPERATIONS

The Iraq experience gives rise to five core principles that should form the foundation of preparing for contingency relief and reconstruction operations:

- Security is necessary for large-scale reconstruction to succeed;
- Developing the capacity of people and systems is as important as bricks and mortar;
- Soft programs serve as an important complement to military operations in insecure environments;
- Programs should be geared to indigenous priorities and needs; and
- Reconstruction is an extension of political strategy

### *Security is Necessary for Large-Scale Reconstruction to Succeed*

A successful reconstruction program requires a balancing of security, political, and economic interests. Reconstruction cannot proceed on a large scale without the requisite security to protect those responsible for implementing and overseeing projects. When embarking on a contingency relief and reconstruction operation, the U.S. government should analyze whether and at what costs those security risks can be mitigated. Projects should only proceed when senior leaders determine that the strategic objectives they seek to fulfill outweigh the risk of failure and the costs of mitigating security risks.

### *Developing the Capacity of People and Systems is as Important as Bricks and Mortar*

The CPA's reconstruction program focused chiefly on large infrastructure projects aimed at improving the delivery of essential services. Little of its money was set aside to boost government capacity. The failure to fund capacity building programs alongside infrastructure construction contributed to a crisis in sustainability that continues to this day. A robust capacity-development program implemented from the outset



of the reconstruction effort could have prevented this. Such a program should be an essential component of any future contingency relief and reconstruction operations.

### ***Soft Programs Serve as an Important Complement to Military Operations in Insecure Environments***

An emerging lesson from Iraq is that when violence is pervasive, soft programs – like those orchestrated by USAID and Provincial Reconstruction Teams – are especially important in advancing U.S. goals. Working through indigenous networks seems to increase community acceptance and provide a higher and more lasting degree of local security than military or private-security protection alone could achieve. Because such programs operate out of view of most U.S. personnel, the selection of metrics and careful monitoring of expenditures are critical to ensuring value for the U.S. taxpayer.

### ***Programs Should be Geared to Indigenous Priorities and Needs***

Host country buy-in is essential to reconstructions' long-term success. In many cases there was a lack of sufficient Iraqi participation in deciding how or what to reconstruct. Detailed joint planning with Iraqi officials – perhaps the most important prerequisite for success after security – only gradually improved over time.

### ***Reconstruction is an Extension of Political Strategy***

If war, as Clausewitz famously said, is an extension of politics by other means, so too is relief and reconstruction an extension of political, economic and military strategy. There is a big difference between pursuing reconstruction to catalyze long-term economic growth and deploying reconstruction to support a counterinsurgency campaign.

## **ORGANIZING THE INTERAGENCY SYSTEM FOR CONTINGENCY RELIEF AND RECONSTRUCTION OPERATIONS**

The U.S. Government did not have the administrative structure and regulatory framework needed to effectively mount a large-scale reconstruction program in Iraq. SIGIR has five major findings concerning the organization of relief and reconstruction operations:

- Executive authority below the President is necessary to ensure the effectiveness of contingency relief and reconstruction operations;
- The U.S. government should develop new wartime contracting rules that allow for greater flexibility;
- Uninterrupted oversight is essential to ensuring taxpayer value in contingency operations;
- An integrated management structure and management information system are needed to effectively oversee interagency reconstruction efforts; and
- Outsourcing management to contractors should be limited because it complicates lines of authority in contingency reconstruction operations.

### ***Executive authority below the President is necessary to ensure the effectiveness of contingency relief and reconstruction operations***

The role of executive authority – and the lack thereof – over interagency coordination lies at the heart of the failures in the Iraq reconstruction program. The question of who was in charge, both in Washington and in Baghdad, was fiercely contested throughout the reconstruction effort. The lack of unity of command in Iraq meant that unity of effort was seldom achieved. Too often, programs were designed to meet agency goals rather than U.S. interests. Stronger integration was needed not only between the military and civilian agencies, but also among the civilian agencies themselves. Reform efforts should press for the creation of structures that will promote the development of a unifying strategy with clearly delineated agency responsibilities and adequate authority to enforce its execution.

### ***The U.S. Government Should Develop New Wartime Contracting Rules that Allow for Greater Flexibility***

The U.S. needs contracting reform that enables U.S. dollars to be more effectively used in contingency relief and reconstruction operations. A “Contingency FAR” should be developed by the Congress and the executive branch. The standard FAR’s complicated contracting regulations, which can be further modified by agency rules, should be knitted into a single set of simplified, uniform rules for conflict environments that all contracting agencies would have to use. A much larger corps of well-trained and experienced contracting officers must be developed and maintained for deployment during all phases of contingency operations, including planning. Similarly, a diverse pool of contractors with expertise in post-conflict reconstruction should be pre-competed and pre-qualified to be available when a contingency operation begins.

### ***Uninterrupted Oversight is Essential to Ensuring Taxpayer Value in Contingency Operations***

In the absence of effective management by government officials, contractors in Iraq were often left in dangerous circumstances to carry out insufficiently defined contracts written by inexperienced contracting officers who lacked situational awareness. Uninterrupted oversight by inspectors general and the Congress – ac-

raised questions regarding what constituted an inherently government activity, and the extent to which oversight authority can be delegated to a contractor.

### **CONTRACTING MECHANISMS AND HUMAN RESOURCES IN CONTINGENCY RELIEF AND RECONSTRUCTION OPERATIONS**

SIGIR has identified three areas where the United States must improve its ability to harness the personnel resources it needs to implement large-scale reconstruction programs:

- The U.S. government needs a new human-resources management system capable of meeting the demands of a large-scale contingency relief and reconstruction operation;
- The U.S. government must strengthen its capacity to manage the contractors that carry out reconstruction work in contingency relief and reconstruction operations; and
- Diplomatic, development, and area expertise must be expanded to ensure a sufficient supply of qualified personnel in contingency reconstruction operations.

#### ***The U.S. Government Needs a New Human-Resources Management System Capable of Meeting the Demands of a Large-Scale Contingency Relief and Reconstruction Operation***

Supplying adequate numbers of personnel with the requisite expertise emerged as a critical bottleneck early in the reconstruction effort. Although personnel recruitment improved somewhat as the reconstruction enterprise matured, at no time were there sufficient numbers of experienced advisors to meet Iraq's critical capacity-building needs. Washington was unable to draw effectively on the extraordinary talent available in America to form a cadre of workers that combined private-sector expertise with academic knowledge and bureaucratic skill. Further, the failure to provide unambiguous authority to the Chief of Mission in NSPD 36 and the reluctance

of the several chiefs of mission to exercise their authority made the effective cross-jurisdictional management of personnel almost impossible. A uniform set of human resource rules that would apply to all federal personnel deployed for contingency operations is needed, as are stronger recruiting mechanisms, a large stable of ready-to-deploy personnel, and a plan for managing long-duration contingencies.

#### ***The U.S. Government Must Strengthen its Capacity to Manage the Contractors that Carry Out Reconstruction Work in Contingency Relief and Reconstruction Operations***

Once Baghdad fell and the looting began, the scope of reconstruction quickly overwhelmed the U.S. government's standing capacity to respond. The post-Cold War downsizing of USAID and military construction capacities increased the U.S. government's reliance on the private sector. Not even the Pentagon could mobilize contractors fast enough. The decision to reduce the number of warranted contracting officers during the ten years preceding the Iraq invasion proved particularly consequential. It became clear that the U.S. and international contractors hired by the Defense Department and the CPA were not ready to quickly mount a large-scale reconstruction operation in a dangerous security environment.

#### ***Diplomatic, Development, and Area Expertise Must be Expanded to Ensure a Sufficient Supply of Qualified Personnel in Contingency Reconstruction Operations***

The Iraq mission suffered from a shortage of personnel with diplomatic skills, language and cultural expertise, and development experience. The Iraq reconstruction experience illustrates the extent to which civilian agencies lack capacity to project power abroad. Cuts at USAID, for example, have halved the number of permanent government employees at that agency. To remedy this weakness, Secretary of Defense Robert Gates has called

complicated by adequately staffed quality-control and quality-assurance programs – is essential to ensuring the efficient and effective use of taxpayer dollars.

#### ***An Integrated Management Structure and Management Information System are Necessary to Effectively Oversee Interagency Reconstruction Efforts***

After the reconstruction program began in 2003, at least 62 offices and agencies played some role in managing projects. There were, however, no interagency project management and information systems that could coordinate the activities of the hundreds of firms and sub-contractors executing construction work orders at thousands of sites across Iraq. Integrated systems could have helped to ensure that programs and projects were planned and completed with effective communication, control, and cooperation.

#### ***Outsourcing Management to Contractors Should be Limited Because it Complicates Lines of Authority in Contingency Reconstruction Operations***

By law, contractors report solely to the government contracting officers or the designated representatives of the agency that awarded the contract. In Iraq, the proliferation of contractors serving as managers and advisors in each of the offices managing reconstruction projects



for a “dramatic increase in spending on the civilian instruments of national security.” The Congress and the President should consider a long-term strategy for building technical and area expertise in the government’s civilian diplomatic and development agencies and creating mechanisms for deploying such capabilities abroad in times of peace and crisis.

### REFORMING CONTINGENCY RELIEF AND RECONSTRUCTION OPERATIONS

On October 14, 2008, President George W. Bush signed into law, as part of the *National Defense Authorization Act, The Reconstruction and Stabilization Civilian Management Act of 2008*, the most significant congressional legislation to date regarding the structure of and planning for contingency relief and reconstruction operations. The Act places responsibility for preparing the civilian side of contingency relief and reconstruction operations within the Department of State and directs the Secretary of State, in consultation with the USAID Administrator, to develop an interagency strategy for executing reconstruction and stabilization operations.

RSCMA establishes in law reforms that President Bush began when he signed NSPD 44, which assigned the State Department the lead in managing government-wide civilian preparation for contingency operations. The State Department’s Coordinator for Reconstruction and Stabilization (S/CRS) now has the responsibility to monitor crises worldwide, prepare contingency plans, and recruit, train and equip personnel for relief and reconstruction missions. Without adequate funding and a large staff, S/CRS will not be able to accomplish the tasks assigned to it. Three things are necessary to fulfill RSCMA’s purpose:

**First, the Congress must provide appropriations suitable to meet the RSCMA mandate**

If Congress expects the RSCMA to succeed, it should consider funding the initiative.

**Second, more must be done to ensure that the interagency coordination and integration required by RSCMA actually occurs**

Even though the law now defines the role of the S/CRS, its ability to foster change across the government remains unproven and many of the same structural obstacles still exist. Contingency relief and reconstruction operations are not inherently the function of any single department.

The Defense Department, usually the largest player in contingency relief and reconstruction, has pursued its own course towards enhancing its capacities for such operations. DoD Directive 3000.05, issued in November 2005, provided that “stability operations are a core U.S. military mission” that “shall be given a priority comparable to combat operations and be explicitly addressed and integrated across all DoD activities.” The directive gave the military departments the responsibility to conduct contingency relief and reconstruction operations if civilian agencies cannot. In response to this directive the Army has made stability operations a central part of its doctrine, and the U.S. Army Corps of Engineers has strengthened its engineering support to combatant commands and enhanced its own capacity to deploy divisions specializing in post-conflict reconstruction. Nevertheless, progress towards meeting the DoD directive’s goals has been uneven.

**Third, the Administration should work to revise and integrate the civilian and military components of contingency and reconstruction operations**

The President and the relevant cabinet secretaries should ensure that all agencies – especially State and Defense – better integrate the structure and resources for contingency relief and reconstruction operations.

### UNITY OF EFFORT

The Iraq reconstruction experience makes clear that contingency relief and reconstruction operations require coordinated and cross-jurisdictional structures, planning, resources, and management. The Iraq endeavor fell short on many occasions because the absence of unity of command prevented unity of effort. Too often, agencies and offices worked in their respective stovepipes without ensuring that their activities fully supported U.S. goals and objectives. As General Petraeus told me, “State is never going to put an ambassador under a general, and DoD is never going to put a general under an ambassador.” A new integrated interagency system for contingency relief and reconstruction operations is necessary to ensure future success.

The Iraq reconstruction experience demonstrates that the U.S. government was neither prepared for nor able to respond quickly to the ever-changing demands of the contingency relief and reconstruction mission we faced. Reforms along the lines of – or going beyond – RSCMA are a prerequisite for future success. The inevitability of future contingency relief and reconstruction operations – whether they result from political conflicts or natural disasters – demands that the U.S. government develop new ways to prepare for the inevitable crises and project civil-military power to manage them.

The President and the Congress should take further steps toward achieving this goal. Time and resources must be devoted to developing a sound doctrine and to increasing the U.S. government’s capacity to conduct relief and reconstruction operations. Great effort, reflection, and imagination could put the Iraq reconstruction experience to good use by developing new approaches and structures build on the hard lessons learned in Iraq. ❧





# Stuart W. Bowen, Jr.

**Stuart W. Bowen, Jr.** was appointed Inspector General for the Coalition Provisional Authority in January 2004. Since October 2004, he has served as the Special Inspector General for Iraq Reconstruction. As the “taxpayer’s watchdog” in Iraq, Mr. Bowen oversees over \$47 billion in U.S. appropriated reconstruction funds, including the Iraq Relief and Reconstruction Fund, the Iraq Security Forces Fund, the Economic Support Fund, and the Commander’s Emergency Response Program.

Since January 2004, Mr. Bowen has made 20 trips to Iraq, managed the production of over 240 audits and inspections, issued 3 comprehensive lessons learned reports, and provided 15 quarterly reports on Iraq reconstruction to the Congress. In 2006 the President’s Council on Integrity and Efficiency awarded Inspector General Bowen and SIGIR the Gaston L. Gianni, Jr. Better Government Award for “demonstrating integrity, determination, and courage in providing independent oversight and unbiased review of United States’ reconstruction efforts in Iraq.”

Inspector General Bowen’s public service career includes service in The White House as Deputy Assistant to the President and Deputy Staff Secretary, Special Assistant to the President and Associate Counsel. From 1994 to 2000, he held a variety of positions on Texas Governor George W. Bush’s staff, including Deputy General Counsel, Deputy General Counsel for Litigation, and Assistant General Counsel. Mr. Bowen previously served as an Assistant Attorney General of Texas and as a Briefing Attorney to Texas Supreme Court Justice Raul Gonzalez. Prior to his appointment as Inspector General, Mr. Bowen was a partner at Patton Boggs, LLP, in its Washington, D.C. office.

Mr. Bowen is licensed by the Texas State Bar, Board Certified in Administrative Law by the Texas Board of Legal Specialization, and admitted to practice before the United States Supreme Court, several other federal courts, and all Texas state courts. Mr. Bowen served four years on active duty as an intelligence officer in the U.S. Air Force, rising to the rank of Captain. He holds a B.A. from the University of the South and J.D. from St. Mary’s Law School.



“ If war, as Clausewitz famously said, is an extension of politics by other means, so too is **relief and reconstruction** an extension of political, economic and military strategy. ”

-Excerpt from *Hard Lessons: The Iraq Reconstruction Experience Testimony* by Stuart W. Bowen, Jr. (p. 50-55)

# Commission on Wartime Contracting in Iraq and Afghanistan

<sup>1</sup>On July 18, 2007, Senators Jim Webb (D-VA) and Claire McCaskill (D-MO) introduced a bill to establish an independent, bipartisan Commission on Wartime Contracting to study U.S. wartime contracting in Iraq and Afghanistan. The bill was inspired by the work of the “Truman Committee” which conducted hundreds of hearings and investigations into government waste during and after World War II that resulted in an estimated savings of more than \$178 billion (in today’s dollars) to the American taxpayer.

This bill was the first joint initiative of freshmen senators, including Senators Webb, McCaskill, Amy Klobuchar (D-MN), Bernie Sanders (I-VT), Jon Tester (D-MT), Sherrod Brown (D-OH), Sheldon Whitehouse (D-RI), Ben Cardin (D-MD), and Bob Casey (D-PA). Majority Whip Senator Dick Durbin, Armed Services Committee Chairman Senator Carl Levin, and Senators Tom Carper, John Kerry, Diane Feinstein, Barbara Boxer, Barack Obama and Tim Johnson also served as co-sponsors of the original amendment, filed as no. 2206, to the National Defense Authorization Act (NDAA) for Fis-

cal Year 2008. Following a Senate floor debate September 27, 2007, the landmark provision won broad bipartisan approval and was incorporated in the defense bill.

Congressman John Tierney (D-MA) also introduced language similar to the Webb-McCaskill amendment in the House of Representatives in September 2007 as a stand-alone bill. The bipartisan legislation was supported by key taxpayer watchdog groups including: the Project on Government Oversight, Taxpayers for Common Sense, the Government Accountability Project, OMB Watch, Common Cause, U.S. PIRG, and Iraq and Afghanistan Veterans of America.

The FY2008 NDAA, originally identified as H.R. 1585,

was subsequently renumbered H.R. 4986 after H.R. 1585 was vetoed by President Bush on December 28, 2007. On January 16, 2008, H.R. 4986 was passed by the House of Representatives and, on January 22, by the Senate. The bill was signed into law by President Bush January 28, 2008. However, in signing H.R. 4986, the President identified a number of provisions of the Act, including section 841 (which establishes the Commission on Wartime Contract-

## Commission



Commissioners hear testimony at the Feb. 2, 2009, hearing. Left to right: Robert Henke, Clark Kent Ervin, Chairman Michael Thibault, Dov Zakheim, Linda Gustitus, Charles Tiefer

<sup>1</sup> [www.wartimecontracting.gov](http://www.wartimecontracting.gov), “Background Information and Chronology”



DoD Principal Deputy Inspector General Thomas F. Gimble shakes hands with Commission Co-Chair Michael J. Thibault after the hearing. In the background is Commissioner Clark Kent Ervin

ing), that he claimed “purport to impose requirements that could inhibit the President’s ability to carry out his constitutional obligations to take care that the laws be faithfully executed, to protect national security, to supervise the executive branch, and to execute his authority as commander in chief.” In his signing statement the President continued, “The executive branch shall construe such provisions in a manner consistent with the constitutional authority of the President.”

The law establishing the Commission defines a broad and substantive mandate. The Commission is required to study, assess and make recommendations concerning wartime contracting for the reconstruction, logistical support, and the performance of security functions in Iraq and Afghanistan. The Commission’s major objectives include a thorough assessment of the systemic problems identified with interagency wartime contracting, the identification of instances of waste, fraud and abuse, and ensuring accountability for those responsible.

Numerous audits, investigations, and congressional hearings have documented the magnitude of the problem. The Defense Contract Audit Agency estimated in 2007, for example, that there were more than \$10 billion in questioned and unsupported costs relating to the Iraq reconstruction and military support contracts valued at \$57 billion that it had reviewed. The agency noted that contracts worth \$300 billion remained to be audited.

Similarly, congressional testimony by the Department of Defense Inspector General (DoD IG) staff in May 2008 revealed that its review of 702 U.S. Army commercial payments in Iraq, Kuwait, and Egypt indicated the Army made an estimated \$1.4 billion in contract and vendor payments that lacked minimum supporting documentation and information for proper payment. When payments were not properly supported, the Army lacked assurance that funds were used as intended. The DOD IG also estimated \$6.3 billion in Army commercial payments had the minimum supporting documents and information for a proper payment, but lacked support needed to comply with various laws and regulations.

To achieve its objectives, the Commission is empowered to hold hearings, take testimony, receive evidence, and provide for the attendance and testimony of witnesses as well as the production of documents. The Commission is able to secure from any agency of the federal government any information or assistance that it considers necessary to enable it to carry out its mandate to study, assess, and to make recommendations to Congress on wartime contracting. The Commission is also empowered to refer to the U.S. Attorney General any violation or potential violation of law it identifies. The Commission is required to make two reports to Congress: an interim report in 2009, and a final report in 2010.



[SPEECH]

# Immigration Enforcement and Social Security: An IG Perspective

*Every year SSA receives 245 million wage reports from employers representing 4 trillion dollars in earnings*

**BY INSPECTOR GENERAL  
PATRICK P. O'CARROLL**

*Condensed from a speech delivered by Patrick P. O'Carroll, Jr., Inspector General for the Social Security Administration, on November 18, 2008 at a Federal Bar Association seminar, Worksite Enforcement and Immigration, Loyola University, Chicago, Illinois.*

It's a pleasure to be here with you in Chicago, and I'm honored to have been asked to speak. You've had a lot of excitement here in Chicago lately, from the Cubs' run for the World Series to a native son's first appearance as President-elect. I can't compete with such momentous events, but I do hope to give you an understanding of how the mission of my office intersects with the topic of your conference—workplace enforcement and immigration.

The federal government, with its nearly 3 million-strong workforce can feel somewhat amorphous, with only vague distinctions between one agency and the next. The truth, however, is that Congress has done a good job of giving Executive Branch agencies their own patches of earth to tend, so to speak.

For the Social Security Administration, that patch of earth is administering the programs enacted by the Social Security Act in 1935—as well as programs added to that mandate in the years since. One critical component of that mission involves the integrity of the Social Security number, or SSN. And as the uses of the SSN have expanded over the years, so has the number of places in which our



mission intersects with the missions of other agencies.

Today, we're discussing immigration, and where our jurisdiction intersects with that of Immigration and Customs Enforcement. But we could just as easily be talking about identity theft, where we intersect with the Federal Trade Commission, disaster-related fraud (such as in the wake of Katrina), where we intersect with FEMA, or any number of other areas in which the SSN is in play.

Before I go too far, though, I want to start by placing this discussion in context. I realize that some of you may not be familiar with the role of an inspector general or with our organization specifically. Then I'll zero in on how we work with the Social Security Administration, or SSA, and other agencies to combat SSN misuse in all of its forms, including

in the context of immigration and worksite enforcement.

Federal inspectors general serve as watchdogs over Executive Branch agencies, in an effort to increase public accountability and transparency in Government operations. Our mission is to help improve our agencies' programs and operations by conducting audits and investigations aimed at preventing and detecting fraud, waste, and abuse.

The Office of the Inspector General, or OIG, for SSA was created in 1995, when SSA became an independent Federal agency, separate from the Department of Health and Human Services. Today we are a team of 575 auditors, investigators, attorneys, and others which produced over 100 audit reports and closed over 10,000 investigations last fiscal year.

These are big numbers—but let me put

those accomplishments in perspective. We oversee an agency that manages the largest social insurance program in the world. Last year, SSA paid 614 billion dollars to over 50 million people. Our challenging mission is to protect and improve SSA's already well-oiled machine.

Each year, we receive upwards of 100,000 allegations of Social Security-related fraud, and I mentioned that last year, we closed over 10,000 investigations. Only about 9 percent of those cases were classified as Social Security number misuse, while 70 percent were related to fraud in SSA's disability programs—both Disability Insurance, which is an earned benefit, and Supplemental Security Income, for low-income disabled individuals.

Nevertheless, SSN misuse has certainly been one of our most enduring challenges over the 13 years of our existence. Despite its relatively smaller share of our caseload, maintaining the integrity of the Social Security number remains a key part of our mission, because of its role as the cornerstone of SSA's programs and operations.

This 9-digit identification number was created in 1936 for only one purpose: to uniquely identify individuals so that SSA could accurately track their earnings and contributions, and pay them benefits when the time came. Of course, we all know that today, Social Security numbers are used for much more than that original purpose. You are just as likely to have to supply your SSN to go to the doctor or buy a cell phone, as to report income to the IRS and Social Security or apply for retirement benefits.

As identity theft appeared on the horizon and became the crime of the new century, we found ourselves investigating more and more SSN misuse cases that had no true bearing on SSA's programs and operations. In recent years, however, I've led the OIG in an effort to focus our resources on combating only that SSN misuse which is directly linked to SSA's programs and operations.

We now generally refer identity theft allegations to those Federal, State and lo-

cal law enforcement agencies which have taken the lead on fighting bank fraud, mail fraud, and other identity theft crimes not directly related to Social Security. This refocusing of our resources has allowed us to more specifically target SSN misuse that directly affects SSA's programs and its beneficiaries. For example, we often find that individuals will misuse SSNs in connection with receiving government assistance, medical services, or other benefits.

Over the last 3 years, for example, we have participated on a Department of Justice task force dedicated to combating fraud related to Hurricanes Katrina and Rita. In the storms' wake, many individuals took advantage of the chaotic situation and defrauded disaster assistance programs. There were people who claimed they were living in a hurricane-affected area when they never had. Some individuals filed dozens of false claims using made-up names and SSNs. And many cases involved pure identity theft—someone pretending to be another individual who rightly deserved the funds.

Most of these cases involved some degree of Social Security number misuse, and we also found that many of those suspected of fraud against FEMA and HUD were also Social Security beneficiaries or SSI recipients. As a result, we have been involved in a number of task force investigations. Overall our hurricane fraud investigations have led to 52 convictions and the recovery of significant government funds.

Of course, Social Security number misuse also occurs for the purpose of obtaining a job in the United States. The need to maintain the accuracy and integrity of SSA's records gives the OIG a stake in identifying and preventing this type of SSN misuse. In fact, I believe our efforts are critical to maintaining the integrity of the entire Social Security system. That's because the system is based on SSA's ability to match workers' earnings to their Social Security records, so that when those workers become disabled or retire, they will receive the monthly

benefits they have earned.

Every year, SSA receives 245 million wage reports from employers, representing 4 trillion dollars in earnings. Americans must be confident in the knowledge that SSA will correctly record those earnings, and that they will get the full benefits due them. When earnings are incorrectly recorded, the individual worker and all taxpayers bear the cost of getting the record corrected.

Our work in this area reaches in many directions, and one of those paths intersects with the mission of Immigration and Customs Enforcement at the Department of Homeland Security. When employers or self-employed people report earnings on a W-2 form or 1099, SSA validates the name and Social Security number against its own records. When an earnings report contains a name or SSN that does not match SSA's records, and the discrepancy can't be resolved, SSA posts those earnings to a virtual repository known as the Earnings Suspense File, or ESF.

Sometimes the error is due to a simple discrepancy in SSA's records—for instance, when a woman marries and changes her name, but neglects to notify SSA. If her employer reports her wages under her new name, that name won't match up with her SSA record, so the Agency may post those earnings to the ESF. Of course, sometimes these errors are caught by the beneficiary, and the earnings record can be corrected.

However, most wage items remain in the ESF. As of October 2006, the ESF had accumulated about 586 billion dollars in wages and 264 million wage items. This creates an enormous resource drain for SSA and creates the risk that untold numbers of individuals will not receive the benefits they are due at retirement, upon becoming disabled, or as the result of another life-altering event.

We have conducted substantial audit work related to the Earnings Suspense File, in an effort to understand why wage reports end up in the file. The most well-known of those audits came up with a list of 100 employers with the most wage

items in the ESF, and analyzed those items for errors or SSN misuse. We found that many of the 100 employers were in the service, restaurant, and agriculture industries. We also found that SSN misuse seemed to be the reason for most of the mismatched records.

We then conducted an audit focusing on just the service, restaurant, and agriculture industries. We analyzed a sample of the wage reports in the ESF that were submitted by employers in these industries. Twenty-five percent of the SSNs had never been assigned, and 75 percent belonged to someone else—in fact, many belonged to young children or deceased individuals. That audit also found that 48 percent of wage items contributed by agricultural employers during the three-year period we reviewed failed to match SSA records.

Thus, while many of the ESF entries may be the result of simple error, we believe that the main contributor to the ESF is unauthorized work by noncitizens. Unfortunately, we also determined that there's little SSA can do to stem the tide of erroneous wage reports. Although we recommended that SSA assist IRS in developing an employer penalty mechanism, we're not aware that any such effort has been undertaken.

To this point, I've spoken about employment-related SSN misuse in general, but that broad term encompasses many variations. An individual may create an SSN out of thin air to supply to an employer, or use a deceased or living relative's number, or they may have bought a fake Social Security card on the street. In rare instances, they may have even acquired a genuine number from an SSA employee.

When an unauthorized worker uses an SSN that belongs to a living individual, that individual and SSA face administrative challenges in getting his or her earnings record corrected. And if the error is never caught or the record corrected, the true number holder may be paid the wrong amount of benefits, which over a lifetime could mean millions of dollars lost to taxpayers.

Another administrative challenge is posed by the fact that any unauthorized worker who later becomes authorized to work can go to SSA and request that wages in the ESF be attached to his or her earnings record. So even though the wages were earned and reported under another SSN, that person can qualify for benefits if they can prove that they earned the wages and are now authorized to work.

In light of the direct impact on SSA programs and operations, we do choose to participate with ICE to a very limited extent in worksite enforcement investigations related to employment-related SSN misuse. Specifically, we choose to participate only in those worksite enforcement operations where an employer is complicit in providing its workforce with fraudulent SSNs.

These employers harm the integrity of not only Social Security's records, but also its operations, by intentionally reporting false information year after year for dozens or even hundreds of individuals, and sometimes even by supplying counterfeit Social Security cards.

Even in those investigations we join, the OIG's role is often limited. But when we can stop employers from providing workers with fictitious SSNs or the SSNs of other people, the impact on SSA programs and operations can be significant.

In one egregious case, ICE requested our assistance with an investigation of a Boston company with a Department of Defense contract worth 100 million dollars. This company manufactured, among other things, bulletproof vests and backpacks for military personnel in Iraq and Afghanistan. ICE suspected the company's owner and plant managers of conspiring to hire unauthorized workers on a large scale.

We joined the ICE investigation, and in reviewing SSA's records, we found that over five years, the company had repeatedly failed to respond to SSA's correspondence informing them of erroneous wage reports. What's more, they never took any corrective action to prevent the

misuse. We discovered that up to 85 percent of the company's employees were using SSNs not assigned to them by SSA. As ICE pursued 360 unauthorized workers, our agents sought out and arrested the company's owner and three managers for conspiracy.

We also arrested a previously deported man who was running a counterfeit document enterprise out of a Boston-area storefront. The company was referring workers to the counterfeiter to obtain false documents that the company then accepted for hiring and wage-reporting purposes. The counterfeiter eventually pled guilty and was sentenced to time served, and transferred to ICE for deportation proceedings. The company's owner and managers also pled guilty and are awaiting sentencing in Federal court.

As you can see, our agents often find themselves working to combat document fraud, which can go hand-in-hand with SSN misuse. Unfortunately, there is a profit to be made by counterfeiting Social Security cards and immigration documents and selling them to unauthorized workers. As a result, the SSA OIG participates on ICE's Document and Benefit Fraud task forces in major U.S. cities, including Washington, D.C. There, as part of a continuing investigation known as Operation Card Shark, our agents have helped dismantle seven fraudulent document laboratories and secure convictions for 60 individuals to date.

As part of another task force led by State law enforcement officials, we also helped break up an extensive document mill operation run by MS-13 and other Latino gangs throughout New York City







and New Jersey. After months of undercover operations and surveillance, we arrested dozens of people, and seized thousands of fake Social Security cards.

As we delve deeper into these issues, we've found that many unauthorized workers have found a new way to slip through the cracks. In the past, they generally used fake documents containing invalid SSNs or SSNs that did not match the names on the documents. But now the trend is toward using entire identities of actual United States citizens.

Identity theft rings obtain personally identifiable information, and then sell documents containing these valid identities to unauthorized users. This new scheme has evolved as a way of circumventing employer verification services, which look for a match between the individual's name and SSN.

This is our newest employment-related challenge, because there's no way to identify this type of fraud unless the true number holder comes forward to report discrepancies in his or her earnings record. And because some of these number holders are children, we may not have that opportunity until they enter the workforce years from now.

Although detecting this fraud, and then investigating to a successful resolution, is difficult, we are making strides on audit and investigative fronts. For example, last September we released an audit assessing the validity of earnings posted

to the records of children ages 7 to 13. Although SSA flags earnings posted to records of children 6 or younger, this process does not cover ages 7 to 13.

We found that 88 percent of the earnings we reviewed did not appear to result from legitimate employment. Many of the employers were in industries that do not normally employ children, because they offer jobs not allowable for children under guidelines set by the Department of Labor.

SSA agreed with recommendations we made in that report, including that the Agency explore the idea of legislation to allow the disclosure of SSA information that may help other Federal agencies more effectively accomplish their missions. One such data-sharing effort already underway is the Department of Homeland Security's E-Verify program. Because SSA data is the foundation of this effort, we have been involved in evaluating and providing feedback.

In fact, last year, at the request of Congress, the OIG undertook three such evaluations, focusing on data accuracy and security. The first of these Congressional Response Reports, Accuracy of SSA's Numident File, has been oft-quoted by the media—and even more frequently mis-quoted.

In that study, we found errors in SSA's records that might result in what we call a "tentative non-confirmation" of an employee's work authorization. The media often cite that finding as evidence that E-Verify will cause innocent workers to be fired, and employers to be sued for discrimination.

Unfortunately, they're taking our findings out of context. Our auditors estimated that about 4 percent of all SSA's Numident records contained discrepancies in name, SSN, date of birth, or citizenship status that could result in a mismatch if submitted through E-Verify. What the media fail to mention is that our findings were based on a random sample of SSA's records, so many of those records belong to people whose SSNs were assigned decades ago. They are either deceased or retired, and would not

be applying for new jobs. Also ignored is the important fact that many of the errors are caused by individuals' failure to update their SSA

records when they get married or become legally authorized to work.

Of course, all Social Security numbers are vulnerable to misuse, but it's misleading to imply that using E-Verify will risk innocent employees' jobs. All employees would be given ample opportunity to correct their records with SSA before an employer could take any adverse action.

Nevertheless, we are fighting an uphill battle. No matter how many employers we arrest and how many audit reports we issue, we won't solve the problem of employment-related SSN misuse and discrepant earnings records until and unless we address our inability to share information among the various Federal agencies with a role in this process.

Rest assured that we will continue our audit work in these areas. We will continue our investigations, such as those I've described today. In particular, we will continue to pursue employers who knowingly provide false SSNs or documents to employees and false wage reports to SSA. And we will continue to work with SSA, Congress, and other agencies to make these efforts more effective.

I should note that all of the audit work I've mentioned today is available on our Web site, [www.socialsecurity.gov/oig](http://www.socialsecurity.gov/oig). The OIG, as an oversight body, will continue to do everything it can to ensure the integrity of the Social Security number. We will also encourage its protection by private and public entities; and provide meaningful sanctions for those who fail to protect it or who misuse it themselves.

Thanks once again to the Federal Bar Association for its efforts to foster a productive exchange on this issue of critical importance. I'm honored to have the opportunity to be here today, and I thank all of you for your interest and attention. ❧



# Patrick P. O'Carroll

**Patrick P. O'Carroll, Jr.** currently serves as the third Inspector General (IG) for the Social Security Administration, having been appointed to that position on November 24, 2004. Under his direction, the SSA Office of the Inspector General inspires public confidence in the integrity and security of SSA's programs by conducting independent and objective audits, evaluations, and investigations. Since assuming the SSA OIG leadership, Mr. O'Carroll has intensified the OIG's efforts to identify and prevent fraud, waste, and abuse in SSA programs through the institution of innovative and collaborative approaches to the office's core functions and the management and development of human and technological resources.

The results of these efforts can be seen in the OIG's most recent achievements. In FY 2008, the OIG's investigators reported over \$370 million in investigative accomplishments through SSA recoveries, restitution, fines, settlements, judgments, and projected savings. OIG auditors issued 108 reports with recommendations identifying over \$1.1 billion in federal funds that could be put to better use and \$2.4 billion in questioned costs. And OIG's attorneys reported over \$6.5 million in civil monetary penalties and assessments.

In addition to directing an OIG workforce of almost 600 auditors, attorneys, investigators, and support personnel nationwide, Mr. O'Carroll also chairs the Investigations Committee of the Council of the Inspectors General on Integrity and Efficiency, which addresses issues that transcend individual Government agencies, and increases the professionalism and effectiveness of IG personnel throughout the federal government. Under Mr. O'Carroll's leadership, the Committee has sought new ways to improve investigative functions, establish investigative guidelines, and promote best practices and training opportunities for thousands of agents in the federal IG community.

Prior to his appointment as Inspector General, Mr. O'Carroll held a number of increasingly responsible positions in the SSA OIG organization, including Assistant Inspector General for Investigations and Assistant Inspector General for External Affairs. Mr. O'Carroll also brought to the OIG the benefits of his 26 years of experience with the United States Secret Service.

Mr. O'Carroll received a B.S. from Mount Saint Mary's College in Emmitsburg, Maryland, and a Master of Forensic Sciences from the George Washington University, Washington, D.C. He also attended the National Cryptologic School and the Kennedy School at Harvard University. Mr. O'Carroll is a member of the International Association of Chiefs of Police and the Association of Government Accountants.

# 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 professional and scholars on topics important to the Inspector General community.

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

By mail:  
Department of Defense  
Office of Inspector General  
400 Army Navy Drive, Room 1034  
Arlington, VA 22202

By email:  
[JournalofPublicInquiry@dodig.mil](mailto:JournalofPublicInquiry@dodig.mil)



*Disclaimer: The opinions expressed in the Journal of Public Inquiry are those of the authors. They do not represent the opinions or policies of any department or agency of the United States Government.*

Journal  
of Public Inquiry



**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;