

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

The Journal of Public Inquiry



FALL/WINTER

2007-2008

PRESIDENT'S COUNCIL ON
INTEGRITY AND EFFICIENCY

EXECUTIVE COUNCIL ON
INTEGRITY AND EFFICIENCY

Editorial Board

Christine C. Boesz, Inspector General, National Science Foundation

Earl E. Devaney, Inspector General, Department of the Interior

Gregory H. Friedman, Inspector General, Department of Energy

J. Russell George, Treasury Inspector General for Tax Administration

John P. Higgins, Jr., Inspector General, Department of Education

Patrick O'Carroll, Inspector General, Social Security Administration

Staff

Editor-in-Chief

Claude M. Kicklighter, Inspector General, Department of Defense

Publisher

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

Publication Manager

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

Editorial Services

Bill McGloin, Editorial Assistant, Office of Communications and Congressional Liaison, Department of Defense Office of the Inspector General

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

Note:

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.

FOREWORD

Welcome to the Fall/Winter 2008 issue of the Journal of Public Inquiry. Once again, we are able to offer a wide selection of informative articles about the Inspector General (IG) community and the issues important to its members. It is our goal that the Journal serve as a source of information that allows the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) to share knowledge regarding issues that transcend individual government agencies, and can serve as lessons to all in the IG community. In so doing, the Journal provides insight and accountability on the IG community's efforts to work together and thus improve how the government serves the American people.

The Journal is a semiannual publication of the PCIE and ECIE, which together includes 64 statutory Inspectors General who oversee stewardship in the federal government. Our work continues to grow in order to keep pace with changes in how the government responds to national and international events. By sharing our lessons learned and best practices with one another, we maximize our opportunities for improvements. The Journal is an exceptional platform to share these ideas and draw attention to the new challenges that lie ahead. Communication within the oversight community is essential to avoid duplication and gaps in effort; leverage each other's work; support each other's efforts to form mutually beneficial partnerships that replace interagency rivalry; and avoid mistakes of the past.

We are pleased to present over a dozen entries ranging from essays, speeches and Georgetown University capstone papers. The entries encompass themes ranging from audit advisory committees, the role of inspectors general in Eastern Europe, public integrity and the importance of identity protection. The highlighted article in this version of the Journal is entitled, "Sunshine is the Best Antiseptic," and outlines the work that the IG Community has done to improve transparency in government and identifies the challenges that lie ahead.

We have also included a speech from the President and CEO of the Council of Excellence in Government, Patricia McGinnis, which she gave during the October 2007 PCIE/ECIE awards ceremony. The theme of the speech, trust in government, reminds us of our goal as Inspectors General.

Finally, a capstone paper from the Georgetown University Masters in Policy Management program focuses on ways to improve counterterrorism efforts by better coordination among the different agencies involved in counterterrorism policy.

A special thanks to all the authors who contributed their expertise and insight to this issue of the Journal of Public Inquiry.

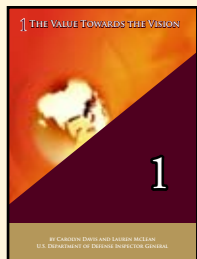


Claude M. Kicklighter
Inspector General

ARTICLES

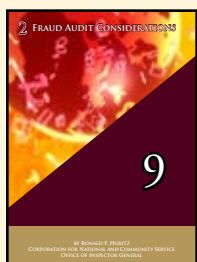
FEATURED ARTICLE

Audit



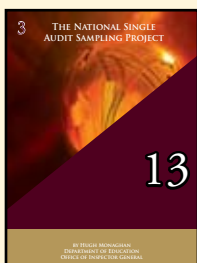
The Value Towards the Vision

Written by Carolyn Davis and Lauren McLean



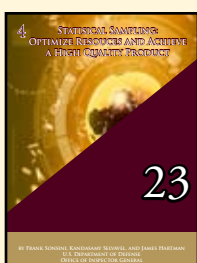
Fraud Audit Considerations

Written by Ronald Huritz



The National Single Audit Sampling Project

Written by Hugh Monaghan



Statistical Sampling

Written by Frank Sonsini, Kandasamy Selvavel, and James Hartman



Is Your Identity Being Thrown Out with the Trash?

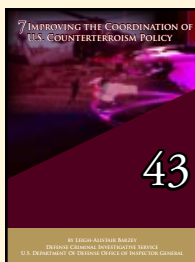
Written by Lou Major

Investigation



Procurement Fraud Investigations

Written by Colonel Joe Ethridge, Curits Greenway, and Wesley Kilgore



Improving the Coordination of U.S. Counterterrorism Policy

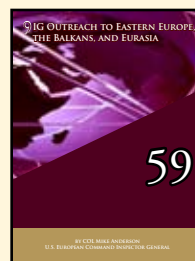
Written by Leigh-Alistair Barzey

Outreach



Developing a Hotline for the 21st Century

Written by Joseph Vallowe and Christina Lavine



IG Outreach to Eastern Europe, the Balkans, and Eurasia

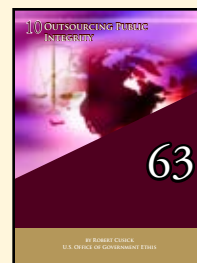
Written by Colonel Mike Anderson



30TH ANNIVERSARY OF THE IG ACT

Gregory Friedman
Inspector General
Department of Energy

Speeches



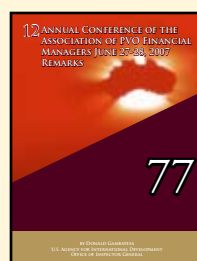
Outsourcing Public Integrity

Remarks by Robert Cusick



PCIE/ECIE Awards Ceremony

Remarks by Patricia McGinnis



Annual Conference of the Association of PVO Financial Managers

Remarks by Donald Gambatesa

* Denotes the end of an article.

30TH ANNIVERSARY OF THE IG ACT

“Sunshine is the best antiseptic.”

These simple words of Justice Louis Brandeis remain as relevant today as ever, particularly as the Federal Inspector General community begins its 30th year of service under the Inspector General Act.

This comes at a time when the Inspector General community finds itself in the middle of a swirl of controversy and scrutiny. Perhaps as at no time in its history, has there been more public interest in the activities of the community, including current consideration of new legislation proposed, according to its sponsors, with the intent of strengthening the Inspector General concept.

The Inspector General Act established independent and objective units -- Inspectors General -- within most federal departments and agencies. While the Act describes the mission of the IGs in formal terms, I view the IG's as having four major responsibilities:

- Providing an independent set of “eyes and ears” on the efficiency and effectiveness of Department operations;
- Serving as objective fact finders in controversial, high profile matters of agency concern; and,
- Bringing to justice those attempting to defraud the U.S. government.

Finally, and perhaps most importantly, the Inspector General community works to ensure that the interests of the U.S. citizens are represented when important governmental decisions are made.


The current issues and concerns that have been raised regarding the community, serious as they are, require some balance and perspective.

Let's look at the record.



The Inspector General Act has placed our community of accountability professionals at the vanguard of so many of the great public challenges of this or any day. These include, as examples issues ranging from, the complexities of managing the aftermath of Hurricane Katrina to defending vigorously the nation in the wake of the mortal threats presented by global terrorism. Further, the IG community commits a huge proportion of its resources on an annual basis to auditing the financial statements of each department and agency. Taken collectively, this effort is one of the largest financial statement audit engagements ever undertaken. This may sound like mundane work, but the results provide the basis for audit opinions on statements reflecting trillions of

dollars in operations throughout the federal sector. Both the Administration and the Congress view this work as a priority as they endeavor to enhance federal government accountability. Our most important work as IGs on behalf of the nation is as it has been consistently for the past 30 years: helping to ensure that the Government works as efficiently and effectively as possible for the people, and, of course, with appropriate accountability and transparency.



Much work has been done, but much work remains. In our 2006 progress report to the President, the Federal Inspectors General reported the following results: \$9.9 billion in identified potential savings; \$6.8 billion in investigative fines and recoveries; and 8,400 criminal prosecutions. This record of accomplishment is consistent with the community's performance over many years of service. Indeed, the 11,000 members of the Federal IG community can be proud of all that it has achieved.

The work of safeguarding public resources, to be sure, is not ours alone. Consequently, it is essential to recognize the many contributions of all our partners, dedicated public servants who perform the critical missions of Government and share our commitment to seeing that the right thing is done, that it is done the right way, and that it is done well.

The mission of the IGs is not just to find fault even when fault is due, but also, we strive to identify risks to the ongoing and future effectiveness of government. The tackling and correcting of long-term, often well entrenched, intractable systemic deficiencies is perhaps a less glamorous, but no less important task before us. And while the fruits of this labor may only be harvested over time, the citizens of the nation should know that we are at work every day, in countless ways, to help improve the efficiency, effectiveness, integrity, and yes – the transparency – of government operations.*



GREGORY H. FRIEDMAN
INSPECTOR GENERAL

U. S. DEPARTMENT OF ENERGY

Gregory H. Friedman was nominated by the President and confirmed by the U.S. Senate as Inspector General of the U.S. Department of Energy in 1998. Mr. Friedman started his Federal career in 1968 at the Department of Defense and has been with the Office of Inspector General since 1982.

Since January 2005, Mr. Friedman has also served as Vice Chair of the President's Council on Integrity and Efficiency (PCIE). The PCIE, established by Executive Order, addresses government-wide integrity, economy, and effectiveness issues. The Vice Chair manages the Council's day-to-day activities.

Mr. Friedman received a Bachelor's degree in Business Administration from Temple University and a Master's degree in Business Administration from Fairleigh Dickinson University. In 1979-1980, Mr. Friedman was selected as a Princeton Fellow in Public Affairs and spent a year in residence at Princeton University's Woodrow Wilson School for Public and International Studies.

1 THE VALUE TOWARDS THE VISION



BY CAROLYN DAVIS AND LAUREN MCLEAN
U.S. DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

INTRODUCTION

The Office of the Assistant Inspector General for Audit Policy and Oversight (APO) within the Department of Defense Office of the Inspector General recently issued a report on “Best Practices for Audit and Financial Advisory Committees Within the Department of Defense.” Whereas we do not “oversee” audit committees, we do recognize the value they bring towards the goal of creating accountability and transparency within the DoD. The Assistant Inspector General for Audit Policy and Oversight suggested that we ascertain best practices for audit committees to assist the Department in audit preparedness for a financial statement audit or in facilitating a financial statement audit. In accomplishing this effort, we were not necessarily interested in recommending that every DoD organization that develops and submits financial statements or that is working towards audit preparedness start an audit committee. However, what we did want to create was useful information that highlighted the benefits of audit committees, facilitated an understanding of their value, and made it easier for DoD organizations to consider establishing audit committees (whether required or not) to understand what they were doing and how to do it.

BACKGROUND

In March 2003, the DoD Comptroller directed the establishment of audit committees for 21 DoD entities and required the DoD Office of Inspector General to provide representation on each committee. The January 2006 DoD Financial Management Regulation required the establishment of 3 additional audit committees. Of the 16 DoD audit committees that we reviewed, 10 focused on audit preparedness and 6 performed oversight of the financial statement audit. The Office of Inspector General acted as advisors to the financial audit advisory committees and committees for audit preparedness and performed oversight of the external auditor that conducted the financial statement audits.

We began a review in December 2006 to ascertain best practices of audit committees since we saw them as a useful tool for strengthening the integrity, efficiency, and effectiveness of Department of Defense programs and operations, and we felt they had a potential towards moving the Department towards its accountability and transparency goals. Also paramount in our minds was the increased emphasis on audit committees inherent in the Sarbanes-Oxley Act. Also, the Government Auditing Standards increased recognition of organizational governance, including the role of audit committees. The Government Auditing Standards states that:

“Those charged with governance have the duty to oversee the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing the financial reporting process, subject matter, or program under audit including related internal controls.... In some entities, multiple parties may be charged with governance, including oversight bodies, members or staff of legislative committees, boards of directors, audit committees, or parties contracting the audit.”

In May 2007, the Department of Defense established an Audit and Financial Management Advisory Committee to provide independent advice and recommendations to DoD on financial management, including the financial reporting process, systems of internal controls, the audit process, and processes for monitoring compliance with applicable laws and regulations.

HITTING THE HIGHLIGHTS

The purpose of this article is to hit the highlights of our review of Audit and Financial Advisory Committees within the Department of Defense and to bring more visibility to a tool that can foster transparency and accountability for

Federal Government organizations and entities. We recognize that there is no one-size fits all solution to achieving quality financial statements and audits. As stated in the “Foreword” to the Best Practices Review Report, “Financial audit advisory committees benefit an organization either by assisting with audit preparedness or by providing increased confidence in the credibility of the organization’s financial statements.... If effectively designed, the committee can be a strategic partner in conducting quality audits, preparing auditable financial statements, and improving business operations.”

WHAT IS AN “AUDIT ADVISORY COMMITTEE” ANYWAY?

Audit advisory committees in DoD generally serve one of two functions: financial statement audit preparedness or financial statement audit oversight. Committees for audit preparedness provide oversight and make recommendations to help the organization improve business operations through improvements to financial reporting processes and procedures. The scope of each committee’s work depends on the status of financial management within the organization. When the entity is prepared to undergo a financial statement audit, the committee’s focus shifts from audit preparedness to oversight of the financial statement audit, and the committee assumes additional oversight and advisory responsibilities. A financial audit advisory committee can provide independent oversight of an organization’s annual financial statement audit, risk management plan, internal control framework, and compliance with external requirements. Acting in an advisory role, the committee promotes independence, enhances accountability, and facilitates communication between management and the external auditor that conducted the financial statement audit. The scope of each committee’s work varied depending on the status of financial management within the organization.

WHAT ARE THE BENEFITS OF AUDIT ADVISORY COMMITTEES?

Financial audit advisory committees benefit an organization either by helping with audit preparedness before financial statements are ready for audit or by providing increased confidence in the credibility of the organization’s financial statements that are ready for audit. Other significant benefits that an independent and objective financial audit advisory committee provides include enhanced communication on financial management problems among senior managers, a vehicle for resolving differences. Most importantly, an audit and financial advisory committee provides accountability and transparency for financial reporting throughout the organization and to the public. The committee ensures that the organization achieves the goals and objectives of the financial audit, provides expertise on accounting and financial reporting issues, and ensures early identification and resolution of audit-related problems. The committee acts as an independent third party to review, discuss, and validate the results of the independent public accountant’s work. Financial audit advisory committees assist with audit preparedness by helping ensure that the organization maintains its focus on audit readiness, suggesting ways to improve the organization’s business and financial reporting processes, and emphasizing the importance of fiscal responsibility throughout the organization.

THE ROLE OF THE AUDIT ADVISORY COMMITTEE

The role of the audit advisory committee needs to be clarified before you get out of the starting gate. The Audit Advisory Committee does not take the place of management. DoD committees for audit preparedness help the organization prepare for audit while simultaneously making recommendations to improve internal controls and business processes. Committees that are acting as advisors during the annual financial statement audit may have responsibilities such as providing oversight and advice, acting as a liaison between management and the external audit conducting the financial statement audit, monitoring management’s internal control program, and educating DoD

personnel on the importance of the audit and the work of the committee. The financial audit advisory committee can make recommendations to ensure that the organization has implemented appropriate internal controls to address organizational risks, and that those internal controls are operating effectively. The audit advisory committee can consider developing a newsletter as a way to educate the organization about the work of the committee.

WORKING TOGETHER AND INCREASING ACCOUNTABILITY?

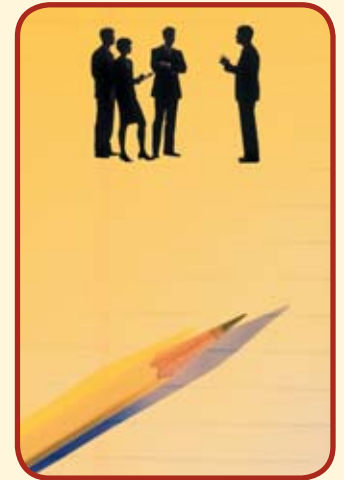
The central function of the committee is to increase the accountability of the organization. To achieve this goal, the committee should work to ensure trust and faith between it and the organization, rather than an “us against them” relationship. The committee should collectively work to develop recommendations to improve the organization’s financial reporting and business processes. To contribute to the mission and goals of the committee, members should understand the essential business of the agency, interpret federal laws, understand federal financial accounting and reporting requirements, and know federal requirements for systems certifications. Most importantly, members should ask the agency’s top managers how they intend to ensure agency compliance with relevant laws and regulations.

Committees should work with management and share suggestions to improve financial management throughout the organization. Management contributes to the success of the committee by providing ongoing communication regarding the status of the audit and should brief members on changes in financial reporting and business operations that might affect the committee’s work. Each member should try to communicate the work of the committee to show what they are accomplishing and emphasize the importance of the financial statement audit.

I WANT TO START ONE, SO WHAT DO I DO NOW?

Tips to Consider When Establishing a Committee

- Define your goal, develop and adhere to your charter and mission
- Maintain open communication with all stakeholders
- Maintain open communication with the agency
- Select a good and effective leader
- Select good members
- Train new members
- Meet as frequently as necessary



Reading the bulleted list of tips above – you might be inclined to say duh! This list would work regardless of the type of committee you are establishing and that thought would be true. A little more information, PLEASE!

The committee charter should consist of the committee’s objectives, authority, composition, member tenure, roles, responsibilities and expectations as well as reporting requirements and administrative agreements. If that doesn’t help enough, the report on our Internet site at <http://www.dodig.mil/Audit/reports/apo08.htm> provides appendices with sample (fill-in-the-blank) charters for a Federal Advisory Committee Act-Compliant Audit Committee charter and a Financial Audit Advisory Committee Charter. An audit committee that complies with the Federal Advisory Committee Act (FACA) includes members outside of the Federal Government. FACA-compliant audit advisory committees must meet certain requirements such as advertising meetings 15 days in advance in the Federal Register, being open to the public unless limited statutory basis for closure applies, being attended by a Designated Federal Officer, and having minutes available for public inspection.

THE RIGHT MIX

A Good and Effective Audit Advisory Committee Leader Should: Lead from the front—decide what the committee is going to achieve, plan a schedule, and push it through vigorously, keeping up the momentum. Initiate individual meetings with the Inspector General, Chief Financial Officer, and any other officials affected by the work of the committee. Establish the schedule for meetings to ensure that the members have enough time to propose recommendations that are effective. Ensure that the committee's decisions and concerns are reported to the agency regularly both orally and in writing. Know or learn enough about the audit and how it is organized to be able to ask the independent public accountant probing questions. Be responsive to requests to consult with the auditors alone outside of the meetings. Ask management for regular updates on the status of audit findings. Ensure that the committee has the flexibility to respond quickly to unexpected findings, outcomes, and issues. That's enough though the list goes on.

Membership Has The Right Stuff. You should make sure that you have continuity of membership and that your members are independent and have sufficient financial expertise (In case you're not certain, components of financial expertise are listed in the report). Other factors to consider when recruiting members to assist with audit preparedness include: expertise and experience leading an organization through a first-year financial statement audit, experience helping an organization obtain and maintain an unqualified audit opinion, understanding of the organization's financial improvement process, and understanding of the organization's culture, mission, and diversity of operations. Collectively, the committee members should have an understanding of the Chief Financial Officer's Act requirements, Federal information systems requirements, Federal accounting and financial reporting requirements, and an understanding of legal, actuarial, and strategic planning.

The Right Stuff for Committee Members Includes: the ability to encourage openness and transparency, the ability to act independently and be proactive in advising the organization of issues that require further management attention, the ability to ask relevant questions, evaluate the answers, and continue to probe for information until completely satisfied with the answers provided, independence of thought, an appreciation of the entity's culture and ethical values and a determination to uphold those values, the ability to work with management to achieve improvement in the organization, and the ability to adequately explain technical matters to other members of the committee where members have been chosen for particular technical skills.

ONCE YOU START ONE, HOW TO HAVE IT OPERATE EFFECTIVELY

To have an effectively operating committee, you need to orient and train its members, ensure the committee has certain essential resources at its disposal, and make sure there is open communication with the external auditor throughout all audit phases. You should ensure that your committee has a clear focus and understanding of the organization's annual plan; summaries of the results of audit testing; future audit steps and audit deliverables; quarterly and annual financial statements; audit and financial statement timelines and milestones; Government-wide and internal financial indicators; information technology weaknesses; changes to regulations and updates on Federal financial reporting guidance; and annual briefings on financial statements and all audit findings by the independent public accountant. Periodically, the committee chairperson should have meetings with the agency head or other senior officials to discuss the work of the committee. Committees are encouraged to conduct Executive Sessions with the Inspector General, Chief Financial Officer, senior management, and the independent public accountant at least annually. However, the committee may request an Executive Session at any time. Annual committee performance evaluations provide an opportunity for the committee and chairperson to identify opportunities for improving the operation of the committee. Committee

members should continuously strive to improve organizational performance and identify new ways to add value to the organization. Financial audit advisory committees should consider conducting comprehensive self-evaluations annually.

BEING A PART OF THE PAR

A suggested best practice for Federal audit advisory committees is to consider including an “Audit and Financial Management Advisory Committee Report” in the agency Performance and Accountability Report (PAR) describing the committee responsibilities, significant accomplishments, and the results of the committee’s review of the PAR. Committee review of the PAR enhances the credibility of the document. The committees should also consider endorsing the agency’s “Management Response to the Independent Auditor’s Report,” which is included in the agency’s PAR.

THE LONG ROAD AHEAD

Thomas F. Gimble, then Acting Inspector General of the DoD IG, stated in his August 2006 testimony before the Subcommittee on Federal Financial Management, Government Information and International Security Senate Committee on Homeland Security and Governmental Affairs on “Financial Management at the Department of Defense:” “The Department’s financial statements are the most extensive, complex, and diverse financial statements in the Government....The Fiscal Year 2005, DoD Agency-Wide Principal Financial Statements reported \$1.3 trillion in assets, \$1.9 trillion in liabilities, and \$635 billion in Net Cost of Operations....DoD’s financial management problems are so significant that they constitute the single largest and most challenging impediment to the U.S. Government’s ability to obtain an opinion on its consolidated financial statements.” The process for auditing financial statements gets more challenging each year. With additional financial statement requirements and tougher auditing standards as well as human capital challenges, financial audit advisory committees are one possible means of assisting organizations in achieving their audit goals. In management’s efforts to obtain an opinion on agency financial statements, audit advisory committees effectively designed and operated can be a useful tool and a solution enabler towards achieving quality, auditable financial statements, and improved business processes.

DoD audit advisory committees focus on DoD audit preparedness efforts and financial statement audit oversight. The best practices of audit committees report on the DoD IG Internet site at <http://www.dodig.mil/Audit/reports/apo08.htm> provides criteria, purposes, operations, and best practices of audit and financial advisory committees operating in both the public and private sectors. If effectively and efficiently designed, financial audit advisory committees can represent another set of eyes and a strategic partner in moving towards quality audits, auditable financial statements, and improved business operations. To achieve true benefit from financial audit advisory committees, messaging and implementation need to be very well planned and executed including such things as getting the right mix of committee members; establishing a clear charter for the committee; and fostering a positive culture amongst the committee, the external auditor, and the organization. Audit advisory committees can help facilitate understanding and assist organizations in working through challenges by performing additional functions such as helping track recommendations; and analyzing problems and control failures so that corrective action plans can be appropriately developed and tailored. Audit advisory committees can be a tool in your organizations tool box with benefits that add value to organizational efforts toward providing transparency and accountability to foster public trust.*

Excerpts for this article were taken from DoD IG Report No. D-2008-6-001, “Best Practices for Audit and Financial Advisory Committees Within the Department of Defense” – Major contributors to the report were Wayne C. Berry, Carolyn R. Davis, Robert Kienitz, Lauren McLean and Allison Tarmann.

AUDIT POLICY & OVERSIGHT DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

BEST PRACTICES FOR AUDIT COMMITTEES

AUDIT COMMITTEES WORK BEST WHEN THE ORGANIZATION AND THE COMMITTEE HAVE...

- Commitment to the Same Goals
- A Partnership Relationship
- Senior Management
- Participation
- Interest
- Support
- Communication throughout all audit phases

WHAT MAKES AN AUDIT COMMITTEE SUCCESSFUL

THE RIGHT MIX. An effective chairperson and members, whether internal or external, with the necessary functional area expertise, skills, and experience including financial expertise.

FOCUSED ATTENTION.

Fosters public trust by providing focused attention on organizational accountability issues with a third party perspective that offers checks and balances between the organization, auditors, and stakeholders.

VALUE-ADDED SERVICES.

Provides services that assist the organization in mission accomplishment through effective follow-up on actions to improve financial reporting and business operations.

BENEFITS OF AUDIT COMMITTEES

- Independent
- Objective
- Enhanced Communication
- Audit Problem Resolution Vehicle
- Confidence and Credibility Builder
- Provider of Public Accountability and Transparency
- Audit Issue Visibility
- Real Time Problem Solving
- Prevents Management Complacency
- Provides Audit Finding Credibility
- Independent Third-Party Evaluation of External Audit Results

AN AUDIT COMMITTEE CAN PROVIDE

- Oversight
- Advice
- Liaison
- Monitoring of management responsiveness
- Organization assistance with improved strategy
- Focus on audit readiness
- Suggestions for improved processes
- Emphasis on fiscal responsibility

AUDIT COMMITTEES SHOULD

- Have a charter
- Annually reassess their charter
- Annually assess their performance
- Include financial expertise
- Have right composition of expertise
- Keep current on changes in financial reporting requirements
- Serve as an intermediary

COMMITTEE CHAIRPERSON SHOULD

- Have a sound financial background
- Be strong, independent, and able to lead
- Be able to foster open communication
- Possess exceptional critical thinking skills
- Be tactful and diplomatic

A GOOD COMMITTEE MEMBER

- Understands the business
- Understands Federal financial reporting requirements
- Uses expertise to problem solve
- Focuses on mission and goals
- Has personal credibility
- Has good leadership skills
- Exercises sound independent judgment in a relevant field or discipline



WHAT CAN WE DO FOR YOU?

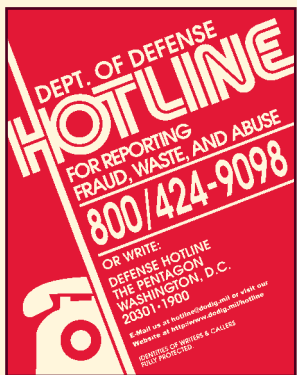
CONTACT US:

INTERNAL AUDIT & CONTRACT AUDIT FOLLOWUP
(703) 604-8877

CONTRACT AUDIT & SINGLE AUDIT
(703) 604-8789

AUDIT POLICY & OVERSIGHT
400 ARMY NAVY DRIVE
ROOM 1016
ARLINGTON, VA 22202

WEBSITE:
WWW.DODIG.MIL
FAX: (703) 604-9808



CAROLYN R. DAVIS
DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

Carolyn R. Davis is Deputy Assistant Inspector General for Audit Policy and Oversight at the Department of Defense Office of the Inspector General. Ms. Davis has 24 years of auditing experience including 16 years of management. Over the past 10 years, she has become one of the foremost experts in assuring the quality of audits and has been an integral participant in a number of efforts that contributed to improving the quality of audits within the DoD OIG and throughout the Federal Audit community. She received her Bachelors of Business Administration degree from Howard University in 1983 and her Master of Science in Administration from Central Michigan University in 2004. She is a Certified Public Accountant licensed in the state of Maryland since August 1992. Ms. Davis received the President's Council on Integrity and Efficiency (PCIE) Award of Excellence for Working Group on Updating PCIE Guide on Conducting External Quality Control Reviews. She also received the Inspector General's Meritorious Civilian Service Award for contributions to improving the quality of audits within the DoD OIG and throughout the Federal audit community; and the Superior Civilian Service Award for the successful development and execution of Defense and government-wide audit policy and oversight efforts.

BIOGRAPHIES



LAUREN S. MCLEAN
DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

Lauren S. McLean is an Auditor Technical Specialist within the Office of the Assistant Inspector General for Audit Policy and Oversight. Ms. McLean received her Bachelors Degree in English from Regis College in Weston, Massachusetts and is currently pursuing a Masters in Public Administration from Georgetown University. Ms. McLean is a Certified Internal Auditor, a Certified Information Security Specialist, and has served as a Contracting Officer's Technical Representative. She is an active member of the DC Chapter of the Institute of Internal Auditors where she has served on the Government Relations Committee for the past two years and is currently the Vice President of Professional Activities. Her honors, awards, and special accomplishments include Chairperson, USAID, Human Resources Council - 2003-2004; USAID Group Achievement Award for the FY 2003 GMRA Audit - 2004; U.S. Customs Service Employee Awards for Outstanding Contributions - 1997, 1995.



2 FRAUD AUDIT CONSIDERATIONS

BY RONALD F. HURITZ
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
OFFICE OF INSPECTOR GENERAL

In his 2002 State of the Union address, President George W. Bush issued a Call to Service to Americans in response to the horrific series of tragedies that occurred in September of the previous year. The primary goal of the Call to Service was to kick start a compelling sense of volunteerism throughout the American population, and engage as many citizens as possible in efforts to reach out and help their neighbors, drawing on the overwhelming spirit of humanitarianism that was generated during the 9/11 crisis. Those events sparked the volunteerism movement in America to a degree unequalled at any other time in American history.

During a more subdued time period in the early 1990s, the Clinton Administration also recognized the need to get many more people involved in civic, social and education projects. Thus was born the Corporation for National and Community Service in 1993, a legislative combination of two older agencies: ACTION, which administered the VISTA and Senior Corps programs, and the Commission on National and Community Service, the parent organization of two programs focused on students and young adults, known as Learn and Serve America and the National Civilian Community Corps. Today, the Corporation is often referred to as the “domestic Peace Corps”, although the two agencies have no connection whatsoever.

The Corporation, one of about two dozen smaller federal agencies that operate under the Government Corporation Control Act, presently boasts a cadre of over two million volunteers who promote a culture of citizenship, service and mentoring across the country. Corporation management has ambitious goals for expanding its reach and promoting volunteerism over the next few years. Its current 5-year plan, ending in 2010, hopes to embrace an additional 10 million people, including college students, members of the Baby Boomer generation, and active seniors who offer a variety of mentoring skills.

The best known of the agency’s core programs, AmeriCorps, is a network of grant-driven programs that provide funds to support diverse volunteer activities at the community level. Most of the funds are channeled through State commissions appointed by each State governor. The commissions then sub-grant the monies to nonprofit

groups and other entities to support the community service efforts of AmeriCorps members throughout the United States and American territories.

Among their most visible activities in the recent past, scores of AmeriCorps volunteers were dispatched to the gulf coast states to perform a variety of relief duties following Hurricanes Katrina, Rita and Wilma. Other funding recipients, called National Direct grantees, receive monies directly from Corporation appropriations rather than through the state commissions. At the end of their term-of-service, usually 1,700 hours, AmeriCorps members qualify to receive an award of \$4,725 that can be used toward education expenses at a college or university, or to pay down a student loan.

Like every other federal program that is fueled by taxpayer dollars, the Corporation is charged with the stewardship responsibility of minding those dollars closely. But despite its modest size of about 600 employees and just-under \$900 million budget, there are no fewer opportunities for the Corporation to be victimized by fraud, waste and abuse than any other government agency.

PUNCHING THE TIME CLOCK

Because education awards that are paid to volunteer members are earned when they complete the required service hours, OIG auditors find all too often that time sheets used for recording those hours are falsified, inaccurate, incomplete, or not properly signed and authorized. As one example, time sheets that show an excessive number of hours served, say 60 or 70 per week, have the effect of shortening the time period that a member needs to stay enrolled in the program before he or she is eligible to receive the education award.

AmeriCorps program rules dictate that the typical period of service should be between 9 and 12 months. Serving 1,700 hours in 6 or 7 months instead violates those rules. The auditors have no choice but to question the entire education award, and recommend to program officials that the improperly earned award be recovered from the entity that paid the award for the abbreviated period of service.

Education awards also have a living allowance component. Depending on the location of their assignment, some members may be paid as much as \$10,000 or more to defray their living costs while actively serving in AmeriCorps programs. Again, timekeeping records are the critical element. If a member is absent from their assignment for school, family or other personal obligations---in other words, not actively serving---their living allowance may be overpaid if time sheets do not accurately show their on-duty or off-duty status. Falsely claiming living allowances for extended off-duty time periods results in auditors questioning the costs.

“Grant programs, both large and small, are sometimes easy pickings for fraudsters.”

Time sheet fraud is tantamount to a false claim submitted to the government for reimbursement. The more egregious cases, which often originate as audit findings and are then referred to the OIG’s Investigations Section, may develop into criminal cases that are brought to trial by United States Attorneys’ offices.

CRIMINAL BACKGROUND CHECKS – A NECESSARY EVIL

AmeriCorps members, as well as volunteers enrolled in other Corporation programs, frequently come into contact with what the regulations refer to as “vulnerable populations.” School-age children and elderly citizens are two obvious examples. Society being what it is these days, most if not all human services programs are under a duty to take precautions in protecting these groups.

To that end, framers of the Corporation’s operating procedures recognized the need to obtain criminal background checks on volunteers exposed to those populations. Nearly all volunteers are affected, but seniors who serve as Foster Grandparents in schools and day care centers are especially scrutinized.

Why are criminal background checks a necessary evil? They cost money – money that the average grantee

would rather use to achieve its program goals rather than enriching private investigation firms or law enforcement authorities. Ranging from an average of \$6 for simple fingerprinting up to \$45 for computer database searches, grantees with a hundred or more volunteers per year can make a sizable dent in their budgets ensuring that convicted felons and other undesirables don’t prey on children and unsuspecting elders.

OIG auditors ask themselves two questions in performing their reviews. Did the grantee obtain a criminal background check on each volunteer, and was it obtained in a timely manner, preferably before the volunteer began serving in the program? If the answer to either question is “no,” the auditors write a compliance finding indicating a violation of Corporation policy.

While the absence of a background check itself may not be viewed as fraud in the traditional sense, it can actually have a much more damaging impact. A newspaper or television account of a felony committed by an AmeriCorps or Senior Corps volunteer while actively serving in a government-funded program would have a devastating effect on the public’s confidence, and might jeopardize future program funding if it were discovered that a Corporation grantee had failed to perform the background check.

FRAUD COMES IN ALL SHAPES AND SIZES

To the uninformed, the Corporation and its programs might be viewed as a lesser government entity that operates in relative obscurity compared to the better known cabinet-level agencies. But the fact is that the OIG has audited, investigated and prosecuted enough errant grantees to gain respectability in the IG community. While not disclosing the confidential facts of any ongoing case, I can report that my office is on the verge of presenting to the United States Attorney in Washington, DC, a prosecution referral that could return to the government coffers at least \$500,000 in misspent grant funds.

Grant programs, both large and small, are sometimes easy pickings for fraudsters. Recently a small grantee operating an AmeriCorps program in a southern state for only a

dozen youngsters, used most of his \$135,000 grant to have his house painted by the youngsters, an unallowable activity not permitted by either the grant agreement or Office of Management and Budget expenditure rules. This would have seemed to be a slam dunk for indicting and prosecuting the bad guy, except for the fact that the grantee was a minister. Cleverly, the grant was channeled through the minister's church, which served as a protective cover and thwarted all attempts to seek recovery of the funds. Sometimes the little fish get away. However, the irreverent minister is now on the Federal debarment list for a period of two years.

AN OUNCE OF PREVENTION

From time to time, the OIG conducts fraud awareness briefings across the country for groups who are current or potential Corporation grantees. The objective of these briefings is to introduce audit and investigation concepts to people who may be unfamiliar with the accountability and reporting responsibilities that attach to Federal grant awards. Amazingly, there are too many people who still think that government money is free for the taking. These outreach sessions are one of the best ways to educate grantees about the realities of fighting fraud, waste and abuse of taxpayer dollars.

SUMMARY

America's volunteerism movement, guided in large part by the Corporation for National and Community Service, presents a number of opportunities for OIG auditors and investigators to protect the agency's operating funds. Grantees may commit fraud in a number of ways that can adversely impact dozens of human services programs overseen by the agency. As the ranks of volunteers grow over the coming years, the OIG will need to commit more resources to ensure that Corporation programs operate efficiently and effectively, and that the goals of President Bush's Call to Service are achieved.*

BIOGRAPHY

RONALD F. HURITZ
CORPORATION FOR NATIONAL AND
COMMUNITY SERVICE



Ronald F. Huritz joined the Corporation for National & Community Service's Office of Inspector General in January 2005. As an Audit Manager, his primary responsibilities include conducting program audits and overseeing the work of contract auditors, particularly annual work performed on the agency's financial statements. He also serves as the OIG's representative to the Washington, DC-based Financial Statement Audit Network. From 1998 to 2003, Ron served as Assistant Regional Inspector General for Audit with the U.S. Department of Housing and Urban Development, Office of Inspector General in Chicago, where he planned and supervised audits of public housing authorities and community block grant recipients in a six-state region.

From 1970 to 1990, Ron was an internal auditor in the commercial banking industry in Illinois and Florida. He is a Certified Fraud Examiner, Certified Government Financial Manager, Certified Financial Services Auditor, Certified Business Manager and Certified Fraud Specialist. Ron holds Bachelor of Science in Commerce and Master of Business Administration degrees from DePaul University, and is a graduate of the School of Banking at the University of Wisconsin-Madison. He has authored articles that have appeared in publications of the Association of Certified Fraud Examiners, Institute of Internal Auditors, and Association of Government Accountants.

3

THE NATIONAL SINGLE AUDIT SAMPLING PROJECT



BY HUGH MONAGHAN
DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Each year, American taxpayers spend billions of dollars for a variety of federal domestic assistance programs. These programs provide a wide range of services, including grants and loans for college students, road construction, public housing and mortgage insurance, temporary assistance for needy families, public health services, food stamps and scores of other services. Indeed, the federal government's Catalog of Federal Domestic Assistance (CFDA) lists more than 1,700 federal assistance programs.¹

The programs are funded mostly by grants, but also by other forms of assistance, including loans and loan guarantees, and donations of commodities and property. Some of this assistance is provided directly to, and administered by states and local government entities and nonprofit organizations. In other cases, it is provided indirectly via pass-through entities. For instance, a large federal grant is made to a state agency (the pass-through entity), which then makes sub-grants to local entities or nonprofit organizations that provide the services. Many kinds of entities receive such awards, including departments and agencies of state governments, counties, cities, townships, public housing agencies, school districts, water, sewer, airport and transit authorities, as well as many nonprofit organizations. When they receive awards, grantees and sub-grantees are required by law, regulations and agreements to:

- account for all assets received;
- ensure that expenditures are reasonable and necessary for the purposes awarded; and
- comply with applicable compliance requirements.

SINGLE AUDITS PROVIDE FOR AUDIT ACCOUNTABILITY FOR FEDERAL ASSISTANCE AWARDS

Billions of taxpayer dollars are awarded under these programs to more than 30,000 state and local government entities and not-for-profit organizations nationwide. Audit accountability is critical to help ensure these awards are properly used for the intended purposes.

To meet this need, the Single Audit Act (the Act) was enacted in 1984, and amended in 1996.² Under the Act, state and local government entities and nonprofit entities expending \$500,000 or more of federal assistance awards in a year are required to have an annual single audit. The audit must cover the entity's financial statements, federal awards and internal controls, and be conducted in accordance with Government Auditing Standards [generally accepted government auditing standards (GAGAS)] promulgated by the comptroller general of the United States.

The Act gives the director of the U.S. Office of Management and Budget (OMB) authority to prescribe implementing guidance. Under that authority, OMB has issued Circular A-133, Audits of State, Local Governments, and Non-Profit Organizations.

In June 2002, former OMB Controller Mark Everson testified at a U.S. House of Representatives hearing about the importance of single audits and their quality.³ In his testimony, he referred to audit work performed by several federal agencies that disclosed deficiencies. However, he said that a statistically based measure of audit quality was needed.

This interest in measuring single audit quality using statistical methods was shared by federal agencies. Representatives of these agencies met with OMB in August 2002 to discuss the feasibility of drawing a national statistical sample of

¹ The Catalog of Federal Domestic Assistance provides a listing of all federal assistance programs. It is compiled and published by the U.S. General Services Administration and may be accessed at www.cfda.gov.

² The Single Audit Act of 1984, Public Law 98-502, was amended by The Single Audit Act Amendments of 1996 (Public Law 104-156).

³ Testimony given at a hearing of the House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, June 26, 2002.

single audits for Quality Control Reviews (QCRs). This resulted in further discussions, followed by comprehensive planning, then the launch of the National Single Audit Sampling Project (the Project). The balance of this article describes the Project, based on the content of the Project report.

THE NATIONAL SINGLE AUDIT SAMPLING PROJECT

The Project was conducted under the auspices of the President’s Council on Integrity and Efficiency (PCIE), as a collaborative effort involving PCIE member organizations, a member of the Executive Council on Integrity and Efficiency (ECIE)⁴ and three state auditors. A Project management staff, consisting of senior federal staff experts on single audits and statistical sampling, designed and managed the Project. A Project Advisory Board, consisting of six federal senior audit executives, three state auditors and an OMB official provided executive oversight, guidance and direction, approving the project design and sampling plan.

The objectives of the Project were to:

- Determine the quality of single audits, by providing a statistically reliable estimate of the extent that single audits conform to applicable requirements, standards and procedures; and
- Make recommendations to address noted audit quality issues, including recommendations for any changes to applicable requirements, standards and procedures indicated by the results of the Project.

The Project involved conducting and reporting on the results of QCRs of a statistical sample of 208 audits randomly selected from the universe of more than 38,000 audits submitted and accepted by the federal government between April 1, 2003 and March 31, 2004.⁵ The sample was split into two strata. Stratum I consisted of audits of entities that expended \$50 million or more of federal awards. Stratum II included audits of entities that expended at least \$500,000 of federal awards, but less than \$50 million.⁶ *Figure 1*, included in the Project report, summarizes the universe and sample drawn.

Figure 1: Summary of Audit Universe and Sample Reviewed in National Single Audit Sampling Project

Stratum	Total Federal Award Expenditures per Audit	Number of All Audits in Universe*	Total Federal Awards Expended for All Audits in Universe*	Number of Audits in Sample
I	\$50,000,000 and higher (Large Audits)	852	\$737,171,328,433	96
II	\$500,000-\$49,999,999 (Other Audits)	37,671	\$143,077,774,976	112
TOTAL		38,523	\$880,249,103,409	208

* Some Federal award expenditures reported for single audits include Federal awards received by sub recipients from pass-through entities which are also covered by single audits of the pass-through entities. The \$737,171,328,433 of expenditures for the universe of Stratum I included \$42,888,498, 211 received through a pass-through entity. The \$143,077,774,976 of expenditures for the universe of Stratum II included \$63,319,321,829 received through a pass-through entity.

⁴ The PCIE is primarily composed of the presidentially appointed inspectors general (IGs) and the ECIE is primarily composed of IGs appointed by agency heads.

⁵ Single Audits are submitted to the Federal Audit Clearinghouse (FAC), a unit of the Bureau of the Census, operated for OMB and funded by major grant making agencies.

⁶ Single audit covering \$300,000-\$499,999 of expenditures were excluded because beginning in 2004 single audits are no longer required for entities expending this range of federal expenditures.

THE PROJECT QCRS

The scope of the QCRs was limited to the audit work and reporting related to federal awards. Audit work and reporting related to the general-purpose financial statements was not reviewed. If the single audit report covered one, two or three major programs, documented audit work related to each major program was reviewed. If more than three major programs were reported to have been covered, three were randomly selected for review. Among the aspects of the audits assessed in each of the Project QCRs were:

- *Reporting*—Were required contents of the auditors' reports included?⁷ Did major program audit findings contain required details? Did the audit documentation include evidence to support opinions on major program compliance, the representations about internal controls and that identified major programs were actually audited as such?
- *Audit Planning*—Were important planning aspects unique to single audits documented as properly covered? These include determination of major programs; attainment of minimum required percentage of coverage of federal awards expended as major programs; and documentation to support determinations that an auditee was considered low risk.
- *Conduct of the Audit Field Work*—Was the audit program adequate for the audit work relating to internal control review and testing, compliance testing and auditing of the Schedule of Expenditures of Federal Awards (SEFA)? For applicable compliance requirements, did the audit documentation demonstrate that required internal control review and testing and compliance testing was performed? Was audit work documented that supported the auditor's opinion on the SEFA?

QCRs were conducted by federal agency staff and by certified public accounting firms contracted to perform QCR field work. A few QCRs were also conducted by state auditor staff. All Project QCRs were conducted using the same methodology. QCR work was reviewed by Project management staff.

Proposed results of each individual project QCR were communicated to each auditor who performed the selected audit. They were requested to comment on each deficiency, and provide information to refute deficiencies with which they didn't agree. These comments and information were fully considered in reaching conclusions about deficiencies and assessing the quality of each QCR.

PROJECT RESULTS

The results of the Project were reported on June 21, 2007, and posted on the PCIE website.⁸ Results are presented in two parts: an Assessment of Audit Quality, and Types of Deficiencies Noted. (A third part of the report presents Overall Conclusions and Recommendations. An Other Matters section includes observations about audit testing and sampling.)

Each Project QCR involved close review of the audit documentation to determine if required work was documented as performed. The Project results are based on the audit documentation. Government Auditing Standards (GAS) applicable for all audits reviewed in the Project, includes the following requirement:

⁷ The reports we made this assessment for were the Report on Financial Statements and Schedule of Federal Awards; Report on Compliance and on Internal Control Over Financial Reporting Based on Audit of Financial Statements, and Report on Compliance With Requirements Applicable to Each Major Program and Internal Control Over Compliance.

⁸ The website is located at www.ignet.gov.

“Working papers should contain...documentation of the work performed to support significant conclusions and judgments, including descriptions of transactions and records examined that would enable an experienced auditor to examine the same transactions and records...” [GAS (1994 revision), ¶ 4.37]

Project QCRs were conducted based on this GAS requirement. Therefore, if the audit working papers did not contain documentary evidence that the work was performed, the project concluded that records did not support that it was performed.

ASSESSMENT OF AUDIT QUALITY

Based on review of the audit documentation selected for each audit, deficiencies were identified. Deficiencies were then considered on an audit-by-audit basis, with the quality of each audit then assessed based on the severity of the deficiencies noted (or an absence of deficiencies). For assessing audit quality, we defined three groups comprising five categories of audit quality.

The acceptable group of audits included audits that fell into two categories, *acceptable* and *acceptable with deficiencies*:

Acceptable (AC)—No deficiencies were noted or one or two insignificant deficiencies were noted.

Accepted with Deficiencies (AD)—One or more deficiencies with applicable auditing criteria were noted that do not require corrective action for the engagement, but should be corrected on future engagements.

Examples of the kinds of deficiencies typical for QCRs classified as AD included:

- Not including all required information in audit findings;
- Not documenting the auditor’s understanding of the five components of internal controls, however, testing of internal controls was documented for most applicable compliance requirements; and
- Not documenting performance of internal control testing or compliance testing for a few applicable compliance requirements.

A group of audits of *limited reliability* was comprised of audits having significant deficiencies:

Significant Deficiencies (SD)—Significant deficiencies with applicable auditing criteria were noted and require corrective action to afford unquestioned reliance upon the audit.

Examples of the kinds of deficiencies typical for QCRs classified SD included:

- Audit documentation did not contain adequate evidence of the auditor’s understanding of the five elements of internal control and testing of internal controls for many or all applicable compliance requirements; however, documentation did contain evidence that most required compliance testing was performed.
- Audit documentation did not contain evidence of internal control testing and/or compliance testing for more than a few compliance requirements, or did not explain why they were not applicable for the auditee.
- Audit documentation did not contain evidence that audit work relating to the SEFA was adequately performed.
- Audit documentation did not contain evidence that audit programs were used for auditing internal controls, compliance and/or the SEFA.

“Each year, American taxpayers spend billions of dollars for a variety of federal domestic assistance programs.”

Audits in the unacceptable group include two categories: *Substandard Audits* and audits with *Material Reporting Errors*.

Substandard Audits (SU)—Audits categorized as substandard were those found with deficiencies so serious that the auditor’s opinion on at least one major program cannot be relied upon.

Examples of the kinds of deficiencies typical for QCRs classified SU include:

- Audit documentation did not contain evidence of internal control testing and compliance testing for all or most compliance requirements for one or more major programs.
- Unreported audit findings.
- At least one major program incorrectly identified as a major program in the Summary of Auditor’s Results Section of the Schedule of Findings and Questioned Costs (plus other significant deficiencies).

Audits with Material Reporting Errors (MRE)—Audits were categorized in the MRE category when other serious deficiencies were not noted, but a material reporting error was noted and the report must be reissued for the report to be relied upon because:

- At least one major program was incorrectly identified as a major program in the Summary of Auditor’s Results Section of the Schedule of Findings and Questioned Costs; or
- The required opinion on the Schedule of Expenditures of Federal Awards was omitted.

Figure 2 from the Project report summarizes the Project’s analysis and estimates of audit quality. Also from the Project report, by number of audits, Figure 3 summarizes the results of all 208 QCRs in the sample within groupings by category.

Figure 2: Audit Quality by Groupings with Statistical Estimates of Audit Quality Based on Numbers of Audits

Stratum	ACCEPTABLE		LIMITED RELIABILITY		UNACCEPTABLE		In Sample	In Universe
	In Sample	Point Estimate*	In Sample	Point Estimate*	In Sample	Point Estimate*		
I – Large	61	63.5%	12	12.5%	23	24.0%	96	852
II– All Other	54	48.2%	18	16.1%	40	35.7%	112	37,671
Total**	115	48.6%	30	16.0%	63	35.5%	208	38,523

* At the 90% confidence level, the margins of error range between ±5.3 and 7.8 percentage points.

** The Point Estimates for the Total were computed with formulas for a stratified random sample, which give more weight to Stratum II because it represents a much larger proportion of the universe. Due to rounding, these percentages do not add to exactly 100%.

Figures 2 and 3 provide estimates of percentages of the number of audits in the stratified universe in the groupings and categories from which the sample was drawn.

Figure 3: Audit Quality Within Groupings by Category with Statistical Estimates of Audit Quality Based on Numbers of Audits

Category	ACCEPTABLE				LIMITED RELIABILITY		UNACCEPTABLE				In Sample	In Universe
	Acceptable		Accepted with Deficiencies		Significant Deficiencies		Material Reporting Errors		Substandard			
	In Sample	Point Estimate*	In Sample	Point Estimate*	In Sample	Point Estimate	In Sample	Point Estimate	In Sample	Point Estimate		
I-Large	16	16.7%	45	46.9%	12	12.5%	9	9.4%	14	14.6%	96	852
II-All Other	23	20.5%	31	27.7%	18	16.1%	0	0.0%	40	35.7%	112	37,671
Total**	39	20.5%	76	28.1%	30	16.0%	9	0.2%	54	35.2%	208	38,523

* At the 90% confidence level, the margins of error range between ±2.1 and 7.9 percentage points.

** The Point Estimates for the Total were computed with formulas for a stratified random sample, which give more weight to Stratum II because it represents a much larger proportion of the universe.

For audits in the sample itself, the Project report also provides an analysis of the results in relation to the dollar amounts of federal awards reported in the 208 audits selected for review by groupings. Figure 4 from the Project report summarizes this analysis.

Figure 4: Distribution of Dollars of Federal Awards in the Audits Reviewed in the Project by Audit Quality Groupings

Stratum	ACCEPTABLE	LIMITED RELIABILITY	UNACCEPTABLE	Total
I- Large	\$52,911,305,271 (93.2%)	\$1,270,684,096 (2.2%)	\$2,621,245,403 (4.6%)	\$56,803,234,770 (100%)
II- All Other	\$232,047,485 (56.3%)	\$39,690,326 (9.6%)	\$140,497,532 (34.1%)	\$412,235,343 (100%)
Both Strata	\$53,143,352,756 (92.9%)	\$1,310,374,422 (2.3%)	\$2,761,742,935 (4.8%)	\$57,215,470,113 (100%)

For the 208 audits we reviewed, this analysis shows that audits covering large dollar amounts of awards (Stratum I) were significantly more likely to be acceptable than other audits (Stratum II).

In reporting the results of the Project, we aimed to be objective and straightforward. Thus, we limited adjectives to those describing the groupings and categories.

TYPES OF DEFICIENCIES

We also designed the Project to identify the types of deficiencies in single audits, and determine their frequency. This information was especially useful in determining some of our recommendations to improve the quality of single audits. The Project report identifies many kinds of deficiencies noted, with rates and estimates of occurrence.

The most significant and/or prevalent deficiencies noted with rates/estimates of occurrence by strata were:

- At least some compliance required testing not documented as performed or not documented as applicable for the audit (47.9 percent in Stratum I; 59.8 percent in Stratum II).
- Testing of internal controls over compliance not documented (34.4 percent in Stratum I; 61.6 percent in Stratum II).
- Obtaining understanding of internal controls over compliance not documented (27.1 percent in Stratum I; 57.1 percent in Stratum II).
- Deficient risk assessments as part of major program determination (13.5 percent in Stratum I; 25 percent in Stratum II).
- Written audit program missing or inadequate for part of single audit (16.7 percent in Stratum I; 38.4 percent in Stratum II).
- Misreporting of coverage of major programs (9.4 percent in Stratum I; 6.3 percent in Stratum II).

We also noted the following significant deficiencies relating to audit findings for which we could not estimate a rate of occurrence, because audit findings do not necessarily exist for all audits:

- Unreported audit findings (22 of 208 audits).
- Information required to be included in audit findings was not included (49 of 208 audits).

These are only some of the most significant and prevalent deficiencies found; many other kinds of deficiencies are noted in the Project report.

CONCLUSIONS AND RECOMMENDATIONS

We concluded lack of due professional care was a factor for most deficiencies, to some degree. The Project report states the following overall conclusions:

“The results of this Project indicate a number of single audits that are acceptable—a majority for the stratum of large audits and almost half of those in the stratum of other audits reviewed. Thus, these results indicate that acceptable single audits can be, and are being, performed. Also, our analysis of results in relation to the dollar amounts of federal awards reported in the audits we reviewed indicates that single audits covering large dollar amounts of federal awards were more likely to be of acceptable quality than other single audits.

However, the results also indicate significant numbers of audits of limited reliability with significant deficiencies and unacceptable audits with material reporting errors and that were substandard. These results pose a challenge: What can and should be done to reduce audit deficiencies and eliminate audits that are of limited reliability or unacceptable?” This last question is by far the most important one posed by the results of the Project. Much thought was given to answering it, and in response, the Project report recommends a three-pronged approach:

1. Revise and improve single audit criteria, standards and guidance to address deficiencies identified by the project;
2. Establish minimum requirements for completing comprehensive training on performing single audits as a prerequisite for conducting single audits and require single audit update training for continued performance of single audits; and
3. Review and enhance processes to address unacceptable audits and not meeting established training and continuing professional education requirements.

The recommendations for the first prong are contained in the part of the report that describe audit deficiencies, and involve specific recommendations to revise:

- OMB Circular A-133;

- Statement on Auditing Standards No. 74, Compliance Auditing Considerations in Audits of Governmental Entities and Recipients of Governmental Financial Assistance; and
- the American Institute of Certified Public Accountants (AICPA) Audit Guide used for single audits, Government Auditing Standards and Circular A-133 Audits.

The recommended revisions are to add to or revise parts of these issuances to improve guidance so as to reduce the occurrence of certain specific deficiencies. The key recommendations of the second prong are to establish:

- a requirement for comprehensive training of a minimum specified duration (such as 16 to 24 hours) for staff performing and supervising single audits, as a prerequisite to doing so; and
- a requirement for continuing professional education (CPE) related to single audits every two years afterward.

Additional recommendations of the second prong include:

- Developing minimum content requirements for both the prerequisite training and CPE;
- Amending OMB Circular A-133 criteria related to auditor selection to provide that single audits may only be procured from auditors who meet the training requirements; and
- OMB encouraging professional organizations and qualified training providers to offer and deliver the training in ways that it is accessible to auditors throughout the United States.

The recommendations for the third prong are to review existing ways, and consider new ways, to address unacceptable audits and improve audit quality.

NEXT STEPS

The report was issued to OMB on June 21, 2007, with the recommendation that OMB implement the report's recommendations in consultation with other key stakeholders in the single audit process. These key stakeholders include federal agencies, the AICPA, state auditors, through the National State Auditors Association and state boards of accountancy, through the National Association of State Boards of Accountancy (NASBA).

Given the implications of the Project results, and the scope and impact of its recommendations, thorough study and consideration are needed prior to implementation—and this will take time. As of the writing of this article, this process has begun, and is expected to continue into 2008.

Initial reaction to the report has been positive. The accountability of the single audit process is too important to ignore the need for improvements in the quality of many single audits. Therefore, this writer is optimistic that the Project will result in significant actions to improve the quality of single audits.*

Copyright 2007. Association of Government Accountants. Reprinted with permission. All rights reserved.

POSTSCRIPT

Since it was issued, the National Single Audit Sampling Project has proved to be a catalyst for heightened interest in single audits, and work to implement many of the Project's recommendations. On October 25, 2007, the U.S. Senate Committee on Homeland Security and Governmental Affairs-Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security held a hearing: "Single Audits: Are They Helping to Safeguard Federal Funds?" Chairman, Senator Tom Carper (D-Delaware) chaired the hearing with active and lively participation by Ranking Minority member Sen. Tom Coburn (R-Oklahoma) and former Missouri State Auditor, Senator Claire McCaskill (D-Missouri).

At the hearing, testimony was given by four key stakeholders in the single audit process. Testifying for the President's Council on Integrity and Efficiency (PCIE), which issued the Project report, Project Director Hugh M. Monaghan summarized the Project results. Then, in her testimony, Government Accountability Office (GAO) Director Jeanette Franzel reviewed the history of the single audit, and GAO's past work evaluating the quality of governmental audits, including single audits. In the testimony, GAO expressed support for the project recommendations, offering comments on some implementation issues. Next, Office of Management and Budget (OMB) Acting Controller Danny I. Werfel testified for OMB. He expressed support for the most of the Project Recommendations, and testified that, among other actions, OMB has taken initial steps to draft amendments to Circular A-133 in response to issues raised in the report, and to evaluate measures to improve the quality and effectiveness of Single Audits. Finally, Mary Foelster, Director, Governmental Accounting and Auditing of the American Institute of Certified Public Accountants (AICPA) testified for the AICPA. She described AICPA efforts over 20+ years to assist members perform quality single audits, including the establishment in 2004 of the AICPA Governmental Audit Quality Center, which she heads. With respect to the Project report and its recommendations, Ms. Foelster stated that the AICPA has established seven task forces to work on implementing project recommendations.

The testimony was followed by a round of questioning in which all three Senators demonstrated keen interest in the single audits and their quality, and expressed the importance that the recommendations are acted upon. They stated that after about 18 months, a follow-up hearing may be scheduled about single audit quality. In addition to those presenting oral testimony, David Costello, President and Chief Executive Officer of the National Association of State Boards of Accountancy (NASBA) submitted written testimony expressing NASBA's interest to work with governmental agencies to establish a process for referrals to State Boards. He encourages government agencies to work with State Boards and NASBA to ensure there is a process in place for communication of substandard practice so State Boards can take appropriate action.

OMB has also met with the PCIE Audit Committee and National Single Audit Coordinators of Federal Departments and agencies, and is establishing workgroups to assist OMB to implement the Project recommendations. OMB has also met with the AICPA to coordinate with them. In January 2008, representatives of NASBA held meeting with OMB and the PCIE Audit Committee to discuss State Boards working with the Federal government on single audit quality issues. Obviously, initial interest in single audit quality generated by the Project report has been substantial, and efforts to address the Project recommendations are ramping up. These efforts will continue through 2008. - *Hugh M. Monaghan*

BIOGRAPHY

HUGH M. MONAGHAN
U.S. DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL



Mr. Monaghan is Director, Non-Federal Audits for the Office of Inspector General, U.S. Department of Education. He manages all aspects of ED/OIG's activities relating to audits required to be performed by Independent Auditors engaged by entities funded by ED. This includes audit quality review, provision of technical assistance and guidance, and updating of audit guidance. Mr. Monaghan was Director of the National Single Audit Sampling Project. The Project was awarded the 1st Barry R. Snyder PCIE/ECIE Joint Award in 2007. Mr. Monaghan has over 36 years of Federal service, including 32 years in the IG Community, with HUD OIG (1976-1980) and Education OIG (since 1980). He is a graduate of the City University of New York, and is a Certified Government Financial Manager.



4 STATISTICAL SAMPLING: OPTIMIZE RESOURCES AND ACHIEVE A HIGH QUALITY PRODUCT

BY FRANK SONSINI, KANDASAMY SELVAVEL, AND JAMES HARTMAN
U.S. DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

OVERVIEW

In this paper, we avoid technical terms, notations, and formulas so that persons with little or no statistical background will be able to understand the contents and application of sampling in the auditing environment. We structured this paper into sections that discuss approaches for collecting data, benefits of sampling, measures and audit applications of statistical sampling, and types of sample designs.

Statistical sampling is an important tool in the field of auditing as well as agriculture, engineering, medicine, social sciences, and many other disciplines. Sampling methodologies are often crucial to enhance understanding and to provide support to decision makers in these fields. When the targeted universe is too large to study in its entirety, statistical sampling allows defensible inferences to be made about the targeted universe more efficiently. There are numerous sampling designs available in the statistical literature that a statistician can choose from, or a statistician can design a sampling plan tailored to address particular needs of the project.

Statistical sampling methodologies can be integral to improving audit quality, which is emphasized by the President's Council on Integrity and Efficiency and inherent in the President's Management Agenda. The emphasis to audit high-risk areas, with fewer resources and shorter audit cycles, further supports the need to employ statistical sampling. Consequently, auditing in this demanding environment requires improved audit planning and better audit tools to efficiently leverage resources and optimize the audit process.

THREE APPROACHES FOR COLLECTING QUANTITATIVE AUDIT DATA

The way in which audit data are collected is a major determinant as to the amount and kind of information the data contain, and subsequently how that data can be used appropriately. Regardless of which type of audit measure is under consideration, operationally there are just three kinds of approaches for collecting audit data

about these measures: (1) census, (2) judgment sampling, and (3) statistical sampling.

A census approach requires auditing every item in the universe and produces a single exact or certain value for the audit measure of interest. But obviously, a census requires the maximum amount of audit resources among the three approaches. This approach generally is too time consuming and prohibitively costly for most audits. However, when a census can be afforded, its results exactly describe the audit universe examined.

A judgment sampling approach requires auditing only a subset of the universe items, and like the census, produces a single value for the measure of interest. Judgment samples may be purposeful, for example, "the largest dollar transactions," "some from each region," "the most suspect items," or haphazard, such as "pick some," without a specific criterion in mind. They are generally smaller in size and therefore less costly and quicker to complete than a census or statistical sample designed for the same audit purpose. The main limitation of a judgment sample is that the results describe only the items actually examined. Results cannot be generalized to the audit universe because of the inability to assess the risk of doing so. That is, the results are useful in demonstrating the existence of the condition of interest in the audit universe but cannot address its magnitude with respect to the entire universe.

Statistical sampling is less costly than a census but more informative than judgment sampling. The main benefit of statistical sampling is that the information it yields approximates the census universe, while the costs associated with statistical sampling are more in line with those of judgment sampling.

BENEFITS OF STATISTICAL SAMPLING

Statistical sampling results describe the entire audit universe, but they do so with an estimated value coupled with a risk assessment of the uncertainty, rather than a single value. Statistical sampling differs from judgment sampling in that it must involve a formal randomization process. Randomization requires the use of a random

number table or more commonly today a pseudo random number computer program.¹

Statistical estimates can be projected onto the entire audit universe, but the tradeoff when compared to a census and judgment sample is that statistical estimates must be stated as a numerical interval that is associated with a confidence level instead of a single value. Statistical sampling facilitates larger findings than judgment sampling, but with less cost and shorter audit cycle time than a census. Statistical results usually are unbiased, that is, equally likely to overstate or understate the true universe value. When correctly designed, executed, analyzed, and presented, the statistical sampling results are defensible against technical challenges.

“Statistical sampling is an important tool in the field of auditing, as well as agriculture, engineering, medicine, social sciences, and many other disciplines.”

The audit risk component of relying on a sample estimate can be quantified when statistical sampling is used. The audit risk component is the complement of the confidence level. For example, a confidence level of 95 percent contributes 5 percent to the audit risk. A better understanding of the quantified audit risk can be enhanced through a better understanding of a confidence level. For example, a 95 percent confidence level means that if the population was repeatedly sampled with samples of the same size and structure, the true population value of the condition being audited would be contained within the confidence interval in 95 percent of those samples. We conversely know that 5 percent of those many samples do not contain the true population value of the item being measured; hence, the audit risk component is 5 percent.

Quantification of the audit risk through the statistical sampling methodology helps the auditor address Government Auditing Standards' requirements for sufficiency of evidence. With the assistance of a

¹ A computer program that produces a good approximation of the true random numbers is called a pseudo random number computer.

statistician, a sampling plan can be designed where the statistical bounds of the estimate will provide sufficient statistical evidence to support the audit findings.

MEASURES AND AUDIT APPLICATIONS OF STATISTICAL SAMPLING

There are two types of measures of interest used in the statistical sampling. They are called attribute and variable measures. Many audits involve evaluating items in the audit universe on at least one measure of interest. Frequently, though, an audit will require evaluating multiple measures, including one or more of each type.

Attribute measures assume discrete values, that is, the values are countable such as “yes/no” or “good/bad” answers and the results are expressed as numbers, proportions, rates or percentages, such as error rate, percent unsupported. Typical attribute measures in Department of Defense Office of Inspector General (DoD IG) audits focus on the number of errors and error rate in supporting documentation and the number of items unsupported and errors between inventory and inventory records. It is appropriate to use attribute measures in performance, readiness, logistics, or compliance audits.

Variable measures assume a continuous scale, that is, the values such as time or dollars. Variable measures are used in financial statement, contract, and acquisition audits where a dollar estimate is needed and the results are expressed most often as totals or averages, such as total dollar error or average dollar error. Variable measures in DoD IG audits most often focus on financial statement (Chief Financial Officer) audits to estimate dollar misstatements and on performance audits to estimate total dollar misstatement in inventory and timeliness of material movement. Variable sampling designs usually require larger sample sizes as compared to the attribute designs and can be used for both attribute and variable sampling estimates. Generally, the sample size for an attribute sampling design is not sufficiently large enough to support variable estimates with adequate precision.

Statistical sampling designs in financial audits can provide reasonable assurance of detecting material misstatements and sufficient competent evidential matter to support an opinion. Sampling techniques can also be employed for control testing in audit projects. Guidance for internal control testing is found in the Financial Audit Manual for different tolerable error rates. Tables of required sample sizes and an acceptable number of errors are given for assessing low, moderate, or high control risks with 90 percent confidence level at both the 5 and 10 percent level of precision.

In control testing, the statistical outcome is different from classical statistical sampling. For control testing, which is also known as acceptance sampling, the number of incorrect items in the sample is compared to acceptable number of errors. If the number of errors in the sample is greater than the acceptable number of errors, then the system is not in control. Internal control, compliance, and attestation audits typically use this type of sampling design.

TYPES OF SAMPLE DESIGNS

The sampling literature is replete with various statistical sampling designs. To design an efficient sampling plan, several factors such as the audit objectives, universe size and structure, audit measures of interest, audit risk and precision requirements, cost, time, and travel need to be considered. With this information, the statistician can construct a sample design to obtain maximum information about the population measures of interest with minimum costs. All statistical sampling designs are based on three basic design components.

Simple Random Sampling: The simplest sample design is simple random sampling without replacement. In simple random sampling, each sample of a fixed size has the same probability of being selected from the audit universe. The mathematical computations are relatively straightforward for this type of sampling design. Generally, a simple random sampling design is not the most efficient design because it does not control for audit concerns such as high dollar items, locations of the selected items, or items with different risks.

Stratified Sampling Design: A widely used sample design in audit is the stratified sample design. Stratification can be achieved by dividing the universe into non-overlapping strata or subpopulations. These strata may be defined by different dollar amount ranges, different accounting or procedural requirements, different risk levels, or any other factor that may influence the audit measure. Then the sample records are chosen by simple random selection without replacement within each stratum, which maintains representation of the sample to the universe. In general, this is a more efficient design when compared to a simple random sampling design. Strata such as high dollar items can be easily isolated using this sampling design. That is, if the individual stratum sample sizes are large enough, then separate projections can be made for the strata or sub-populations as well as an overall projection for the entire universe. However, this design does not necessarily control for location per se. The selected sample items may be disbursed through the universe, which generally increases travel cost and time to complete the audit. In this respect, the stratified design is similar to the simple random design.

Cluster Sampling Design: The auditor often encounters situations where the universes are geographically or organizationally decentralized. In these cases, simple random sampling or stratified sampling design are not well suited. The cluster sampling may be an effective design that controls for locations thereby minimizing the site visits and travel costs. If economy is the main concern, then cluster sampling may be more applicable. However, this design produces a larger variance and therefore is less efficient when compared to the simple random sample design. If the sub-universes at the sampled locations are large enough, they also may be audited through sampling rather than complete census. The result is a multi-stage design.

By combining these three basic designs in various ways, a statistician can also create more complex designs to afford maximum efficiency and effectiveness in the sampling process. Typical variations are multi-stage designs to control for numerous sources of variation, probability proportional to size designs to put more emphasis on high dollar or high frequency items, and random sampling with replacement as compared to typical sampling

without replacement. To achieve optimal audit results, the appropriate sample methodology should be tailored to the specific objectives of the audit.

For various reasons the project team may not be able to execute the methodology first suggested by the statistician. For example, travel costs may be prohibitively too expensive, the audit may exceed the budgeted amount for the audit, and audit cycle time may be too short. In these circumstances, statisticians can modify the designs to accommodate the audit priorities.

A person with minimal statistical knowledge should be able to use a simple random sampling design without the help of statisticians. Statisticians should be involved in other sampling designs since they require analysis consistent with the design in order to produce valid and defensible results. In audits, using statistical sampling evidence, a statistician should be consulted to ensure proper presentation of statistical findings in order to defend challenges to any of the statistical information.

CONCLUSIONS

Statistical sampling is an approach that is widely used in various disciplines and research area and eliminates the need to perform a census or judgmental sample. Statistical sampling should be an integral part of the audit process, beginning in the planning phase and continuing through findings and recommendations phase. Statistical sampling at one phase of the audit process is a precise planning methodology, and at another phase is a mathematical tool that identifies, measures, and estimates. For complex designs, analysis must be consistent with the sampling designs. In order to produce valid and defensible results involving complex sampling designs, statisticians should be consulted early in the process. Having a statistician involved early in the development of the audit benefits the process by ensuring that the audit is focused, which is a precursor to defining what will be measured in the audit. After the audit topic is defined and scope of the audit is developed, statisticians can assist in developing and defining the population, establishing the target precision level, and the allowable level of audit risk. The audit risk (complement of the confidence level) is determined either by published guidance or in consultation with the statistician and audit management.

Statistical sampling when appropriately applied and implemented can efficiently leverage available audit resources, thereby yielding reportable and defensible results. In addition, it allows auditors to report larger findings and complete their audits in a more timely fashion. In general, this sampling approach produces unbiased projections or estimates when applied correctly. If audit management is willing and in a position to offer additional resources and more time for the audit, then a statistician can optimize the sample design with a lower risk, a higher confidence level, and a better level of precision.*

ACKNOWLEDGEMENT

We thank Ms. Monica Noell for her comments and suggestions that helped to improve the paper.

REFERENCES

- Cochran, W.G. (1977). *Statistical Techniques*. 3rd., New York, N.Y.: Wiley.
- Guy, D.M., Carmichael, D.R. (2002). *Whittington, R. Audit Sampling*. 5th ed., N.Y.: Wiley.
- Kish, L. (2004). *Statistical Design for Research*. Hoboken, N.J.: Wiley
- Lohr, S. L. (1999). *Sampling: Design and Analysis*. Pacific Grove; CA.: Duxbury.

BIOGRAPHIES

*Pictured from left to right are authors,
James Hartman, Frank Sonsini, and Kandasamy Selvavel*



JAMES D. HARTMAN
DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

Mr. James D. Hartman, Jr. has been an Operations Research Analyst in the Quantitative Methods Directorate of the Department of Defense Office of Inspector General, providing statistical and quantitative support for numerous types of projects for eight years. In 2004 he was detailed to the CPA-IG and deployed to Iraq to provide statistical support for audits, inspections and investigations. He is a certified ISO-9000 assessor/lead assessor. His undergraduate degree is in Experimental Psychology from Wofford College, Spartanburg, SC, MBA from University of South Carolina, Columbia and did doctoral work at Clemson University in Industrial Management.

FRANK C. SONSINI
DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

From February 1998 to January 2008, Mr. Frank C. Sonsini was the Director of Quantitative Methods for the Department of Defense Office of Inspector General. In this capacity, he led a team of quantitative experts in providing technical advice and oversight to DoD auditors, inspectors, evaluators and contractors. During his career, he has held positions as Chief, Operations Research Section and Chief, Quantitative Analysis Branch with the U.S. Office of Personnel Management; Statistical Advisor for the Department of Transportation, Office of the Inspector General; and Chief, Operations Research Branch for the Defense Office of the Inspector General. Currently he is an associate with Booz Allen Hamilton. Mr. Sonsini holds a Master's degree in Psychometrics from the Johns Hopkins University and a Bachelors degree in Mathematics and Computer Science from the University of Illinois.

KANDASAMY SELVAVEL
DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

Dr. Kandasamy Selvavel has over six years of statistical consulting and oversight experience with the Department of Defense Office of Inspector General. Dr. Selvavel has published over 20 research papers in various professional journals. Prior to joining OIG, Dr. Selvavel worked for over three years as a Mathematical Statistician at the Census Bureau. He also taught several college level mathematics and statistics courses at universities for 10 years prior to joining Government. Dr. Selvavel holds Master of Arts and Doctor of Philosophy degrees in mathematics with major in statistics from Bowling Green State University, Ohio.



5 IS YOUR IDENTITY BEING THROWN OUT WITH THE TRASH?

BY LOU MAJOR
UNITED STATES NAVY
NAVAL AUDIT SERVICE

“None of the bases audited believed they had a problem – but every base audited did. Does yours?”

This was the question posed to major Navy and Marine Corps commands last year by Auditor General of the Navy Richard Leach. An email message was sent to audit liaisons throughout the Department of the Navy (DON), after a series of “dumpster diving” audits by the Naval Audit Service (NAVAUDSVC) determined that Navy and Marine Corps facilities across the nation were improperly discarding paper documents loaded with personally identifiable information (PII), including Social Security Numbers (SSNs). During the series of audits, NAVAUDSVC notified DON leadership as soon as the vulnerabilities were discovered, and the leadership immediately began taking aggressive corrective actions to improve policy and internal controls, train the workforce, and put personal information of DON uniformed and civilian personnel under tighter control. The issues the auditors identified in DON were occurring as the Government and the nation learned of exposure to potential identity theft of 26 million active and retired military personnel in the summer of 2006.

Fortunately, the stolen computer, which had been routinely taken home by a Department of Veterans’s Affairs (VA) employee, was later recovered with no evidence that the personal data contained on the unit’s hard drive had been accessed or compromised. While that incident did not result in any permanent harm, loss of privacy data continues to be a challenge for the Federal Government – as it does for the rest of the Department of Defense (DoD) and DON. During the 18 months after the VA computer theft, DON had more than 100 incidents involving the loss of privacy information, reportedly affecting more than 200,000 Navy and Marine Corps uniformed personnel, civilian employees, retirees, and family members.

WHAT IS BEING DONE ABOUT IT?

After the VA computer incident, the media and the public watched with keen interest as the U.S. Congress began asking questions about how federal agencies protect their computers and the personal data that is stored in them. In response to the VA incident, as well as other instances

of inadvertent exposure of PII within the government, DON’s Privacy Office requested all commands to conduct self-assessments of their activities’ compliance with Navy and DoD guidance on collecting and handling sensitive personal data.

Just as the government’s biggest organization – DoD – joined other Federal agencies in issuing new guidance or reminders concerning existing rules and regulations, NAVAUDSVC had already begun to share the results of the series of internal audits that had begun before VA’s computer loss, and that continued into the months after the computer theft and recovery. While the VA incident highlighted the security problems involved with protecting PII on electronic media, the Audit Service’s reports brought to the fore the risks posed by the handling and disposal of paper documents.

Most of the PII-related audits were in a series that resulted in what were irreverently called “the dumpster diving” reports that focused on the possible consequences of improperly performing a simple office chore – throwing away the trash. When auditors were looking at a Naval training command’s management of its DON-mandated Privacy Act Program (at that Command’s request), they found a major problem concerning how paper documents that contained privacy information were being discarded. Intact documents containing PII were being placed into a dumpster that was picked up weekly by a commercial recycling firm. When the team visited the commercial facility to determine what happened to the documents after they were picked up, auditors found the documents being dumped on the floor, pushed onto a conveyor belt, baled, and sold to the highest bidder. With that discovery, and realizing the potential for exposure of a significant number of DON personnel to identity theft if the problem were not isolated to that one base, the auditors began focusing on internal controls over the disposal of paper documents containing PII at additional locations. NAVAUDVSC quickly scheduled a series of similar audits at seven more Naval and Marine Corps bases across the country, during which auditors did literally pick through office trash and other dumpsters looking for – and finding – discarded papers containing PII.

At every facility visited, personnel were putting material into the office trash for recycling on the good-faith assumption that the handlers of that trash were ensuring that the PII that might be on those papers was being protected until it was burned or shredded. But that assumption was mistaken. The Naval auditors were finding case after case in which discarded office forms and other papers that contained PII were accessible intact to those who should not have had access to the personal information. They found hundreds of official documents bearing thousands of names, SSNs, and other elements of PII that could identify DON's uniformed and civilian personnel. The auditors found that:

- At every location audited, documents were found in bales that were accessible by unauthorized personnel before they were sent to a paper mill for recycling, instead of being destroyed before or immediately after they were picked up.
- One program office was found to be storing burn bags that contained forms with PII in a break room, with possible access by unauthorized personnel.
- Another program office placed program-sponsored sporting event forms containing PII (including credit card numbers, names, addresses, and dates of birth) into trashcans accessible to other people in the office. Once picked up, that trash was available to even more people, including those people picking up and transporting the trash to disposal facilities. Another office placed completed health information forms with many elements of PII information into trash cans.
- At one location, an auditor picked up a piece of blowing trash near a dumpster on base and found it to be a document containing PII from a tenant command; the PII on that document was accessible to anyone walking in that area.

While the loss of paper documents might not seem to compare to the potential of the loss of a computer loaded with data, the potential damage from inappropriate handling of documents is significant. One inappropriately discarded document found during an audit listed more

than 2,000 names and SSNs. A privacy training program on DON's privacy website states, "Over 20 percent of breaches are due to improperly disposing of documents containing PII."

During this period, one base held a program to educate personnel about the risks of identity theft, and the sign-up form required names and SSNs. Personnel signing in for the identity theft class could easily have noted names and SSNs of other personnel who had signed in ahead of them.

WHAT COUNTS AS PII?



The Department of Defense, following the Privacy Act of 1974 and guidance from the Office of Personnel management, defines PII as information that can be used to identify a person uniquely and reliably, including, but

not limited to: name; Social Security number; home address, telephone number, and email; and mother's maiden name. Other identifiers, which must be protected when combined with a name, are race, religion, family and/or personal health data, and work-based information such as performance ratings, and payroll and leave information.

Information that could link personnel to the Defense Department is also a concern, even though it may not fall under the provisions of the Privacy Act. DoD and DON homeland security guidance issued by the Office of the Secretary of Defense states that exposing the names of DoD personnel is a threat to national security because it identifies such personnel to, and makes them targets of, terrorists. This information, like PII, can be inadvertently revealed by improper disposal of paper records.

But some PII is easily available from the phone book and the internet.

That doesn't matter. For DON's purposes, it does not matter that some PII that must be protected may be readily available from other public sources, such as names and addresses in telephone books, and email addresses and even credit histories from various internet sources. DoD and DON have each issued guidance – DoD for all of the military services, and DON specifically for the Navy and Marine Corps – on how operations must be conducted to comply with the Privacy Act. Congress passed that law in 1974 to establish protections for Americans' whose PII is collected by Government and businesses. For purposes of compliance with the Privacy Act and homeland security guidance, information that identifies Navy and Marine Corps personnel, or links them to DoD, should be safeguarded and disposed of properly.

The auditors found that many Naval and Marine Corps personnel were unaware that, in DON, even a person's name, without any other identifying information, is considered PII based on the current guidance, and must be protected. Secretary of the Navy Instruction 5211.5E defines PPI (PII) as "any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, Social Security number, or biometric records." Thus, when material contains even a single name of a DON military or civilian employee, it must be treated with the same precautions and safeguards as material that contains multiple types of directly associated PII. DoD and DON are both currently reviewing their PII-related guidance, so it is not known if this strict interpretation of what must be protected will remain in place.

BUT EVERYBODY TOSSES UNNEEDED STUFF IN THE TRASH CAN...

Yes, but not everything that goes into the trash can is just trash. PII on documents is not trash – it is valuable information that can provide clues to steal someone's identity, and establish credit accounts and run up debts or commit fraud in their name.


DON guidance states that documents and other material containing PII should not be discarded intact into trash cans and waste bins. Hard copy documents should always first be destroyed by shredding, burning, or other methods that render the document beyond recognition or reconstruction. Even dedicated containers to collect material for recycling can be problematic, as the Naval auditors found. On bases near commercial recycling centers where unshredded documents with PII were found, personnel in the Navy commands thought the material they were discarding was being destroyed by someone else before it left the base. However, no one had reviewed the chain of custody from the "recycle box" in the offices, to the mills where the documents would actually be reduced to paper pulp.

As a result, numerous personnel who did not have proper authority – government employees, contracted collectors of the trash, personnel at the receiving stations where the material was baled, and/or workers at the paper mills – could have had access to intact pages containing PII. The auditors had no way of determining whether any inadvertent accessing of PII documents by unauthorized personnel actually occurred.

BUT IS SHREDDED PAPER RECYCLABLE?



Some of it is, some isn't. Ironically, goals to protect the environment by recycling while also protecting PII through shredding can lead to a contradictory outcome. Some forms of shredding – particularly cross-cut shredding that produces tiny diamond-shaped confetti rather than strips of shredded paper – reduce the fibers in paper to the point that, in many cases, it is not suitable for reconstruction. The result is that papers with PII that are cross-cut shredded cannot be recycled and must be burned or buried in a landfill. Many local governments across the country, and even some military bases with recycling programs, specifically state that cross-cut shredded paper is not wanted. However, Navy guidance does allow for shredding into strips of a size that are still usable for



recycling. At locations where offices have already invested in cross-cut shredders, the recycling of some material may have to be sacrificed to the concerns for personal identity protection and national security.

WHAT OTHER PRIVACY CONCERNS DOES DON HAVE?

As the events surrounding the loss of the VA computer unfolded, auditors were also completing an audit of an entire Naval district's management of Privacy Act information (PPI/PII), to verify whether management controls were adequate within the district's operations and systems to reduce the risk of unauthorized disclosure of PII.

“One inappropriately discarded document found during an audit listed more than 2,000 names and SSNs.”

During that audit, auditors found that the district's Privacy Act Program was not being properly managed: privacy managers for records systems were not being designated, personnel were not being trained on their responsibilities regarding privacy information; and proper records were not being kept. Auditors also found:

- Nine of 15 program offices at one command unnecessarily collected and used full SSNs to verify civilian and military personnel eligibility for services and benefits, even though records could have been retrieved by combining another identifier, such as a date of birth or the last four digits of an SSN, with the individual's name – thus not requiring a full SSN.
- A program office was storing vehicle registration forms with SSNs in unlocked cabinets that were accessible by unauthorized personnel.
- A program office did not password-protect a computer used for recording customer information that included PII from military and civilian personnel.

- A program office did not mark, using For Official Use Only (FOUO) language, transmittal documents that contained PII.

WHAT HAPPENS IF THERE IS AN ACCIDENTAL RELEASE OF PII?

Commands are now addressing that issue. In addition to the issues in collection, handling, and disposal of PII, the auditors found another problem: none of the program offices visited had a plan of action in case of a breach of information. In the past, there were no criteria requiring program offices to have such a contingency plan, but in the wake of inadvertent disclosures in recent years, DON, DoD, and other federal agencies have adopted requirements for their offices and activities to develop contingency plans.

WHY DID ALL THIS HAPPEN?

The problems cited above occurred because priority was being given to collecting Privacy Act information rather than to the overall management of PPI, the audit concluded. This hindered the district's efforts to balance the need to maintain information for official use, with the obligation to protect individuals against unwarranted invasions of their privacy. This resulted in a less-effective Privacy Act Program that increased the risk of information compromise. Commanders concurred with all of the recommendations in the report and took appropriate actions to beef up the district's Privacy Act Program.

WHAT IS DON DOING ABOUT PII NOW?

After reports on the eight “dumpster diving” audits were issued, NAVAUDSVC issued a summary report to the highest military and civilian levels of DON, recommending the establishment of new Navy-wide and Marine Corps guidance ensuring that proper procedures for disposing of PII-containing paper waste were established, and that internal control procedures be established to ascertain that the disposal procedures are being followed throughout the Navy and Marine Corps. Navy and Marine Corps leadership to whom the recommendations were directed agreed and took aggressive corrective actions.

In his message to the audit liaisons, the Auditor General recognized that at every location where the disposal problems were found, corrective action by Navy and Marine Corps personnel was swift. The auditors notified the commanders of each base immediately upon discovering the problems, and the commanders in turn notified the various commands, activities, and offices on each base. The issuance of the audit reports was something of a formality, for by the time the reports were published, new guidance was being written, procedures for discarding and collecting paper documents containing PII had been appropriately revised, personnel were being trained, and documents were being shredded before being discarded.

DON leaders also stressed the importance of protecting PII. The Auditor General briefed DON's General Counsel (OGC) and the Secretary of the Navy (SECNAV). The brief to SECNAV led to a cooperative effort by NAVAUDSVC and the Office of the DON Chief Information Officer to draft an "all-hands" message from the SECNAV, Hon. Donald C. Winter, in July 2007 to keep the issue of privacy front and center in the minds of Navy and Marine Corps uniformed and civilian personnel.

DON military and civilian employees can rest more easily that internal controls are in place to protect their personal data so they do not become exposed to potential identity theft.*



BIOGRAPHY

LOU MAJOR
UNITED STATES NAVY
NAVAL AUDIT SERVICE



Lou Major is the Privacy Officer at the Naval Audit Service, Washington Navy Yard. After retiring from a 30-year career in daily newspaper journalism in his native Louisiana, he joined the Naval Audit Service in 2003. In addition to editing audit reports, he serves as the Freedom of Information Act officer and responds to media FOIA requests, oversees the agency's Privacy program, helps teach a report writing course for auditors, and handles some of the agency's photography needs.



The Naval Audit Service (NAVAUDSVC) audits and assesses business risks within the Department of the Navy (DON). Internal audits give DON managers objective feedback on efficiency and effectiveness of DON programs, systems, functions, and funds. Audits have defined objectives and are done following generally accepted Government auditing standards (GAGAS) issued by the Comptroller General of the United States. These are professional auditing standards that include those professional standards required of private sector public accounting firms. Based on their work, auditors certify or attest to the accuracy of data or to the assertions of management. The work and opinion of auditors, within the bounds

of their profession, carries recognized legal weight in court proceedings. Each audit report presents conclusions on pre-established audit objectives, and where appropriate, summarizes a condition that needs management's attention, explains the root causes and effects of the condition, and recommends potential solutions. Audit reports are provided to the Department of the Navy commands and activities; Department of Defense Inspector General (DoD IG); Congress; and, via the Freedom of Information Act, to the public.

6 PROCUREMENT FRAUD INVESTIGATIONS DURING MILITARY OPERATIONS IN SOUTHWEST ASIA



BY COLONEL JOE ETHRIDGE, CURTIS GREENWAY, WESLEY KILGORE
701ST MILITARY POLICE GROUP
U.S. ARMY CRIMINAL INVESTIGATION COMMAND

INTRODUCTION

Procurement fraud¹ investigations can be exceedingly difficult and complex in the best of circumstances. These investigations may involve thousands of documents, key witnesses who are located throughout the world, highly technical subject matter, and sophisticated and resourceful subjects. Procurement fraud investigations are even more difficult when conducted in the midst of United States military operations² in a foreign country.

This article describes the work of the U.S. Army Criminal Investigation Command (often called Army CID) and several other federal agencies to investigate fraud arising in contracts supporting the U.S. Army's operations in Afghanistan, Kuwait, and Iraq. The article starts with a discussion of the procurement fraud threat in modern military operations. It then describes the assessment of the fraud threat in Iraq, the deployment of fraud special agents to Southwest Asia, and the results of the investigative activity to date. Finally, in what we hope will be the real value of this article, we discuss some of the lessons learned from this experience. Although this article discusses procurement fraud investigations during military operations, similar issues might arise in other extraordinary circumstances – such as natural disasters in the U.S. or overseas, or terrorist attacks – where the U.S. response involves significant levels of government contracting.

1 By “procurement fraud” we mean any intentional deception related to procurement that is designed to unlawfully deprive the United States of something of value or to secure from the United States an unentitled benefit, privilege, allowance, or consideration. These cases frequently involve bribes, gratuities, false statements, false claims, false weights or measures, misrepresenting material facts, adulterating or substituting materials, falsifying documents, and secret profits, kickbacks, or commissions (see Enclosure 2, DOD Instruction 5505.2, Criminal Investigations of Fraud Offenses, February 6, 2003).

2 In consideration of those unfamiliar with the military, we will use the term “military operation” to refer to any use of the U.S. military for national defense or national security missions. Within the Defense Department, such operations may be called “contingency operations” (Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms) or more recently, “expeditionary operations” (Report of the Commission on Army Acquisition and Program Management in Expeditionary Operations, available at www.army.mil/docs/Gansler_Commission_Report_Final_071031.pdf).

THE PROCUREMENT FRAUD THREAT IN MODERN MILITARY OPERATIONS


Profiteering and fraud are not new to warfare. Those with the desire to enrich themselves from the misfortunes of war have been present throughout American military history. In the Revolutionary War, for example, Major General Nathaniel Green was appointed Quartermaster General of the Continental Army because the Continental Congress was concerned about fraud and the resulting abysmal state of supply at Valley Forge. In the Civil War, Brevet Brigadier Montgomery C. Meigs, who had made a name for himself by speaking out against profiteering lobbyists in search of Corps of Engineers contracts in the pre-war years, was appointed as Quartermaster General of the Army to stop massive frauds perpetrated on the Union Army.³

Three factors have increased the risk of procurement fraud in modern military operations. First, logistical support that was once provided by organic military units is now contracted out. As a result, the U.S. government now has more contractor personnel in Afghanistan and Iraq than it has soldiers.⁴ This is plainly visible in a visit to any of the military dining facilities in Baghdad or Balad, Iraq. The only personnel you will see in uniform are the diners, and nearly half of those diners may be in civilian clothes themselves. The headcount clerks, the cooks, the servers and the clean-up crews will all be contractors. The doctrinal Army combat service support imperative to “man, arm, fuel, fix, and move forces in combat operations” could, and probably should, be amended to “acquire contract goods and services.”

3 The Civil False Claims Act (31 U.S. Code §§3729 to 3733), one of the most effective tools available to counter procurement fraud, was enacted as a result of fraud encountered during the Civil War.

4 The Gansler Commission estimated that the U.S. has 160,000 contractors in these two countries, over 50 per cent of the total force. See www.army.mil/docs/Gansler_Commission_Report_Final_071031.pdf at p. 13.





Second, the acquisition workforce was cut substantially in the 1990s. There now are fewer contracting specialists available to define the Army's needs, to acquire quality contractors to provide goods and services, and in particular, to monitor contract performance and insure quality control. Third, the Army's need for immediacy, in service and delivery of goods and services, in austere environments creates vulnerabilities. Distributed operations over vast distances, the norm on modern battlefields, dilute the supervisory chain.

Thus, our reliance upon contractors for combat service and support (a reliance that will only increase over time given the complex maintenance requirements of modern equipment and digital communications networks and the desire to optimize soldier strength on the task of waging combat), a shortage of acquisition personnel, the contingency environment, and the business model relative to this environment place the Army in a challenging position. Given the vast dollar amounts involved, the opportunity and the motive exist to illegally and opportunistically make a fortune in a very short period of time in this environment.



ASSESSMENT OF THE CONTRACTING ENVIRONMENT IN THEATER

Army CID's Major Procurement Fraud Unit (MPFU) consists of civilian special agents who specialize in the investigation of fraud in major acquisitions and weapons systems. These special agents are located throughout the United States near concentrations of major defense contractors. Before the year 2005, these special agents had not been utilized in a combat environment as their function was to provide the capability to conduct complex investigations of fraud at the CONUS industrial base of the supply chain. In short, MPFU's wartime mission was intended to be in the United States to provide oversight of the major defense contractors as they increased production in response to wartime demands, concentrating on the procurement actions directly impacting upon soldier safety and Army readiness. Through the performance of this mission, the MPFU developed the predominant expertise in the arena of fraud investigations within Army CID.

In early 2005, the Major Procurement Fraud Unit began to suspect that conditions in Iraq were favorable for procurement fraud. This suspicion arose based on criminal intelligence information, reports from commanders, fraud and procurement irregularities cases reported by the Army's active duty criminal special agents in Iraq, and the dollar volume of contracts being issued there.

An assessment was necessary to determine the full extent of the fraud threat and whether the deployment of fraud special agents to the theater was necessary to address that threat. The assessment began in the spring of 2005. Special agents reviewed criminal intelligence data, spoke with the Army's Procurement Fraud Branch,⁵ and consulted with specialists in Army contingency contracting.

Special agents then traveled to Iraq in July 2005 and again from September to December 2005 to assess the situation on the ground. They spoke with contracting officials, audit and internal control personnel, and military legal counsel. They studied contract files and the contracting procedures in use at the time. The conclusion from all of this groundwork was inescapable. Conditions in Iraq were highly conducive for fraud because of a number of factors:

- 1) the sheer dollar volume of all contracts being awarded, and the dollar amounts of individual contracts, could provide an incentive for kickbacks, bribery, disclosure of procurement sensitive information, and other violations of law,
- 2) numerous contracting files did not exist or were not prepared according to normal standards,
- 3) auditing and internal control resources were in short supply in Iraq,
- 4) the operational tempo was high,
- 5) there was no formal structure for reporting and investigating allegations of procurement fraud,
- 6) contracting procedures were relaxed,
- 7) sufficient checks and balances were not in place,
- 8) quality assurance and contract administration were weak or nonexistent, and
- 9) a large number of contracts issued were cost reimbursement contracts.

⁵ The Army Procurement Fraud Branch, located in Arlington, Virginia, is responsible for the coordination of remedies in all significant cases of fraud in Army procurements.

DEPLOYMENT OF CRIMINAL SPECIAL AGENTS

The Major Procurement Fraud Unit opened a fraud investigation office in Iraq in December 2005. It was planned that the office would be staffed continuously with special agents who would deploy for six month tours of duty, reinforced by military agents already serving in theater on one year rotations. Initially, the office was manned with civilian special agents, all of whom had volunteered for the duty, and most of whom had never previously worked in a combat environment. Before departing the United States, the special agents processed through a replacement center, where they completed medical, dental, and legal processing; they obtained uniforms and necessary equipment; they received training in rules of engagement, the law of land warfare, first aid, cultural awareness, hostage survival skills, code of conduct, and improvised explosive device recognition; and they qualified with individual weapons.

The first rotations of special agents established the framework for the long-term presence of the fraud office in Iraq. The active duty CID agents already present in Iraq helped to establish the fraud office. The special agents began to develop working relationships with contracting offices, internal review and audit offices, and military legal counsel. They developed confidential sources of information and worked with Army units to enhance fraud awareness and crime prevention efforts. After finding a target-rich environment of potential fraud cases, they focused on corruption (kickbacks, bribery, and illegal gratuities) by soldiers and Army civilian employees and placed an emphasis on major fraud cases.

The mission required frequent travel between Iraq and Kuwait, but this travel was dangerous and time consuming. In June 2006, a fraud office was opened in Kuwait to support the Iraq fraud office and to investigate cases arising from contracts issued in Kuwait. Eventually, an office was opened in Afghanistan and another office was opened in Iraq, for a total of four fraud offices in the theater.

The investigations in Iraq required the efforts of several other federal agencies. The Defense Criminal Investigative Service provided a number of their own fraud special agents who were co-located with the Major Procurement Fraud Unit special agents. Several attorneys with the Public Integrity Section and the Antitrust Division, Department of Justice, evaluated the cases being developed and arranged for prosecutions in the appropriate venues. Prosecution support has since expanded to include all Divisions of the Department of Justice and numerous US Attorney Districts throughout the United States. Special agents with the Special Inspector General for Iraq Reconstruction, who had been in Iraq for quite some time, provided valuable criminal intelligence and other information. FBI agents located in Kuwait and Iraq provided valuable support through the legal attache system.

As the mission and its complexity grew it became obvious that many and varied resources would be needed in a coordinated effort. In October 2006, Army CID, DCIS, SIGIR, and the FBI formed a joint investigative task force to coordinate efforts, share resources, and expand capabilities. The Department of State Inspector General (DOSIG) and US Agency for International Development (USAID) subsequently joined the task force to form now what is known as the International Contract Corruption Task Force (ICCTF). The ICCTF's mission is to utilize the full measure of investigative, intelligence, audit, and prosecutorial resources to combat corruption and fraud affecting the United States Government's international procurement programs to include all Global War On Terror initiatives. The ICCTF is managed by a Board of Governors consisting of senior representatives of the member organizations. Due to the volume and complexity of the investigations it became necessary to establish a centralized operation to coordinate task force operations and intelligence. Although it previously existed informally, in June 2007 the Joint Operations Center (JOC) of the ICCTF was put into full operation as a capability to capture and analyze criminal intelligence, de-conflict investigations, coordinate investigative resources, and provide operational assistance to the more than 100 ongoing investigations. Although all partner elements are represented in the JOC, the FBI played a key role in its establishment.

THE RESULTS

Since December 2005, the ICCTF has opened over 135 investigations. Subjects include contracting officers, contracting officer's representatives, and other contracting officials (comptrollers, QA, engineers, source selection board members). A total of 24 persons (19 government employees – both military and civilian) have been charged or indicted, fourteen of those have been convicted. In addition to criminal sanctions, administrative and civil remedies are pursued in every case. To date, more than 40 persons or companies have been suspended or barred from contracting with the US Government and more than \$17.6 million in fines and penalties have been levied. These results are very much preliminary. The natural course of fraud investigations involves an extended timeline.

LESSONS LEARNED

Much has been learned from the investigative efforts described above:

1. *Emergencies beget expediencies; expediencies beget opportunities for fraud.* There will always be someone willing to take advantage of a crisis, an emergency, a natural disaster, an armed conflict, or other human suffering.

2. *Federal agency partnerships are crucial.* The Army, like other federal agencies, does not have the fraud investigative resources necessary to cover all aspects of its anti-fraud mission. The formation of the ICCTF was driven by common interests and the desire to bring every tool available to bear to rapidly develop and address the fraud threat facing the Army and the Joint Force. The natural partner for MPFU is the Defense Criminal Investigative Service, which, among its other duties, performs the procurement fraud investigative role in support of Department of Defense agencies. MPFU and DCIS special agents have years of experience in working joint investigations, as there is frequent and obvious overlap in the interests of the Army and other Defense Agencies. That relationship paid immediate dividends. DCIS special agents are co-located with and operate out of the four fraud offices MPFU established in theater. The role of SIGIR personnel in Iraq is to identify and

investigate indications of fraud, waste and abuse of Iraq reconstruction funding. As Army personnel are responsible for the contract administration associated with much of this funding, the missions of SIGIR and MPFU overlap. SIGIR personnel work directly with MPFU agents in Iraq, in task forces formed to pursue priority cases of common interest and in the JOC.

3. *A corollary to Lesson 2: When not facing a contingency or emergency, cultivate good working relationships with sister agencies.* You never know when you might need their help.

4. *Special agents need eyes and ears (that is, criminal intelligence analysts).* Such analysts played a key role in the fraud investigations initiated in Kuwait, Iraq, and Afghanistan. Early in the deployment, the task force recognized that the conspiracy, bribery, and money laundering elements of the crimes (given the complex international environment) contained many similarities to investigations of illegal drug networks. CID sought assistance from the Department of Defense Criminal Investigation Task Force (the CITF), a joint organization responsible for conducting investigations of terrorists for the Department of Defense. The CITF has built a tremendous criminal intelligence capability since the organization was formed in the days following September 11, 2001. Although this capability is focused on terrorism and terrorist groups, these CITF-trained personnel were immediately able to bring analytical tools to bear in order to better identify the relationships between the conspirators involved. Taking another lesson learned from the CITF, criminal intelligence analysts were integrated into the investigative task force, working hand in hand with the special agents, rather than relegating them to backroom intelligence centers or watch centers.

5. *Investigative agencies need to try new concepts of operations.* Over time, the partners of the ICCTF developed a functional concept of operations that will translate to future contingency environments. The fraud offices in theater, enabled by teams of auditors, review contracting operations for crime-conducive conditions and indicators of fraud. These conditions are identified to the leadership of the acquisition community through a crime prevention

survey. The agents open investigations to pursue the indications that fraud has occurred. As individual cases develop, they are forwarded to an operations center in the US for assumption of the investigation. This transfer of the investigation not only reduces the footprint in the theater, but also enables criminal intelligence, money tracking, and prosecutor resources to be brought to bear. The task force headquarters has the freedom to refer investigative leads back to the contingency fraud offices, or to offices of the partner agencies that are stationed throughout the US and, depending upon which partner agencies are involved in the investigative effort, around the world for appropriate action.

6. *Special agents need to be present at the start of a contingency or emergency operation.* First, their mere visible presence will tend to deter procurement fraud. Second, they can work with procurement officials to identify weaknesses in contracting procedures and enhance awareness of fraud indicators before the situation gets out of hand.

7. *A contingency or emergency operation will expand the role of special agents.* The mission will require far more from special agents than the traditional role of establishing whether or not a crime has occurred. We have learned that the role of the MPFU, for all of CID, goes much further. For example, the Army expects that measures will be identified and implemented to correct the crime-conducive conditions that made the organization vulnerable. As a normal course of business, MPFU conducts crime prevention surveys to report and seek corrective action to systemic weaknesses and crime-conducive conditions identified during its investigation of fraud, waste and abuse in the Army. During investigation of contingency contracting in Kuwait, MPFU teamed with the Army Audit Agency and produced a crime prevention survey and an audit survey that the Army has used to identify and correct deficiencies in its contracting operations. The combination of investigation and audit used so successfully in Kuwait to identify fraud and systemic weaknesses is being expanded throughout the theater. Furthermore, as an Army organization, MPFU is heavily engaged in all aspects of the Army's response to correct identified vulnerabilities in contingency contracting and prevent future occurrences. The MPFU

has partnered with the acquisition community to conduct fraud awareness and prevention training to all employees associated with contracting, with priority given to the contingency contracting activities. Also, CID and MPFU are actively supporting the Army Contracting Task Force, established by the Honorable Pete Geren, Secretary of the Army. The task force's mission is to survey Kuwait-based contract actions for analysis and corrective action. Finally, CID contributed to the Gansler Commission's study of the Army's contingency contracting system.⁶

8. *The use of active duty special agents and civilian employee special agents provides synergism.* CID has achieved a great balance in its soldier and civilian special agent personnel. Getting the mix right is important to CID in its constant effort to optimize resources to best posture the command for success in the worldwide environments in which the command is expected to operate. Each type of agent, military and civilian, brings their own set of advantages. Operations in Iraq and Afghanistan have proven that the mix is sound. The soldier-agent is the backbone of CID. The rapidly deployable CID detachments and battalions are manned by active and reserve component warrant officers and noncommissioned officers recruited from every branch of the Army and then trained and credentialed to serve as the special agents who are the first line in investigating felony-level crimes of Army interest all over the world. They can, and do, operate out of the most austere of forward operating bases. Each agent is trained in crime scene processing as a core competency. This training goes against the prevailing norm of designating specialty teams to perform the crime scene processing function, but supports the Army model of operating anywhere in the world rather than from large, fixed air bases and ports. The fraud specialists, as mentioned earlier, as well as crime laboratory technicians, computer crimes agents, and some other specialists of the command, are civilians. The fraud investigations that the MPFU undertakes tend to be of long duration (two years is not uncommon for an individual case) and the prosecution venue is, normally, a U.S. Federal Court. The length of the investigations and the venue for prosecution suggests civilian agents as the appropriate manning. The challenge to this logic is the

⁶ The Commission's report is at www.army.mil/docs/Gansler_Commission_Report_Final_071031.pdf.

contingency environment, but as the major contracting and procurement functions are associated with the larger forward operating bases, rather than the combat outposts, the civilian agents proved to be able to translate their proven skills with great effectiveness. The common thread for both military and civilian special agents is a “community policing” aspect that cannot be overstated. The military agents were soldiers for at least two years before they could apply to be trained as special agents. The majority of the civilian special agents of the MPFU have served previously on active duty, and several continue to serve as agents in the reserve component. The bottom line is that these men and women are very much a part of the “community” that they support in the conduct of criminal investigations and are absolutely committed to the Army. This is a powerful component that cannot be overstated, as police agencies throughout the world have capitalized on in the community policing initiatives.

9. *Out of emergency situations, many fraud remedies will flow.* The special agent’s work does not end with a guilty plea or a prosecutor’s decision to forego prosecution. In most cases, other civil, contractual, or administrative remedies (such as suspension and debarment) will be available to help make the government whole. The special agent must be prepared to support all the remedies available in a particular case.

10. *Bring your lawyers.* A contingency or emergency will generate many legal issues in the areas of criminal law, agent authority, appropriations law, and domestic and international law.

11. *Special agents need to be familiar with their agency’s contingency or emergency contracting authorities and procedures.* Going into the contingency contracting mission, the MPFU and other investigative and audit agencies did not have the experience or training needed to be able to understand the major differences between contingency and sustainment contracting. To turn that around, the assistance of the Defense Acquisition University was solicited to develop the “Investigations in a Contingency Contracting Environment” course. Now, most MPFU agents have been trained along with many from other investigative and audit agencies.

12. *Special agents and their supervisors need to have given some thought to what they need to do to prepare for a possible deployment and the hardships it might bring.* Deploying CID civilian agents and support personnel to a combat environment for the first time brought many challenges to both the individual employee and management. However, after more than two years most of the logistical and administrative requirements to deploy a civilian work force and establish investigative operations in an austere environment have become routine, and a dedicated work force has accepted the challenge to succeed in their mission.

SUMMARY AND CONCLUSIONS

Battlefield and contingency contracting fraud is nothing new. For the United States, the need for fraud investigative capability dates back to Valley Forge and the Revolutionary War. However, the employment of contractors on the battlefield by the Army and all of the Joint Force has increased dramatically over just the past 15 years, a trend with no indications of decline. Army CID, its partners in the International Contract Corruption Task Force, the Army Audit Agency, and the Army acquisition community are developing and implementing the controls to ensure proper oversight of the funds entrusted to the Army by the people of the United States.

The work of the MPFU, and all the partner elements of the ICCTF, is having a positive effect on many fronts. The crime trends and system vulnerabilities are regularly briefed to the senior leadership of the Department of the Army. The crime prevention products have been incorporated into the action plan of the Army Contracting Task Force that is organizing the contingency contracting structure and developing the procedure for future operations worldwide. Contractors who have proven that they are not worthy business partners are debarred or suspended. The criminals that have violated the public trust are being identified, pursued and prosecuted. The Public Trust, the readiness of the Army and all the Joint Force and the safety of the men and women who wear the uniform of the United States make the work of the MPFU, CID and all the partners of the ICCTF so important, and satisfying.*

BIOGRAPHIES



COLONEL JOE ETHRIDGE
701ST MILITARY POLICE GROUP
U.S. ARMY CRIMINAL INVESTIGATION COMMAND

Colonel Joe Ethridge is the Commander of the 701st Military Police Group (CID), the organization responsible for the Army's protective services, computer crimes and major fraud investigations units. He is a former Commander of the Department of Defense Criminal Investigation Task Force and Provost Marshal of the 1st Infantry Division. He has served in Germany, Egypt, Haiti, Kosovo, Bosnia and Iraq. Colonel Ethridge holds Master's degrees in public administration and strategic studies. He has been selected to command a task force in Afghanistan following his current assignment.



CURT GREENWAY
701ST MILITARY POLICE GROUP
U.S. ARMY CRIMINAL INVESTIGATION COMMAND

Curt Greenway earned a Bachelor of Business Administration degree from Ohio University, an MBA from Monmouth University, and a law degree from Ohio Northern University. He has practiced law as a sole practitioner, an assistant county prosecutor, an assistant county public defender, an active duty Army judge advocate, and a litigation attorney with the Army Procurement Fraud Division in Arlington, Virginia. Since 2000 he has advised the 701st Military Police Group, U.S. Army Criminal Investigation Command, Fort Belvoir, Virginia, on procurement fraud and a variety of general legal issues. He is a member of the bars of Ohio, Hawaii, and the U.S. Supreme Court.



WESLEY KILGORE
701ST MILITARY POLICE GROUP
U.S. ARMY CRIMINAL INVESTIGATION COMMAND

Wesley Kilgore has over thirty-four years of law enforcement experience. He retired from the Army in 2002 after serving in law enforcement assignments around the world. In his current position as the Director of the Major Procurement Fraud Unit, U.S. Army Criminal Investigation Command, Mr. Kilgore oversees the investigative activities of over one hundred fifty criminal investigators and staff personnel who specialize in the detection and investigation of major procurement fraud. He attended Ball State University, Muncie, Indiana, where he graduated magna cum laude. He has completed the Army Management Staff College, the Warrant Officer Basic and Advance Courses, the study of German at the Defense Language Institute, and advanced courses in investigative techniques and management. He was the 1992 International Narcotics Officer's Association Agent of the Year and the 1995 U.S. Army CID Special Agent of the Year. He received the Legion of Merit upon retirement from the Army.



7 IMPROVING THE COORDINATION OF U.S. COUNTERTERRORISM POLICY

BY LEIGH-ALISTAIR BARZEY
DEFENSE CRIMINAL INVESTIGATIVE SERVICE

THE ISSUE

The terrorist attacks on September 11, 2001, which resulted in nearly 3,000 dead, were horrific and shocked not only the American public, but many within the U.S. government. In response, President George W. Bush and the Congress created the National Commission on Terrorist Attacks Upon the United States (more commonly known as the 9/11 Commission).¹ Among its many findings, the 9/11 Commission was particularly troubled by the government's failure to coordinate the efforts of agencies with counterterrorism responsibilities. Furthermore, the 9/11 Commission found that, despite extraordinary efforts by individuals, the U.S. government was not properly organized to enable agencies to "adjust their policies, plans, and practices to deter or defeat [the terrorist threat]."² In analyzing the government's reaction immediately following the attacks, the 9/11 Commission also recognized the need for national crisis management. The September 11th attacks proved that in a crisis, it is the president and the West Wing staff that are crucial to marshalling a response.

Unfortunately, some have narrowly focused on the intelligence failures raised in the 9/11 Commission's report, namely the alleged inability of law enforcement officers and intelligence analysts to "connect the dots." Intelligence, whether it concerns the collection, analysis or dissemination of information, is certainly an essential part of America's overall effort to combat terrorism. However, those who believe that intelligence alone can stop terrorism, fail to recognize the nature and scope of the overall threat. Such a one-dimensional approach suggests a fundamental lack of understanding of what an effective counterterrorism strategy should entail: a combination of intelligence, diplomacy, law enforcement, disaster response and recovery, military force and covert operations, acting in concert to safeguard our nation.

¹ Pubic Law 107-306, November 27, 2002.

² The 9/11 Commission Report, Authorized Edition, (W.W. Norton & Company, 2004), p. xvi.

Counterterrorism is unique in the public policy world, because it demands seamless interaction between federal, state and local governments. This level of intergovernmental collaboration requires the skillful coordination of personnel from different agencies, each with their own bureaucratic culture and areas of expertise. As James Wilson has noted, two methods that agencies often use to bolster their position against rivals are to "fight organizations that seek to perform [similar] tasks" and to "be wary of joint or cooperative ventures."³ Effective counterterrorism requires law enforcement and intelligence agencies with similar missions and overlapping jurisdictions to work as partners, not adversaries. If left unchecked and unmanaged by a neutral third party, long-standing agency rivalries can intensify and stymie the best counterterrorism efforts.




Clearly, a coordinated and considered approach to fighting terrorism means that the government must do more than claim that "the walls are down." Instead of rhetoric, the government must designate and empower an organization that has control of the national counterterrorism budget; provides guidance to the president; develops integrated policies and ensures that those policies are properly executed. Of course that begs the question, what government

entity should manage and coordinate the complex, and increasingly expensive, U.S. counterterrorism apparatus? As the danger posed by international terrorism has intensified over the last 30 years, U.S. presidents have increasingly turned to the National Security Council (NSC) to answer that question.

BACKGROUND

Throughout most of its history, the NSC and its staff developed and coordinated long-term national defense strategies, such as the containment of the Soviet Union; and tackled Cold War emergencies, such as the Cuban Missile Crisis. But managing counterterrorism policy is markedly different from those traditional roles, and

³ James Q. Wilson, *Bureaucracy*, (Perseus Books, 2000), p. 189-192.



probably not what Congress had intended when it created the NSC in 1947. That said, the NSC has undergone tremendous changes throughout its 60-year history, and presidents have molded the organization to fit the needs of the time, as well as their own personalities.

In the aftermath of the Iran-Contra scandal, in which an NSC staff member responsible for counterterrorism policy actually sold weapons to one of the biggest contributors of state-sponsored terrorism, President Ronald Reagan convened the President's Special Review Board (commonly referred to as the Tower Commission),⁴ to review and report on what went wrong at the NSC. Among its conclusions, the Tower Commission determined that the NSC and its staff should not conduct operations;⁵ that the NSC staff should be comprised of experienced policy makers, drawn from inside and outside the government;⁶ that the NSC staff lacked institutional knowledge;⁷ and that the intelligence process must be kept separate from policy advocacy.⁸

In 1992, President Bill Clinton's incoming national

“Throughout most of its history, the NSC and its staff developed and coordinated long-term national defense strategies, such as the containment of the Soviet Union; and tackled Cold War emergencies, such as the Cuban Missile Crisis.”

security advisor, Tony Lake, asked Richard Clarke, who was President George H.W. Bush's Assistant Secretary of State for Politico-Military Affairs, to join the NSC and assist with post-Cold War issues. Eventually, Clarke's responsibilities focused on transnational threats, to include international terrorism. Clinton and Lake organized the NSC into three levels: the statutory NSC, comprised of the relevant cabinet members; the Principals Committee,

⁴ The Tower Commission Report, (Bantam Books/Times Books, 1987).

⁵ Ibid, p. 92.

⁶ Ibid, p. 92.

⁷ Ibid, p. 92.

⁸ Ibid, p. 97.

where meetings were chaired by the national security advisor and attended by cabinet representatives; and the Deputies Committee, where the deputy national security advisor chaired meetings which were attended by deputy agency heads.

Below these three levels were interdepartmental working groups (IWG's), each chaired by a senior NSC staff director. One of the IWG's was the Counterterrorism Security Group (CSG), chaired by Clarke and a version of earlier counterterrorism working groups that dated back to the Reagan administration. The CSG membership was comprised of leaders from federal agencies responsible for counterterrorism. Clinton, building on systems started by President Reagan, used the CSG to coordinate all of the administration's counterterrorism efforts, whether they concerned domestic issues or foreign affairs. In May 1998, President Clinton further strengthened the relationship between the principals and the CSG director with a new presidential directive, PDD 62.⁹ That directive elevated the CSG director's role, and established the office

of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism within the NSC. Promoting Richard Clarke to the national coordinator position, President Clinton authorized him to provide advice regarding budgets for counterterrorism programs; to coordinate the development of crisis management plans; and to report to the president through the national security advisor. Despite some inherent weaknesses, Clinton's CSG system had some notable successes, both

with incident response¹⁰ and preemption.¹¹

⁹ White House Press Release regarding President Decision Directive 62, Issued on May 22, 1998

¹⁰ The CSG quickly and effectively responded to the 1998 bombings of the U.S. embassies in Kenya and Tanzania, coordinating the recovery and response with relevant federal agencies. See: Richard Clarke, *Against All Enemies*, (Simon & Shuster, 2004), p. 181-188

¹¹ In late 1999, U.S. law enforcement and intelligence agencies learned of a variety of plots aimed against the U.S. and its allies and timed to coincide with the new century. These plans, which were thwarted, came to be known as the Millennium Plot, and the CSG played a significant role in coordinating the successful efforts to stop them. See: *The 9/11 Commission Report, Authorized Edition*, (W.W. Norton & Company, 2004), p. 179-180

ALTERNATIVES

Consideration of the NSC's performance in counterterrorism management during the last 30 years suggests three possible alternatives to address the coordination problem identified by the 9/11 Commission: (1) President George W. Bush's approach, which relies upon both the NSC and a Homeland Security Council (HSC); (2) a separate executive branch agency, independent of the White House; and (3) an improved version of the CSG, which would reside within the NSC.

HSC/NSC/ODNI Model

In the current Bush administration, responsibility for counterterrorism coordination is bifurcated between the HSC and NSC. Established in the aftermath of the 9/11 attacks, and similar to the NSC in many respects, the HSC is led by a homeland security advisor who directs a staff of thirty-five people.¹² The HSC's official website states that its mission is "to reduce the potential for terrorist attacks and other threats, and to mitigate damage should an incident occur." In addition to the HSC and NSC, President Bush uses the Office of the Director of National Intelligence (ODNI) to assist with the coordination of counterterrorism policy. The ODNI, which was established as the result of a recommendation from the 9/11 Commission, is led by the Director of National Intelligence (DNI), who serves as the principal intelligence advisor to the president and oversees the nation's intelligence community. Created by the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), the DNI has significant statutory power, including, but not limited to: budgetary authority,¹³

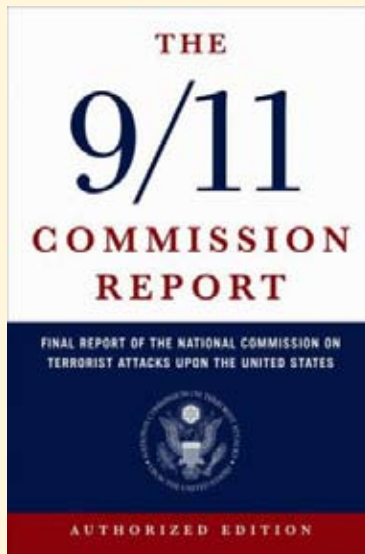
reprogramming authority,¹⁴ and tasking authority,¹⁵ over the intelligence community; and control of the National Counterterrorism Center (NCTC).

Independent CTA Model

A second alternative is to transfer coordinating responsibility out of the West Wing altogether and empower an independent executive branch agency to manage the counterterrorism community, not unlike the ODNI's aforementioned role in the intelligence community. Using the ODNI as a model, the U.S. Counterterrorism Agency (CTA), would not actually conduct counterterrorism operations or investigations. Instead, the CTA would be responsible for determining funding levels for the national counterterrorism budget; developing the nation's overall counterterrorism policy; coordinating the efforts of agencies with related responsibilities and tasking them with specific requirements. The CTA staff would be comprised of career civil servants, and since the focus of the CTA would be oversight, budgetary matters, policy planning and management, its staff would be relatively small in comparison to other agencies.

Improved CSG Model

A third option would be an enhanced CSG, which would improve upon the model used during the Clinton administration. Clinton's approach had two fundamental flaws, which must be corrected if the new version is to succeed. The first defect was the fact that the CSG and the national counterterrorism coordinator position were created by presidential directive, not statute. Clarke was able to wield power, in large part, because of his personality and relationship with President Clinton, not because of any authority inherent to his position. This lack of statutory authority for the CSG model could become



¹² www.whitehouse.gov/hsc.

¹³ The Director of the OMB, at the direction of the DNI, will apportion or direct how congressionally funds will flow from the Treasury Department to each of the cabinet level agencies containing intelligence community elements. Source: Richard A. Best, Jr., Alfred Cumming, and Todd Masse, "Director of National Intelligence: Statutory Authorities," Congressional Research Service Report, No. RS22112, April 11, 2005.

¹⁴ With OMB approval, the DNI has the authority to reprogram or transfer up to \$150 million in funds annually. Source: Ibid.

¹⁵ The DNI has the power to manage and direct the tasking of collection, analysis, production and dissemination of intelligence. Source: Ibid.



The National Counterterrorism Center (NCTC)

an issue as presidential administrations and West Wing relationships change. The second major problem with the Clinton model is that the CSG only had review authority over the nation's counterterrorism budget. This limited authority put Clarke and the CSG in the uncomfortable position of having to argue with cabinet members about how much counterterrorism money needed to be in their overall budget request, and fighting with the OMB about increasing counterterrorism spending.¹⁶ Both of these problems can be corrected by having Congress statutorily establish the position of National Coordinator for Counterterrorism and a Counterterrorism Security Group within the NSC. This would provide the CSG with budgetary authority; a civil service staff and operating budget, separate from the rest of the NSC; and the authority to engage in limited operations, related to antiterrorism preparedness, incident response and crisis management, but not active investigations or covert operations.

The CSG's staff would have to be large enough to properly address its new and increased responsibilities, but not so large that the CSG would become yet another cumbersome bureaucracy, losing its ability to dynamically respond to changing circumstances and emerging threats.

The 9/11 Commission noted that although the staffs at the NSC and HSC have grown 50% larger since the September 11th attacks, they are still consumed by day-to-day meetings that take them away from their responsibilities.¹⁷ Based on that fact, the CSG staff would have to be greatly increased beyond the 12 staff members from the Clinton years, and even the 35 members currently in the HSC.


In order to select the best of the three aforementioned options, it is instructive to apply a set of criteria that can provide a sound basis to analyze their likelihood of success and overall effectiveness. Three evaluative criteria that would prove useful are: "communication and information flow," "policy integration," and, "professionalism." A fourth, and practical criterion, is "political acceptability."

The first criterion, "communication and information flow," goes to the heart of many public policy initiatives, and it is vital in the area of counterterrorism. This criterion concerns: (1) whether policy and operational instructions from the president are fully communicated to cabinet members, agency heads, and federal employees; (2) whether information is adequately shared between federal, state and local agencies; and, (3) whether the president is fully briefed, in a timely manner, on all pertinent viewpoints within the cabinet and provided with all relevant information, while simultaneously managing the information flow to prevent information overload or erroneous facts from clouding the president's judgment and decision-making.

The second criterion is "policy integration." This criterion looks at the ability to fully combine the various aspects of counterterrorism: intelligence, law enforcement, diplomacy, military force, incident response, transportation security and infrastructure protection, into a unified and coherent overall strategy that addresses all contingencies.

¹⁶ Richard Clarke, *Against All Enemies*, (Simon & Shuster, 2004), p. 128.

¹⁷ The 9/11 Commission Report, Authorized Edition, (W.W. Norton & Company, 2004), p. 402.



“Professionalism” is the third criterion, and it refers to the professionalism of the staff engaged in counterterrorism policy coordination: their level of expertise; their ability to provide unbiased and impartial advice, guidance and oversight to both politicians and bureaucrats; and their insulation from political pressure and potential abuse.

The fourth criterion concerns whether the given alternative is “politically acceptable.” The basic questions here are: (1) Would the president accept the option? (2) How would the federal bureaucracy react to the alternative? (3) Would the Congress agree with and support the decision?

“Timeliness is essential in the successful implementation of any public policy, and that maxim is especially true in matters of counterterrorism.”

The Bush administration’s system is arguably limited by its bifurcation. At a time when the integration of foreign and domestic counterterrorism policy should improve and the flow of communication should be unrestricted, the HSC/NSC model is a step backwards.

This fact was clearly recognized by the 9/11 Commission when it stated that “the existing Homeland Security Council should soon be merged into a single National Security Council.”¹⁸ It is unlikely that future presidents would view the HSC as a politically viable and effective means of coordinating counterterrorism policy. Instead, they would probably seek a system closer to that employed by President Clinton.

Although an independent CTA would likely have a professional staff which could effectively integrate policy, and is a better alternative than the HSC in many respects, it too has potential problems. For example, in the event of a crisis, the CTA director would arguably not have the type of access to the president and the national security advisor that a CSG director would have actually working in the West Wing. Furthermore, it is highly unlikely that the idea of a CTA would find much support

in the counterterrorism community. The intelligence community has had a coordinator, at least in theory, since 1947.

The same cannot be said of the counterterrorism community, which is comprised of disparate agencies, some of which have a long history of bureaucratic turf wars with one another. Many agencies would regard the CTA with a great deal of suspicion, even if it did not have an operational role. And the CTA certainly would have difficulty being trusted as a neutral third party in interagency disputes.

Analysis of the third alternative suggests that an improved version of the CSG would be the best option for improving coordination of the nation’s counterterrorism policy and the one which should be put into practice. By strengthening the CSG and placing it back in the NSC, the flow of information would be greatly improved.

The president would have his counterterrorism advisor in the West Wing and would be able to clearly dictate his policy preferences to the CSG for integration and dissemination to cabinet members and the bureaucracy. Theoretically, the CSG director would have more credibility than a CTA director in settling turf battles, because the CSG would pose less of a jurisdictional threat to the federal bureaucracy, and this might make an improved CSG more politically acceptable than the other options.

Although its placement in the NSC prevents total insulation from political pressure, staffing most of the CSG with career civil servants would afford as much protection as is possible in an office inside of the White House. Staff members would have job security and the time to develop subject matter expertise in one or more disciplines. By also staffing the CSG with individuals temporarily detailed from federal agencies, think tanks and academia, the CSG’s permanent staff would be exposed to different viewpoints and learn how policy decisions worked when they were introduced in the field.

¹⁸ The 9/11 Commission Report, Authorized Edition, (W.W. Norton & Company, 2004), p. 406.

Such an approach would provide the president, and the greater NSC, with a CSG staff combining institutional knowledge, pragmatism, fresh perspective and innovation, all of which would be a great asset in counterterrorism coordination. This level of professionalism would provide the president with sound and reasonable advice on which to base long-term policy decisions and manage crisis situations. Finally, if the staff was comprised of civil servants and not political appointees, there would be a greater chance that Congress would view the CSG's recommendations as non-partisan.

IMPLEMENTATION

Timeliness is essential in the successful implementation of any public policy, and that maxim is especially true in matters of counterterrorism.

However, it would be senseless to hastily create yet another organization in the country's national security system without careful study and consideration. The first step in implementing the new-CSG would be an extensive review of the systems used in the Carter, Reagan, George H.W. Bush, Clinton and George W. Bush administrations, with a careful examination of their successes and failures.

The second step would entail meeting with the Cabinet secretaries and agency heads from departments that would be impacted by the creation of the new-CSG and fall under its jurisdiction.

Finally, in order for the new-CSG to be successful, it must have the support of Congress, which would require consultation with the congressional leadership and those committees which would have oversight and budgetary authority in the counterterrorism realm.

CONCLUSION

The battle against international terrorism will be a long struggle. In a free, open and democratic society such as ours, it is nearly impossible to ensure that a terrorist incident

will never happen. That said, there are steps that the U.S. government can take to stop terrorists before they strike, lessen the chance that their attacks will succeed, and if a tragedy does occur, contain the damage, care for the injured and respond in kind. One of the ways to do that is to take advantage of the distinct parts of the U.S. government that are needed to combat terrorism.

By pooling resources, integrating policy and developing long-term strategies, the government can truly make the nation safer, and get beyond political rhetoric. That coordination must happen somewhere and the most logical place for it is in an improved and strengthened Counterterrorism Security Group, residing inside the White House, and part of the National Security Council.

Americans have good reason to be proud of the nation's military, our first responders, the FBI, the CIA and other partner agencies in the counterterrorism community.

But the inherent strengths of those organizations are meaningless if no one is coordinating their efforts and acting as a force multiplier.

By improving on the CSG model, the U.S. government will be one step closer to answering the 9/11 Commission's call for action and protecting our nation.*



DCIS

BIOGRAPHY

LEIGH-ALISTAIR BARZEY
DEFENSE CRIMINAL
INVESTIGATIVE SERVICE
DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL



Leigh-Alistair Barzey is a special agent in the Northeast Field Office of the Defense Criminal Investigative Service (DCIS), U.S. Department of Defense. Since March 2004, Special Agent Barzey has been assigned as the DCIS representative on the Federal Bureau of Investigation's Joint Terrorism Task Force in Boston, Massachusetts.



DCIS special agents assist in recovery efforts at the Pentagon subsequent to the terrorist attacks of September 11th, 2001.

Prior to joining DCIS in December 2001, Special Agent Barzey was a special agent with the U.S. Department of Labor's Office of Labor Racketeering and Fraud Investigations, where he was assigned to the New York Field Office. Special Agent Barzey has also served as an investigator with the U.S. Department of Labor's Office of Labor-Management Standards. Before joining the federal government, Special Agent Barzey was an assistant district attorney in the Bronx County District Attorney's Office, in New York City.

In May 2007, Special Agent Barzey graduated from Georgetown University and received a Master's Degree in Public Policy Management. Special Agent Barzey is also a graduate of Vermont Law School, from which he holds a Juris Doctor degree that was awarded in May 1997, and the New School for Social Research, from which he received a Bachelor of Arts degree in May 1994.



DCIS special agents work with the FBI's Joint Terrorism Task Force.

A hand is shown typing on a computer keyboard. The background features a world map with glowing white outlines of continents, overlaid on a red and white grid pattern. The overall color scheme is dominated by reds and oranges, with a dark red diagonal band across the lower half of the image.

8 DEVELOPING A HOTLINE FOR THE 21ST CENTURY

BY JOSEPH VALLOWE AND CHRISTINA LAVINE
DEPARTMENT OF VETERANS AFFIARS
OFFICE OF INSPECTOR GENERAL

The U. S. Department of Veterans Affairs (VA) provides a wide range of benefits programs aimed at improving the quality of life of 25 million veterans and their families. These benefits include full health care services, as well as compensation, pension, insurance, transition, education, rehabilitation, and memorial benefits that are available to eligible veterans. With approximately 230,000 employees and thousands of facilities and sites of care throughout the Nation and abroad, VA is the second largest civilian agency of the Federal government. It buys more pharmaceuticals than any organization on Earth and contracts for goods and services with thousands of companies and individuals. Over the past three fiscal years (FY) 2005–2007, the VA Office of Inspector General (OIG) has received over 50,000 complaints from veterans, family members, employees, and others who have concerns about VA or veterans issues.



Although the Hotline began operation before the passage of the Inspector General Act of 1978, it employed the same labor-intensive manual processes for the first two decades of its existence. Over the past decade, however, introduction of new workflow techniques, enhanced staff, and electronic technology increased efficiency and impact to a point where this Hotline can serve as a model for modernizing other Hotline operations. This article highlights the key in transforming the Hotline into a 21st Century operation.

BEGINNINGS

The early days of the Hotline have receded into the mists of retirements and other happy endings, but some clues remain. Initially created administratively on January 1, 1978, the OIG established the Hotline in early 1978 with a couple of experienced investigators and auditors. Telephone calls to a toll-free number were automatically forwarded to a voice mail system 24 hours a day, 7 days a week. The staff listened to the calls during regular business hours and determined whether complaints warranted further action. Complaints that were within OIG purview became Hotline cases that were tracked manually in an index card and paper index system by

complainant, subject facility, and subject. The system remained essentially the same into the mid-1990s, although the investigator/auditor staff had been replaced by program analysts.

The voice mail system presented challenges as an effective complaint screening method. Its unlimited capacity allowed a lonely or mentally troubled individual with access to a telephone to speak as long as his or her voice could continue. On Monday mornings, staff had to listen to hours of often-filibuster length calls to determine whether a valid complaint was buried within each message. Other calls might be right on point but with no possibility of follow through by OIG, such as the caller who hung up after stating, “Somebody staff members are stealing narcotics from the hospital.” What staff, what drugs, which hospital? The system had no caller ID feature to allow a call back on this potentially meritorious complaint. Even if the complaint was sufficiently specific, meritorious, and provided contact information, Hotline staff had to call back the complainant to obtain release of identity, additional details, and other information. At minimum, one call to the Hotline led to at least one call back. There was no relief from regulars who repeatedly raised the same issue, regardless of whether it involved an OIG issue or not.

WORKFLOW CHANGES

Following an internal audit of the Hotline that included a review of best practices in other Hotlines; OIG made some

fundamental workflow changes in the late 1990s. The most significant was the commitment to live telephone answering. Live answering allowed staff to focus the caller quickly on an issue and determine within a short time whether the complaint involved specific fraud, waste, or mismanagement in VA programs and operations. The telephone system implemented provided recorded information after business hours that informed callers when live operators were available, pertinent information concerning what to include in a complaint and how to mail or fax documents to the Hotline, but, significantly, did not contain a voice mailbox. This system put an end to the days of “playing back the tapes” and sifting through monologues and diatribes.

A second key workflow change empowered Hotline staff with “cradle-to-grave” responsibilities for handling a complaint from start to finish. In the past, some Hotline staff simply took complaints and logged them in for other staff to work into cases that were referred to other OIG components or to VA program offices. Still other staff members were assigned to follow up to determine the results of case referrals to the VA program office or the OIG investigative, audit, or inspections offices. By attaching a staff member to a complaint throughout the full complaint life cycle, the Hotline staff became accountable for seeing the matter through to resolution. This change also decreased burnout of the few staff who took in complaints from often difficult individuals by rotating all staff onto the phones or opening mail.

Live call answering and cradle-to-grave complaint handling continue today as essential features of the Hotline and dovetail into the area of staff development needed to make both features work effectively.

STAFF ENHANCEMENTS

The evolution of the Hotline included a restructuring of staff positions from lower graded intake clerks to career-ladder/journeyman level GS-13 program analysts, emphasizing the abilities of the staff to apply analytical skills to complaints received. Under the cradle-to-grave approach, each analyst needed the skills to develop sufficient information to determine whether the complaint raised

issues within the purview of the OIG, that is, whether it raised issues of fraud, waste, abuse, mismanagement, or criminal activity in VA programs and operations. If the complaint was within OIG purview, the analyst had to develop sufficient preliminary facts to determine whether the complaint was sufficiently timely, specific, and serious to open an OIG case, and if so, whether to recommend referring that case internally to an OIG component for investigation, audit, or inspection, or whether to make an external referral to a VA program office for review and response. Cases then required analyst follow-up to ensure responses were received timely, whether all issues were addressed, and in the case of external referrals, whether the reviewer was sufficiently independent in position and approach to conduct a competent review.

The establishment of a career track within Hotline commensurate with the same grade-level career track in the other OIG components also improved morale and increased staff retention by eliminating the stigma that Hotline staff members were “second-class citizens” compared to their colleague investigators, auditors, and inspectors. The current staff of seven—a director, deputy director and 5 analysts—has an average time in Hotline of 7 years, which shows that this career track has worked to keep high-performing staff within the Hotline. Current Hotline managers are “home-grown” from the analyst ranks.

To ensure the staff possessed the skills and tools to perform successfully, training expanded to include basic interview techniques, dedicated training on dealing with angry and abusive callers, and in-service training by investigators and inspectors on mission-specific issues, such as veterans benefits eligibility and claims processing, health care eligibility and services, and procurement issues. The staff also took courses to improve writing skills. Weekly staff meetings allowed staff not only to share best practices and new case issues, but it also provided opportunities for bonding and perhaps even a little venting over some of the most difficult contacts.

Supervisors developed standard procedures and resources in a consolidated desktop manual for easy reference and increased efficiency. Included in this manual were specific

names and direct phone numbers for patient representatives at every VA facility, contact information for heads of all VA facilities, and an extensive listing of common referral phone numbers and addresses for non-OIG issues, such as the Department of Defense office that replaces missing military medals, state veterans affairs service offices, and suicide prevention Hotlines. An example of a standard process resource aid developed to further consistent evaluation of complaints appears in Diagram 1, Hotline Analyst Decision Process for Handling Complaints.



The Hotline team also developed an abusive caller protocol in which repeated, abusive callers were documented, warned, and then, after given fair opportunity to act acceptably, cut off the line so that analysts could assist other callers. This protocol not only recovered wasted time and effort from unproductive encounters, but also encouraged the staff on the front line with complainants. The analysts expressed appreciation that management was concerned about protecting them and helping them do their jobs. Other VA staff offices learned about the protocol and substantially adopted it for their own use; one employee commented that she thought “VA could never, under any circumstances, hang up on a veteran, but in these rare abusive circumstances, it was entirely appropriate.”

As an example of how a seemingly small change can reap big benefits, Hotline staff were allowed to select their own shifts answering the phone. Some individuals preferred to do calls all day for a full week, with the following week spent on mail and casework, whereas other individuals preferred staggering their phone shifts every other day or

on half-days. So long as each staff member worked their fair share of shifts, he or she could make his or her own schedule. This practice increased teamwork and morale by empowering the staff.

Finally, staff were given new performance standards which reflected the relative importance and reasonable expectations of the time required to complete the discrete phases of the complaint and case-handling life cycle. All of these enhancements improved the quality and results of the human element of the Hotline. The cradle-to-grave process instilled a pride of ownership in successfully resolving complaints and established a mechanism for holding employees accountable for performance.

TECHNOLOGY TOOLS

In conjunction with workflow process changes and enhancing the staff capabilities, Hotline adopted a series of technological improvements that moved the unit from essentially pen and paper to electronic recordkeeping. They replaced manual contact logs with an Excel worksheet to electronically track contacts and allow for electronic searching and sorting. OIG also implemented an enterprise architecture known as the Master Case Index (MCI) that centralized all OIG work in a central database. Through search engines, OIG staff could determine whether OIG had received, was working on, or had already worked a particular issue. For example, if an investigator is approached at a VA facility by a complainant with an issue of poor quality health care provided to a particular patient or a theft of Government property, that investigator can search from his or her computer by the complaint’s name, facility, or nature of complaint to determine whether this complaint had already been made to the Hotline or another OIG component, and if so, how it had been addressed. Assuming in this example that the investigator opened a criminal case, an MCI search would also reveal if the persistent complainant later contacted another OIG employee that this investigator was already working the complainant’s issue. Under OIG policy, if the investigator did not open an investigation, he would be required to provide the contact information to Hotline to log into MCI for a record of the contact. MCI provided a way to ensure OIG’s limited resources were not spent on duplicating work and to ensure that OIG responded consistently on the same and similar issues. OIG has

shared the software for the Hotline contact log with other staff offices within VA headquarters for their use in tracking callers, who tend to engage in “forum-shopping” in search of someone who will satisfy their requests.

The MCI system also allowed OIG staff to identify related work, such as multiple criminal investigations that arose from the same incident, the same complaint, or involving the same subject. Related work in different offices, whether separate field locations within the same office, or across different components, could also be connected through cross-referencing in the MCI system to relate common issues for future searching. For example, a single Hotline complaint may give rise to multiple criminal and administrative investigations against multiple subjects, a program audit, and a health care inspection. By establishing a root MCI case number for the matter, the system allowed later activities to “tail off” the original number in a way that searches would capture all related work. Although the overwhelming majority of complaints to the Hotline come from veterans, family members and other advocates for veterans, such as veterans service organizations, Hotline also receives complaints referred by public officials and other agencies. MCI allows searches by individual names and in specialized fields for referrals from the White House, Members of Congress, the Office of Special Counsel, and the Government Accountability Office.

“The Hotline team also developed an abusive caller protocol in which repeated, abusive callers were documented, warned, and then after given fair opportunity to act acceptably, cut off the line so that analysts could assist other callers.”

Related to Hotline specifically, this database allows Hotline staff to determine quickly without leaving their desks whether the caller on the line with them has previously contacted the OIG, and if so, what action OIG has taken. MCI also uses drop-down pick-lists of common categories to save time and ensure uniform data entry and searching. The system also allows for preparation of standard and customized reports of activity for trend analysis, progress reporting, performance measurement, and preparation of the Semiannual Report to Congress.

The Automatic Call Distribution (ACD) telephone system assists in workload distribution, and in combination with MCI and work processing, saves time and minimizes errors in opening cases. It routes incoming calls to the next available analyst, allows supervisors to monitor calls for quality control and to intervene in problem calls, allows recording and digital filing of calls that need to be saved, such as a threat of violence, and provides statistical reports to assess unit and individual analyst performance. For example, supervisors can monitor whether there is a run of calls that requires adding more staff to the phones. The system also allows special messages for emergencies, such as when a Washington, DC, snowstorm prevents staff from getting to work—the supervisor can remotely activate the “business closed” response that callers receive. The automated menus can also be reprogrammed when special issues arise that may generate a large volume of calls, such as media reports of problems.

As part of the standardization process, Hotline developed word processing templates to ensure that required boilerplate elements are included but with the flexibility to adapt these templates to the particular case. The interface of the ACD and MCI system allows certain information, such as incoming caller ID, and the initial contact information including name, address, telephone, facility, and synopsis of issues, to be imported from the Hotline contact log directly into MCI and the word processing templates.

This capability minimizes rekeying and reduces errors as well as saving time in opening cases.

Hotline also uses the Web, e-mail, and fax communications to allow for communication with OIG beyond traditional mail and telephone. Fax and e-mail communications proved indispensable when the Washington, DC, anthrax attacks created new obstacles to direct mail delivery. The Hotline Webpage: www.va.gov/oig, allows dissemination of information of what the Hotline can and cannot do with issues and provides helpful tips as to what information should be included in complaints. As the Information Age expands, Hotline has seen an increase of e-mail and faxed communication along with a decline of paper mail. Hotline uses an automatically-generated response to

all e-mails indicating what the complainant can expect in response to the incoming message. Hotline has also migrated from paper resource manuals to online sources.

The latest step in the evolution of technological improvements is paperless case files. All cases have electronic copies of contact logs, e-mails, word processing documents, and scanned versions of hard copies. The paperless files eliminate the steps of creating, copying, and filing hard files, as well as the problem of searching for misplaced files. These files also allow the Hotline staff to leverage other technology by simply clicking and dragging information that is already in electronic form, such as e-mail or MCI information, into the files. The freed storage space has allowed Hotline to convert its file room into a staff office.

Looking towards the future, Hotline is exploring the possibility of adding live Web-chat capability as another method of communication that will allow real-time communication over the Web with complainants while the analyst can be on the phone seeking information for the caller.

As the result of the technology tools available, if necessary, a typical call to the Hotline can be turned into a completed case referral package that is reviewed and transmitted to the OIG office or VA program office for review within an hour.

RESULTS

The present day OIG Hotline has increased its substantiation rate from 21 percent in FY 1998 to 37 percent for FY 2007 for cases containing at least one sustained allegation. Hotline referred 44 percent of these cases to internal OIG components while referring the remaining 56 percent as external cases to VA. During FYs 2005–2007, Hotline processed 51,257 complaints, converting all into electronic form, and opened 3,274 cases and closed 3,248 cases. Monetary impact from Hotline cases alone during the past 3 years

totaled almost \$3.8 million, with over 800 corrective actions implemented. The increase in substantiated cases and the high percentage of internal referrals demonstrates the value of employing better trained analysts rather than lower-graded intake personnel, and of utilizing the cradle-to-grave case management approach to identify higher quality cases and more efficiently refer legitimate complaints.

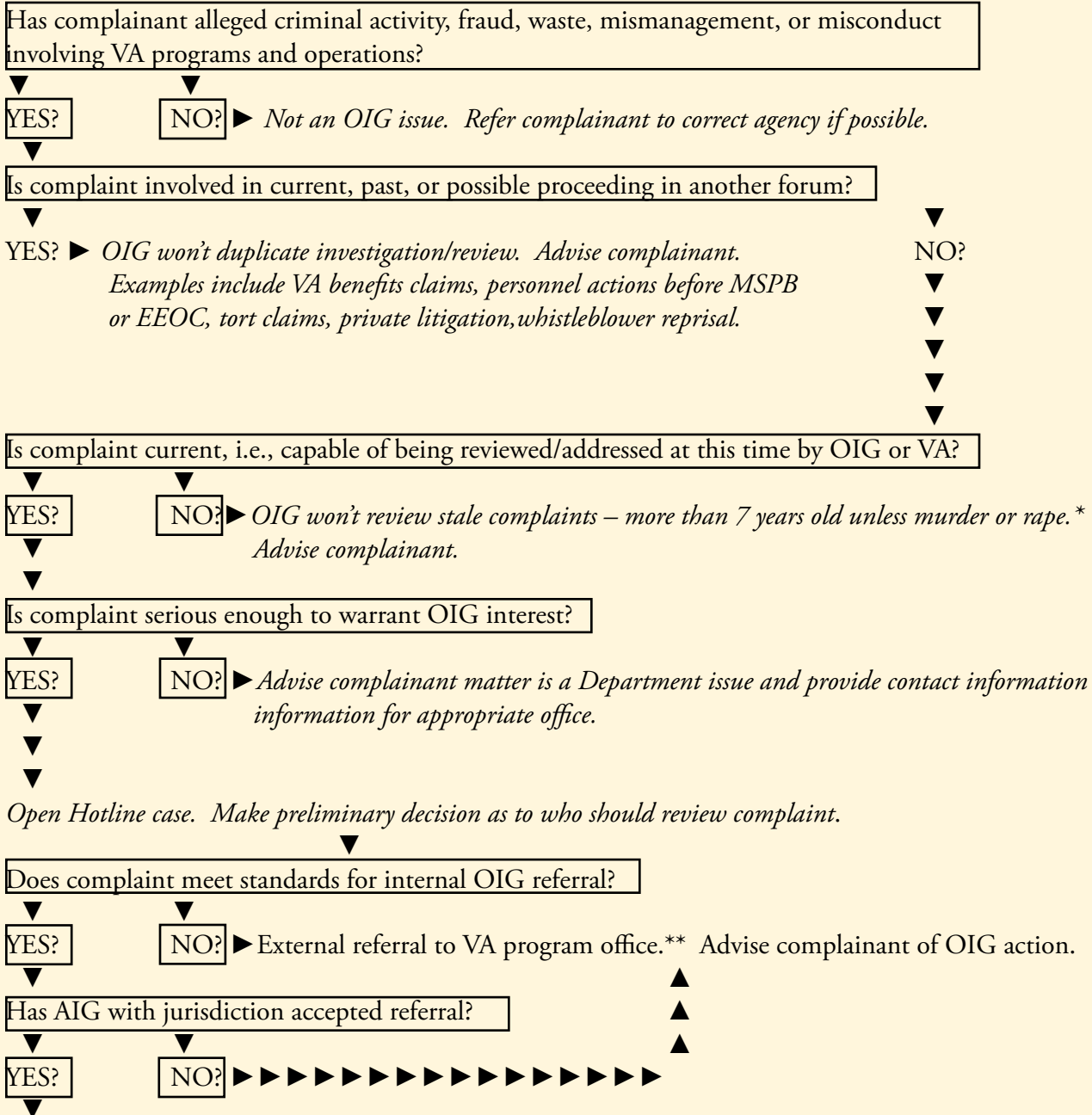
The Hotline has received two PCIE peer recognition awards, and has provided tours and procedural overviews for several congressional and other visitors.

By adopting workflow changes, staff enhancements, and technology tools, the Hotline evolved within the past decade from an archaic, manual office to a streamlined, automated operation with subject matter expertise to quickly sift the wheat from the chaff of voluminous contacts to ensure that meritorious complaints are addressed expeditiously and appropriately. Continued support and encouragement by senior OIG management will provide Hotline the means to explore the feasibility to one day implement a Web-chat feature, enhancing the Hotline's 21st Century operations. In this way, the Hotline continues to perform a critical Inspector General function and contributes to improved activities and services to our Nation's veterans.*



DIAGRAM 1

HOTLINE ANALYST DECISION PROCESS FOR HANDLING COMPLAINTS



*Initiate case referral to Investigations if criminal activity alleged.
 Initiate case referral to Audit if systemic problems with VA programs alleged.
 Initiate case referral to Healthcare Inspections if serious patient care/abuse or systemic health care issue alleged. Regardless of which office(s) involved, advise complainant of Hotline case.*

*Since staleness is relative to the type of complaint and applicable legal statutes of limitations, see Hotline supervisor before dismissing something less than 7 years old as stale.

**If program office management is complainant, see Hotline supervisor before referral.



BIOGRAPHIES



JOSEPH M. VALLOWE
DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Joseph Vallowe is the Deputy Assistant Inspector General (AIG) for Management and Administration for the Department of Veterans Affairs (VA) Office of Inspector General (OIG). He entered the Senior Executive Service in 2004. In his 13 years with the VA OIG, Mr. Vallowe has also served as Acting Deputy AIG for Auditing, Director of the Operational Support Division, Director of the OIG Hotline, and senior staff attorney in the Office of Counselor to the IG. These positions have provided broad and detailed experience in both programmatic and support activities of the Office of Inspector General.

Mr. Vallowe began his federal career as an attorney with the VA Office of General Counsel in 1990. He served as an ethics official, personnel and labor law litigator, and police and security advisor. He joined the Government after practicing civil litigation as a partner in a 70-attorney law firm in Chicago, Williams and Montgomery, Ltd. Mr. Vallowe is a graduate of Loyola University of Chicago with an honors degree in Philosophy and earned a Juris Doctor degree from Northwestern University School of Law in Chicago. He grew up in Belleville, Illinois, a suburb of St. Louis.

CHRISTINA A. LAVINE
DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Christina Lavine is the Director of the Department of Veterans Affairs (VA) Office of Inspector General (OIG), Hotline Division.

Christina began her career with the VA in 1976. She has worked in progressively responsible administrative positions at the VA Medical Center Miami, Florida; the VA Outpatient Clinic, Orlando, Florida; and the VA Medical Center, West Palm Beach, Florida. She transferred to the VA OIG from West Palm Beach in 1998. At that time she accepted a position as a Hotline Analyst and over the past 10 years has progressed to Senior Hotline Analyst, Deputy Director, and in August 2004, she was selected as the Director of the Hotline.

Christina began her Federal career as a Secretary with the United States Coast Guard, Miami, FL, in 1974. She has also worked as a Senior Probation Analyst with the United States Probation Office.



9 IG OUTREACH TO EASTERN EUROPE, THE BALKANS, AND EURASIA

BY COLONEL MIKE ANDERSON
U.S. EUROPEAN COMMAND INSPECTOR GENERAL

“The IG experiences of other nations are precious to us,” offered MG Dragan Milosavljevic, the Chief of Staff of the Armed Forces of Montenegro, Europe’s newest state.

“If nations who are gathered here return home and spread these good practices, we will be creating a positive revolution for good governance and anti-corruption, quite literally around the world,” stated MG Sardar Mohammad Abulfazel, a former Mujahideen and the present IG for the Afghan National Army (ANA).

These were the concluding, laudatory remarks of two of the more than 60 senior representatives from 18 nations who gathered recently at the George C. Marshall Center for Security Studies in Garmisch-Partenkirchen, Germany, 5-7 September 2007. Inspectors General from Kabul to Kiev, from Armenia to Albania, and from Mongolia to Macedonia participated in this first-ever conference, initiated and organized by the US European Command (EUCOM) IG office.



Col. Anderson, US co-chair, opening the IG Conference with Brig. Gen. Naskrent, the German co-chair (right) and Gen. Ward, EUCOM Deputy Commander (left). Lt. Gen. Green, Army IG, is in the foreground.

EUCOM, a Geographic Combatant Command, is responsible for an Area of Responsibility (AOR) comprising 92 nations, nearly half of the nations represented in the UN General Assembly. This conference focused on European and Eurasian states with an interest in either improving or establishing an IG or Ombudsman-type system for their militaries.

All of the Balkan nations were represented (western Balkans; Croatia, Bosnia-Herzegovina, Albania, Macedonia, Montenegro and Serbia, as well as the eastern Balkans; Romania and Bulgaria). From the shores of the Black Sea, Ukraine and Moldova also participated, as did the 3 South Caucasus states of Armenia, Georgia and Azerbaijan. Although not in the EUCOM AOR, Mongolia and Afghanistan also took part and were especially appreciative of the ideas and best practices exchanged.

MODELS; ATTRACTIVE BUT NOT GLAMOROUS

Four different models for providing IG and Ombudsman support to militaries were presented at the seminar as examples for participating nations to study and consider. The French, Bosnia-Herzegovinan, German, and American IG military models were shared. Each offers means for dealing with corruption, combating fraud and

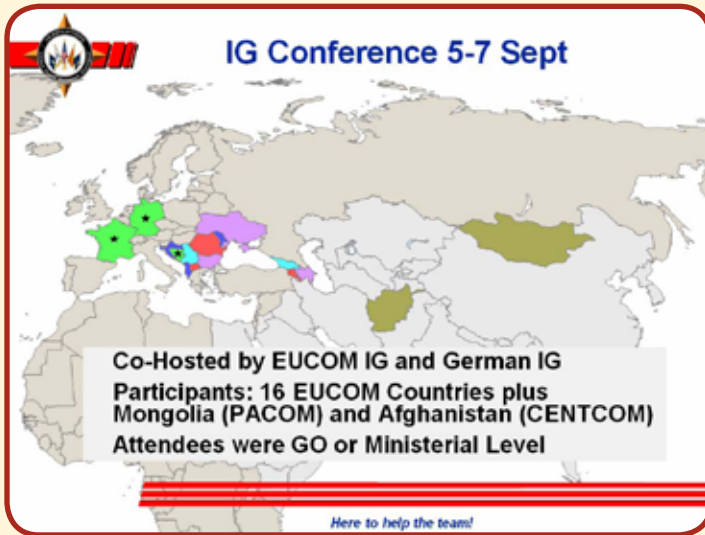


GERMAN/AMERICAN PARTNERSHIP – ‘JA, BITTE’

The conference, titled “Defense Oversight and Inspector General/Ombudsman-type Systems”, was co-chaired by BG Dieter Naskrent, the IG for the German Armed Forces Staff of the Bundeswehr, reporting directly to the Chief of the German Armed Forces, and Colonel Mike Anderson, the IG for EUCOM, reporting to Gen. William Ward, the EUCOM Deputy Commander who also addressed the gathering.

waste, assessing morale, assisting members of the armed forces, safeguarding rights, improving unit readiness, and extending the eyes, ears, and conscience of a Commander, Chief of Defense, or Minister of Defense.

A longer term regional conference may also be held to address the desires expressed by Black Sea littoral states such as Romania, Bulgaria, Ukraine, and Georgia.



Conference working group being facilitated by EUCOM IG team members.

Though a variety of models were discussed, there was consensus as to what an IG can and should be. As Gen. Ward noted during his keynote address “sometimes the IG is a screwdriver, tightening a standard, sometimes a set of pliers, getting a grip on spending, and sometimes a moral compass always pointing in the right direction.” Gen. Ward’s words were endorsed by other senior US Inspectors General present at the forum, including the Honorable Claude Kicklighter, the DOD Inspector General, and Lt. Gen. Stan Green, the US Army IG.

OMBUDSMAN – EASY FOR YOU TO SAY

It was joked that the Swedish language has given the world two notable words; “ombudsman” and ...”IKEA”. “Ombudsman” is probably the lesser known of the two words. It is of course the Swedish word which has been adapted into English and other languages to describe an individual charged with representing the interests of a group by investigating and addressing complaints.

“IG OUTREACH” – QUITE A STRETCH

This gathering was the foundational event for an initiative by the EUCOM IG termed “IG Outreach”. The outreach effort supports EUCOM’s Strategy of Active Security aimed at promoting good governance and endorsing anti-corruption tools throughout its area of responsibility. Promoting the US military IG model is one method of achieving those aims.



Reinhold Robbe, Germany’s Parliamentary Commissioner for the Armed Forces

Participants requested follow-on regional Inspector General/Ombudsman workshops and seminars. A near term, subsequent regional seminar was asked for by Montenegro, for itself and for neighboring Balkan states.

Germany’s military Ombudsman, Reinhold Robbe, also participated in the conference. Robbe, a former

member of the German Bundestag, has been elected by the Parliament to defend the rights of Germany’s citizen soldiers. He reports directly to the Defense Committee of the Parliament, intentionally outside of the influence of the German Ministry of Defense. This feature of the

German system was attractive to a number of participating nations.

BOSNIA: SEEDS TAKE ROOT AND GROW

The IG system presented by Bosnia-Herzegovina's Ministry of Defense IG was the "youngest" of the models discussed. It is younger than the French system which has roots reaching back to 1445, and younger than the American model which stretches to the influence of von Steuben in the late 1700's. It is even younger than the German model, conceived in the 1950s in response to the Nazi horrors. It harkens back only to 1999 when an IG system modeled after the US IG version was imposed as part of the Dayton Peace Accords. In January 2006 the Bosnian IG able was first able to operate independently of NATO oversight.

Today the Bosnian IG, BG Rizvo Pleh, publicly thanks the tutelage that his nation and his IG's have received and continue to receive from both the US Army IG and from the Bosnian "Partnership IG" at US European Command. While Bosnia adopted the US military IG model, they have also "Balkanized" it, adjusting it to fit the unique circumstances of the Bosnian nation and culture. Their lessons were lessons applicable to all conference nations.



Col. Anderson with Afghanistan National Army IG, MG Sardar Mohammad Abulfazel (left) and MG Wakeel Akbari, Afghanistan Chief of Internal Affairs.

CONCLUSION – "RIGHT, NOW FORWARD"

A number of nations expressed interest in adopting the "Bosnian IG model". To be sure, these were predominantly Balkan states with similar histories and sized militaries. Nevertheless, the message was a profound one. A nation torn apart by a civil war merely a decade ago, exposed to the benefits of the US Inspector General system is now better postured to champion the rights of its soldiers, address corruption, and assess unit readiness. It is also today a model for its neighbors.

The story should sound somewhat familiar to U.S. Inspectors General. As it was often pointed out at this conference, the US model itself was an "import", a result of an "IG Outreach" of sorts, and fashioned after a Prussian style of inspection focused on readiness. This exposure to a functioning IG model is the essence of today's EUCOM's "IG Outreach" initiative, so impressively inaugurated in Germany in September within miles of the Hohenzollern castle from where von Stueben offered his services to the Continental Army in 1777.*



GEN Kip Ward, EUCOM Deputy Commander addresses seminar. Hon Kicklighter, DOD IG, LTG Green, US Army IG, and BG Pleh, Bosnian IG look on from the front row.

BIOGRAPHY

Col. Mike Anderson has served as the EUCOM IG since 2006. He and his office provide IG support to both EUCOM and the newly established AFRICOM.

Anderson is a graduate of both the Army and Joint Inspector General courses and a Foreign Area Officer with more than 18 years experience in Europe.

ALABAMA ALASKA ARIZONA ARKANSAS CALIFORNIA COLORADO CONNECTICUT DELAWARE FLORIDA GEORGIA HAWAII
IDAHO ILLINOIS INDIANA IOWA KANSAS KENTUCKY LOUISIANA MAINE MARYLAND MASSACHUSETTS MICHIGAN MINNESOTA MISSISSIPPI MISSOURI MONTANA NEBRASKA NEVADA NEW HAMPSHIRE NEW JERSEY NEW MEXICO NEW YORK
NORTH CAROLINA NORTH DAKOTA OHIO OKLAHOMA OREGON PENNSYLVANIA RHODE ISLAND SOUTH CAROLINA SOUTH DAKOTA TENNESSEE TEXAS UTAH VERMONT VIRGINIA WASHINGTON WEST VIRGINIA WISCONSIN WYOMING

10 OUTSOURCING PUBLIC INTEGRITY



BY ROBERT CUSICK
U.S. OFFICE OF GOVERNMENT ETHICS

I am honored to have been invited here today to address this audience, particularly because I know of some of the speakers who have come before me. I am neither an economist nor a businessman, just a lawyer of nearly forty years experience, albeit one with substantial experience in ethics law. President Bush nominated me to head the Office of Government Ethics - the ethics agency for the Executive Branch of the federal government. In that role, I am a policy maker in the sense that the Ethics in Government Act gives my agency the leadership role in ethics law and policy in the Executive Branch. Our office is a free-standing agency and as such, reports to the White House.

When I was preparing for my Senate confirmation hearing, the matter that bothered me most was the possibility of being embarrassed by a blunt question the answer to which I had not considered. Perhaps the most fearsome was, "What is government ethics?" That question is not addressed in any one place in the law, so I thought about it a great deal. I had been told by at least dozens of friends in Louisville that the answer was easy: It's an oxymoron. They always smiled when they said it, but that wouldn't do and I knew they did not really believe it either. The answer I developed was that,

Government ethics is that system of laws and procedures which tend to ensure that official government decisions are informed by the public interest rather than corrupted by private interest.

As it turned out, no one asked me the question that day, but I liked my definition and I spoke about it anyway and the hearing went very smoothly. Of course, in order

1 Condensed from a speech delivered by Robert I. Cusick, Director of the U.S. Office of Government Ethics, on October 11, 2007, at the David T. Chase Free Enterprise Institute as part of the Distinguished Lecturer Series at Eastern Connecticut University.

for the public interest to be reliably determined as in my definition, there must be press freedom, free speech, an independent legislative body and a serious commitment to transparency and accountability in government.


It is difficult for some people to talk about ethics at all. For some it is a corollary of religious belief, for others it is too general and philosophical; for some it is too legalistic and for others not legalistic enough. Nevertheless, government ethics has a powerful connection with public confidence. How the agents and officers of government act, even within their lawful authority, is assayed as an ethical measure by the public. Government officials often must decide between two goods, rather than between good and evil - in other words a policy decision about which some will inevitably disagree. Not every public policy decision is one that turns on government ethics, but ethics is often the weapon of choice for critics along the Potomac.



At the Dartmouth College Ethics Institute, they say that "ethics is that force which binds power to responsibility." As the federal government has more power than is to be found almost anywhere else, that bond is of critical importance.

I want to talk about one area in which the link between ethics and power is particularly sensitive and which presents risk for the future.

Policies designed to make the government more efficient and cost-effective have focused, since the Reagan Administration, on reducing the size of the federal workforce. In turn, many of the activities once carried out by government employees are now being carried out by employees of government contractors. Let me be plain: There is a place for government contractors.



The Office of Personnel Management reports there are 1.8 million direct federal employees, plus those in the postal service and the military services. Recently, Christopher Lee of the Washington Post estimated the size of the federal government at 14.6 million employees, counting employees, military members, postal workers, persons working on government grants and employees of government-funded contractors. The Wall Street Journal estimated last year that there are 7.5 million government contractors, which it characterized as four times the number of direct federal employees. The last group, in particular, has grown dramatically in recent years. It is not uncommon for someone to point to a government building and remark that “Half of the people in there are contractors.” There is nothing particularly wrong with that in my view, if the right circumstances are present, but my job makes me wonder: Are the right circumstances present?

The government, especially the defense agencies, has relied on government contractors since long before the Constitution was written.

- Even before we had a navy, coastal states sent out armed vessels under letters of marque, creating, essentially, a small fleet of contract sea fighters.
- A few blocks from where I live in Alexandria, Virginia, General Washington organized the large wagon train which would move south to supply the Continental Army at the battle of Yorktown. This was comprised mostly of contractors.
- The industrial strength of government contractors undeniably made a critical difference for the Union forces in the Civil War.

Were these federal officers and employees? Certainly not in a strictly legal sense, but were they working on behalf of the government- a government worker, you might say? Then yes, in some sense they were. Today, we don't know how many of this type of “government workers” we have. The problem is largely definitional. I have seen suggested numbers ranging from 3.6 million to over 26 million, the variance depending on your chosen definition of government worker.

Compared to historic American government, today, in the far more complex, bureaucratic, and publicly visible environment, we would have to give thought to government ethics even if we were not already doing so. The judgments citizens make about the government upon which they rely are strong but imprecise. If there is a problem with a taint of corruption, it is the government, writ large, which is the target of their criticism and decline in confidence. This government certainly includes contractors. The government will be impacted by such criticism, but will survive with some political consequences. The impact on government contractors caught in the same tangle can be even more economically damaging and permanent. The impact on public confidence is the most serious in my view. But it is undeniable that we need contractors in government. Contractors enable government to adapt quickly to changing circumstances; develop technologies the government is not well equipped to do; make personnel adjustments easily; and, they have continued access to highly skilled government retirees and provide more flexible use of wide-ranging government experience and military technical skills.

We all have to think about ethics, government ethics, value based ethics, and normative ethics such as exists in contractor organizations and not only in federal statutes and regulations.

Since the mid-1990s reduction in the government employee work force, the concept of the blended work force has taken hold. The problem is that the record suggests that the people who blended the work force gave little thought to blending the ethics. At some point this will be a problem. It probably is now.

I believe that the ethics programs in the executive branch work rather well. We have clearly stated, if sometimes complex, rules and laws, which directly address individual conduct. We have training mechanisms, enforcement mechanisms and program review procedures. We have easy access to investigators and prosecutors. We have none of this with respect to the employees of government contractors who can commit equally offensive and economically damaging unethical acts. Employees of most government contractors are out of our program's reach unless they commit a crime and we can refer them for investigation and prosecution.

For example:

- Most government contractors' employees do not have to disclose their financial interests to their employer, let alone the government. Consequently, they can purchase from businesses in which they or family members have a financial interest without either their employer or the government knowing. This inevitably leads to higher, non-competitive pricing, competitive damage to the contractor, and higher prices to the government.
- Most government contractors have no detection mechanisms in place to detect employee conduct damaging to them or the government.
- Many contractors have no prohibition on gifts to and from federal employees or potential subcontractors.
- There are no clear standards on abuse of position, disclosing sensitive but not classified government information or using government equipment by contractors' employees.
- We hear increasingly of contractors being hired to assess the work of other contractors. This presents several layers of conflicts of interest as well as the risk of inappropriate transfer of proprietary information.

It is important that we distinguish more clearly between what is an inherently governmental function and what is not. It is upon this point that considerations of management and delegation must turn.

What is the basis for the line of demarcation in ethics between federal employees and contractors? Is it purely structural or is it outcome based?


Ethics grows and flourishes in a context of strong and ethical senior leadership. It is heavily dependent on identity and culture. Who you think you are has a profound impact on what you believe your duties to be. The duties of federal employees run directly to the government, while the duties of contractors' employees run first to their employer, which is responsible to both shareholders and, by contract, to the government. David Walker, Comptroller General of the United States, recently said:

There's something civil servants have that the private sector doesn't, and that is the duty of the loyalty to the greater good – the duty of loyalty to the collective best interest of all rather than the interest of a few. Companies have duties or loyalty to their shareholders, not the country.

This is an important difference and we should not gloss over it. This is so even though most people don't understand me when I try to explain that OGE has virtually no control over the ethical conduct of contractors' employees and no legislative authority to create codes of conduct for them or to review contractors' ethics programs. Yet few areas of federal government are unaffected by it.

This is a major challenge for ethics programs in government. Our present laws and regulations directly address the ethical conduct of government employees, but do not, for the most part, deal with the ethical conduct of contractors' employees. This is certainly not to say that contractors' employees are inherently less ethical than Federal Government employees, but as I said earlier, ethical systems are important for accountability and the systems which exist across the range of government contractors represents a continuum from well organized and conscientious to non-existent. Ethical conduct is very dependent on ethical leadership and ethical culture, yet among thousands of contractors there must be enormous variability in ethical leadership and ethical culture. This is true quite apart from the blunt observation that contractors are businesses organized to make a profit. The Federal Government has some degree of control through regulations and contracts over the ethical conduct of organizations which are contractors for the government, but almost none over the conduct of the employees of those contractors.

So, today, when a decision is made for the government, is a government official actually making it? The formulaic answer still persists that government employees make the official decisions and contractors merely advise, but, at a practical level, the decision may indeed be made by a contractor's employee. The Federal Activities Inventory Reform Act of 1998 attempts to distinguish between inherently governmental functions and functions which are not, but how this distinction is observed in practice is elusive. This is particularly important as the Iraq War



and Hurricanes Katrina and Rita have made it difficult for the average citizen to distinguish federal employees from federal contractors.

I do not suggest that this is a problem for every government contractor, but I think you will agree the observation is generally valid. In the last three years we have become familiar with media pictures of government contractors dressed and armed as soldiers and only a sharp eye might notice the lack of military insignia. And, for years, Navy aircraft carriers have mixed within their crews “tech reps” that lived in officers quarters, sometimes and dressed in clothing similar to that worn by officers, although the public was seldom aware of them. Today, the problem of perception of ethical conduct is greatly complicated by contractor employees who look like government employees.

The problem is also framed vividly in the context of contractors who provide services and advice, including evaluation of other contractors, rather than those who provide equipment or provisions. It is literally true in

“Compared to historic American government, today, in the far more complex, bureaucratic, and publicly visible environment, we would have to give thought to government ethics even if we were not already doing so.”

government buildings in Washington and across the country that an official government decision may be made around a table by persons, some of whom are salaried government employees with no immediate profit motive, and private citizens who work for and report to profit-making organizations. The former group is subject to the ethics system overseen by OGE. The latter group is not. The decision arrived at around such a table may be correct and may have been ethically proper, but that is a hard case to make to a critical private citizen.


This changing dynamic raises some questions. As contractors become more involved in providing advice, making recommendations, overseeing the work of other contractors, and possibly even making decisions on

governmental policy – we have to consider what is being done to ensure that the work of contractor employees is carried out on behalf of the public interest – and not on behalf of some private interest? The companies they work for have a profit motive and it must be assumed that as individuals they are as exposed to temptation as actual government employees. The old adage states that “Public service is a public trust.” Where private contractors are engaged in public service, some mechanisms should be put in place to ensure a reasonable balance is struck between the profit motive and the public trust.

And, as I mentioned earlier, there is no hard data on how many contractors are working for the government, performing work previously considered to be work of government employees. But whatever the number of contractors working in or for federal agencies, it seems safe to assume that they will act in the same way as government employees:

The overwhelming majority will be committed to doing the best possible job for the American public. But, a small minority of contractor employees also will act like a minority of government employees. For example, they’ll be tempted to recommend that the government buy goods and services from their family’s business; or they’ll leak the government’s acquisition strategy to a potential bidder; or they’ll be looking for their next job with a different contractor while they’re supposed to be evaluating that contractor’s work for the government.

There is no real question about whether some segment of the contractor workforce will engage in some type of misconduct. It will. It already has. The question is whether there are adequate safeguards in place to protect against improper conduct which can undermine the public’s confidence in government integrity.



In an effort to ensure integrity in government operations, regular government employees are subject to a highly complex system of criminal and civil statutes and administrative regulations intended to prevent ethical lapses from occurring. The various provisions address a wide variety of subjects, such as financial conflicts of interest, acceptance of gifts, impartiality in decision-making, outside employment and other outside activities, misuse of office, and post-employment activities. Additionally, many regular government employees file financial disclosure forms that are reviewed for potential conflicts of interest by government ethics officials. In many cases, the forms are available to the public to add a degree of transparency to the system. Employees also are required to attend ethics training to remind them of the rules that apply. And of course, the various rules are enforced through criminal or civil prosecution, or disciplinary action by the offending employee's agency.


On the other hand, contractor employees are not subject to most federal ethics requirements nor are they subject to direct discipline by the government. It can be argued that in most cases involving contractors, this is for good reason. However, where the duties of contractor employees more and more resemble or seem indistinguishable from duties performed by regular government employees, questions inevitably will be raised about whether the government has sufficient safeguards to ensure that such close reliance on contractor employees does not compromise the government's interests in the integrity of its operations. It is not a question of whether the system is broken, but whether there is a real system in place at all. It can become quite ambiguous when, for example, the contractor/decision makers own stock in the company that will profit from the official decision. For a government employee, that could be a serious criminal violation. Should not contracting organizations be paying close attention to this issue? Such individualized motivation can not only tarnish the reputation of government, it can reduce the legitimate profit to the contractor.

The kinds of situations at issue typically do not involve contracts for the procurement of products or other clearly commercial activities such as supplying military

mess halls. The situations that have the potential to raise questions usually involve services contracts where there is close interaction between government and contractor employees, and where the government historically has been accustomed to relying on federal personnel for the services. An example might be an advisory services contract, especially where the advisor regularly performs in the government workplace and participates in deliberative meetings with government employees. Concerns about ethical conduct also are more likely to arise with broad management and operations contracts, such as those used to run laboratories and other major scientific or technological programs; and possibly with the large indefinite delivery or "umbrella" contracts that involve the de-centralized ordering and delivery of services at multiple agencies or offices. To the degree that such operations are decentralized, the ethical conduct of such operations can become difficult to achieve and ethical oversight a distant concern. The use of contractors inevitably attenuates the scope of ethical oversight.

“Ethics grows and flourishes in a context of strong ethical senior leadership.”

There are a number of current provisions designed to address contractor employee misconduct. For example, the Procurement Integrity Act prohibits disclosing or obtaining certain confidential procurement information; the Foreign Corrupt Practices Act (15 U.S.C. § 78dd-1) bars giving bribes or illegal gratuities to foreign officials; and the False Claims Act (31 U.S.C. 3729) bars defrauding the government. Contractors also would be subject to the anti-bribery statute at 18 U.S.C. § 201 if they were deemed to be “public officials.” But many ethical problems do not fall neatly under any of these provisions, which generally are aimed at truly criminal conduct. And while many companies that contract with the government have issued employee codes of conduct, these codes typically address compliance with the applicable criminal laws, or conflicts with the companies' interests rather than conflicts of other kinds.



What kind of misconduct should be covered by ethics rules, but currently is not? The types of ethical problems that are likely to be unaddressed by current laws or rules governing contractor employee misconduct can be illustrated by a few examples.

- **Financial conflicts of interest.** Financial conflicts arise when a contractor employee stands to gain or lose financially from his work. For example, an agency may hire a contractor to assess the performance of a small company that is developing a new document tracking system for the agency. As it turns out, the contractor's employee has invested heavily in the company developing the tracking system. The contractor employee would have a financial conflict of interest because his assessment might affect the value of the company as well as the interest of the government.

- **Lack of impartiality.** Concerns about a contractor employee's impartiality would arise where the individual's work could benefit or harm an outside party with whom the employee is associated. For example, the government hires a contractor to provide expert advice on the latest technology to authenticate identity for remote computer access. The contractor employee's brother owns a company developing such technology. If this were known, the contractor employee's impartiality would reasonably be questioned when he recommends that the government procure the technology from his brother's company. But how will it be known?

- **Misuse of non-public information.** Although there are already a number of laws or rules that apply to disclosure of confidential or classified government information, there is no general prohibition on the disclosure of any non public information by a contractor employee. For example, a contractor is hired by an agency that is seeking to procure highly specialized military weapons. The agency intends to use the contractor to help develop an acquisition strategy. The contractor's employee is hoping to get a new job with another company that could be interested in eventually submitting a proposal to provide the weapons. He leaks the acquisition strategy to the company, thus giving it a head start on preparing a possible proposal. How can this be discovered?

- **Gifts.** Unless a prosecutor can prove that a gift is a bribe, there is no rule or law that bars a contractor employee from accepting gifts from someone doing business with the government. For example, an agency hires a contractor to be its conference planner. The contractor employee's job involves visiting hotels to determine if they are suitable for the agency's needs. A hotel offers to give the contractor employee a free weekend visit for him and his family after the conference is over. If the contractor selects that hotel and accepts lodging for his family, there is a reasonable appearance that the contractor employee was influenced in his decision by the gift of free lodging. What system is in place to prevent this?

- **Misuse of government property.** On occasion, contractor employees may be permitted to use government property in performing a contract. This might occur, for example, when the contractor works at a government facility and uses a government car to travel to other government facilities. If the contractor employee also uses the car for personal business – for example by transporting his son and his teammates to soccer practice – he has likely violated the terms of the contract with the government, but no specific penalty would apply to him. By contrast, a regular government employee would receive a 30-day suspension for the same misuse. See 31 U.S.C. 1349.

Another pervasive weakness affects ethical conduct in government contracting. The Freedom of Information Act, which provides for broad public access to government documents, and which is used to powerful effect by the media and non-governmental organizations for oversight purposes, does not generally apply to private companies which are government contractors. The FOIA may require release of the contract itself or of certain reports in the hands of government, but certainly no wholesale examination of private company documents. Consequently, transparency in government which is generally regarded as supportive of an ethical culture is proportionally reduced as privatization of government increases.

The problem we face now in the context of expanded government contracting has several faces:

There is no comprehensive ethics system as exists in the Executive Branch.

There is no financial disclosure system to protect against financial conflicts of interest which may exist among contractors' employees.

Such ethical leadership as may exist is fragmented over the landscape of thousands of government contractors.

The degree to which an ethical culture exists among particular contractors is almost impossible to assess.

Transparency in government is reduced to some substantial degree.

Regulation of contractor entities is not, for ethical purposes, the equivalent of regulation of their employees.

It is perfectly understandable how the advocates of outsourcing government requirements for perceived economic benefits might not have been focused on these problems, but they exist. Something must bind power to responsibility.

More than a hundred years before the Ethics in Government Act, President Abraham Lincoln said something worth remembering,

*"...If you want to test a man's character, give him power."**

BIOGRAPHY

ROBERT I. CUSICK
U.S. OFFICE OF
GOVERNMENT ETHICS



The U.S. Senate confirmed the President's nomination of Robert I. (Ric) Cusick as the sixth Director of the U.S. Office of Government Ethics on May 26, 2006.

Mr. Cusick had a long and distinguished career as a partner in the Kentucky law firm of Wyatt, Tarrant & Combs, LLP and was active in legal and public officer ethics. He served as a member of the Board of Governors of the Kentucky Bar Association, as a member of the Kentucky Board of Bar Examiners, as Chairman of the Jefferson County (Kentucky) Ethics Commission, and as Chairman of the Kentucky Bar Association committee redrafting legal ethics rules in the context of Ethics in 2000. He is a graduate of the Brandeis School of Law of the University of Louisville. He served on active duty as a Navy JAG officer and retired as a Captain in the reserve in 1998.

Mr. Cusick is a Fellow of the American Bar Foundation and is a member of the American Bar Association Center for Professional Responsibility.



11 PCIE/ECIE AWARDS CEREMONY OCTOBER 23, 2007 REMARKS

BY PATRICIA MCGINNIS
THE COUNCIL FOR EXCELLENCE IN GOVERNMENT



It's quite an honor for me to be here today at the 10th annual awards ceremony of the President's Council on Integrity and Efficiency.

Thanks Dan [Levinson], for inviting me to be with you, for the important work you do at the Department of Health and Human Services, and for your commitment to the vision we all share – excellence in government.

I also want to thank your chair, Clay Johnson, my friend and someone who could be called the Results Czar or perhaps the “Honorary IG for Results” for the federal government. Clay, thank you for your relentless insistence on accountability and results from federal programs and for the example you always set for personal and professional integrity and excellence.

I especially want to thank all of you, the members of the President's Council – and the Executive Council – on Integrity and Efficiency; the extraordinary leaders who will be honored today; and your friends, families, coworkers and colleagues who are here to celebrate your work on behalf of the American people.

This beautiful Andrew Mellon Auditorium is the perfect place to recognize great public servants. Dozens of important government events have taken place here since this building was dedicated by President Franklin D. Roosevelt in 1935. You may be surprised to know that this building originally housed the Department of Labor and the Interstate Commerce Commission.

It was the site of the very first Selective Service System lottery in 1940, and the North Atlantic Treaty was signed in this room by President Truman in 1949, which led to the formation of NATO.

The auditorium was named for the Pittsburgh steel baron who was the only person to serve as Treasury Secretary under three different Presidents. Secretary Mellon was also President Hoover's Ambassador to Great Britain.

Some might also say that this is the perfect setting for a gathering of IG's because Andrew Mellon was one of the most investigated cabinet secretaries in modern history... but there were never any formal charges of misconduct. Fortunately he is far better known and remembered as a philanthropist, who underwrote the construction of the National Gallery of Art and donated his substantial art collection in 1937.

Enough about Andrew Mellon -- I want to talk to you today about excellence in government – I think that's what Dan had in mind when he invited me.

When I became President and CEO of the Council for Excellence in Government in 1994, I was thrilled to be leading an organization of many of the most esteemed former public servants in the country. It's quite an impressive group --

The living ex-Presidents are our honorary co-chairs.

Our board and members (whom we call Principals) have all served in government, they are Republicans, Democrats and maybe some Independents who have held appointed, elected or career positions in federal, state or local government. The thing they all have in common is that they believe in government and they want it to be effective – just like all of you.

So, early in my tenure, one of the Council's trustees asked me – how do you define excellence in government? What does it mean – what does it look like – how would you know if we achieved excellence?

Of course, I thought about the mission of the Council – to improve government performance and accountability to the public. But that’s not a definition.

What a great question – How would you define excellence in government? I thought about this quite intensely in the context of my work in government, and drawing upon my education in political science and public policy. I posed the question to people in government and people not in government. I asked my colleagues, board members, and Principals. Together, we came up with 5 words to communicate what we mean by excellence in government – you’ll see them on the wall when you come to the Council – Leadership, Innovation, Participation, Results and Trust.

The order of the words is important, with the pinnacle being trust, which follows results. Results require innovation and collaboration, and it all starts with leadership.

Abraham Lincoln’s vision was more eloquent – “government of the people, for the people and by the people” captures the essence of excellence in democracy. The Gettysburg Address is my favorite Presidential speech of all time – clear, timely, inspirational and only three minutes long.

The pinnacle is trust. Public service is a public trust and you are the guardians of the public trust. That could be your title, or your job description. If you think about it this way, you can see beyond the occasions when your visits or phone calls to government leaders are met with impatience, annoyance, concern, fear or worse.

Actually, when I was thinking about what to say today, I asked two people who work at the Council – both were senior federal executives at major agencies before coming on board – what they would do “if the IG called.”

Lynn [Jennings], obviously influenced by her legal training, replied that she would get all of her files in order and close at hand, make sure that her calendar entries were correct and up-to-date, and probably

have another staffer in the room when she returned the call. The other, Carl [Fillichio], obviously shaped by years of education by Catholic nuns, simply replied: “I’d pray.”

So, lets be honest – maybe you will never be greeted with warm fuzzy hugs, but you should be greeted with respect.

You can take pride in the results you achieve for the people you serve. Your Fiscal Year 2006 record of achievement is very impressive: IG audits, inspections, evaluations, and investigations that resulted in:

- Almost 10 billion dollars in savings from audit recommendations; and
- Nearly 7 billion dollars in savings in investigative recoveries

Citizens across the country as the customers and owners of government – need to hear more about your work “for the people.” They need to know that you are not only rooting out fraud, waste and abuse, but that you are insisting on effective government.

There is a crisis of trust in government today...and I’d like to suggest that you have an important role to play in turning things around. Trust in the government “to do the right thing” all or most of the time has declined steadily since the 1960’s (76%), except for brief uptakes



in the Reagan and Clinton administrations and a very steep increase in the Bush Administration after the terrorist attacks on September 11, 2001. But after a few months it began to fall and in July, 2007, only 24% of the public expressed trust in the federal government. We don't necessarily want or need 100% trust in government. A healthy balance between skepticism and trust should be the goal. In my view the level of trust should be in the 50-75% range – we have some work to do.



Mr. Clay Johnson III, Deputy Director of Management for the Office of Management and Budget, and Chairman of the PCIE, presents an award at the PCIE/ECIE Awards Ceremony.

Of course, there are many factors that affect trust in government. As you well know, it's not just about performance and results. What I call "Atmospheric pressures"...such as partisan politics, the media, and economic conditions also have a significant impact on public perception.

- The 24/7 news media certainly play a role. Scandal sells...News coverage of government has become less factual, more judgmental, and more negative, according to a Council study of the coverage of government in the first years of the Reagan, Clinton and George W. Bush administrations. It is a challenge to get good news out – we know the public would like to have more of it – so we have to keep trying.
- Partisanship has increased, especially in Washington. Who's up, who's down and who's winning has too often become a more important measure for leaders than accountability to the public for solving problems and

making progress on the issues they care most about. Other than Iraq and national security, the people's top priorities are jobs and the economy, healthcare, education, energy and the environment. But it is too often unclear to the public how government is making a difference on these issues – in ways that are relevant to their lives and the future. We need to do a better job in communicating about how government is performing -- straight talk about what is going well, what's not and where improvement is needed.

- The scarcity of resources – both natural and financial – is a significant factor in the trust equation. In the U.S., we face rising budget deficits that many, including me, believe are simply untenable. So, it is even more critical to invest in programs and strategies that work – based on rigorous evaluation and evidence of effectiveness.


As guardians of the public trust, your efforts to identify waste, fraud, and abuse – and to make recommendations to prevent and correct these situations – are needed now more than ever.

I would also like to challenge you to focus your leadership in three areas that I think are critical to efficiency and integrity – and to achieving a healthy level of public trust in government.

First, I suggest that you pay more attention to the rigorous evaluation of government programs in order to develop and share information about which approaches are effective and which are not. The Government Performance and Results Act and the Performance Assessment Review Tool both point to the value of rigorous evaluation but too few of our programs are the subjects of such independent assessment.

Second, as a community of professionals, you have the opportunity to learn from each other, to develop your leadership potential, both individually and together, to mentor others, to make the whole of your government wide network greater than the sum of your agencies.

Dan mentioned that you are working more collaboratively across agencies and levels of government. It would be great to see OIG employees as a leadership corps – with the agility



to move across agencies and assignments – to improve the performance and accountability of a wide range of programs and locations. The President’s Council provides visible leadership to your community. Communications, face to face meetings and joint leadership development opportunities all focused on how to be more effective guardians of the public trust – can enhance the value of your whole community.

Finally, my last suggestion – which is really a request – and that is to ask you to work together to attract and recruit the next generation of leaders to follow in your footsteps.

We all know about the “brain drain” from government as 90% of civil servants and 60% of senior executives become eligible to retire. Gen Y (18-30) is much smaller than the baby boom cohort so competition for talented workers in the future will be fierce.

Some good news on that front -- a recent study by the Council for Excellence in Government and The Gallup Organization showed that more than one third of Gen Y expressed significant interest in working in the federal government as did a significant number of professionals including those in law, public policy, and accounting -- all of which are professions in demand for your future federal workforce. These key prospects are attracted not only by the mission of government but more than that they are looking for intellectual stretch and growth potential – the opportunity to innovate and to make a real difference for real people. There is a generational difference here – for Gen Y, intellectual stretch and growth potential are most important, and job security and compensation are less important.

To harness this potential, you will have to recruit more strategically and creatively, streamline the hiring process and then, to keep talent, offer opportunities to lead, to work in teams and to be held accountable for important results sooner rather than later.

Let me read you two interesting quotes from our focus groups with Young Feds (under 30):

1. “One thing I did not know about the government going in is that the pace for advancement is very slow. And for somebody who’s starting right out of college it can be very frustrating.”

2. “I love the days that I walk out of the office grinning like an idiot because I know that I did something to positively affect where the country is headed.”

Your leadership and mentorship is critical to that “can-do” attitude and what can be achieved in an environment that values results and impact.

Let me end with a few of my favorite quotes about leadership from real leaders. Harry Truman, that great public servant, usually got right to the heart of things in a very few words. He once said a leader is “someone who can get other people to do what they don’t want to do and like it.” Good ole Harry Truman.

What does it take to be a leader? John Gardner was a legendary public sector leader (Secretary of HEW) who started the White House Fellows Program, founded Common Cause and won the Presidential Medal of Freedom. He said that leadership is not to be confused, as it often is in Washington, with status, power, or official authority. Instead, effective leadership focuses on vision, values, crossing boundaries, thinking into the future, the challenge of constant renewal, and inspiring and raising trust

Willard Wirtz, President Kennedy’s Secretary of Labor, would often talk about leadership by telling the story of visiting an elementary school during his tenure. A young girl came up to him and said: “I’m the labor secretary of the fourth grade!”

“That’s wonderful! But what exactly does the labor secretary of the fourth grade do?” Wirtz asked.

With great pride, the girl said that she washed the blackboard and clapped the erasers at the end of the day; on Friday, she cleaned up all the mess so that everything was in place to start fresh on Monday. And then she inquired: “What exactly do you do, as Secretary of Labor?”

Without missing a beat, Willard Wirtz replied: “Pretty much the same thing as you.”

So, what do leaders do? John Gardner said that leaders define what the future should look like, they align people to that vision, and inspire them to make it happen despite the obstacles. Or, as Willard Wirtz might say, they set the stage, cleanup the mess and cheer their colleagues on.

Management guru, Peter Drucker said that popularity is not leadership. Results are. Leaders are visible. They, therefore, set examples.

You are the examples. What you do matters a great deal. So thanks for what you are doing now and what you will do to make a difference and inspire trust. Congratulations and thanks for including me today.*

BIOGRAPHY


PATRICIA MCGINNIS
COUNCIL FOR EXCELLENCE
IN GOVERNMENT



Patricia McGinnis is President and CEO of the nonpartisan, nonprofit Council for Excellence in Government. The Council’s mission is to improve the performance of government at all levels and to strengthen the connection between citizens and their government. Among major Council initiatives are its leadership programs for senior career managers in the federal government and for Presidential Appointees and White House Staff, organized at the request of the Bush and Clinton Administrations. The Council’s Center for Democracy and Citizenship organizes bipartisan retreats for legislators in the U.S. Congress and also at the state level. The Council draws upon a national network of business, government, nonprofit and media partners to promote innovative, results oriented leadership and management in government. Specific accomplishments include the collaborative development of a blueprint for electronic government, an agenda of public priorities, recommendations and performance metrics for homeland security and emergency preparedness, and a series of town hall meetings to shape a public agenda for jobs and the economy.

Ms. McGinnis serves on numerous committees and boards, including the Dean’s Alumni Leadership Council of the Kennedy School of Government at Harvard University and the Board of Visitors at the University of Maryland School of Public Policy, where she is also an adjunct professor. She is a fellow of the National Academy of Public Administration, a member of George Washington University’s Homeland Security Policy Institute Steering Committee, on the Center for the Study of the Presidency’s National Council of Advisors and is currently a Director of the Brown Shoe Company in St. Louis, Missouri, and the Logistics Management Institute in McLean, VA.

She holds an M.P.A. from the Kennedy School of Government at Harvard University and a B.A. in political science from Mary Washington College of the University of Virginia.



12 ANNUAL CONFERENCE OF THE
ASSOCIATION OF PVO FINANCIAL
MANAGERS JUNE 27-28, 2007
REMARKS

BY DONALD GAMBATESA
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT
OFFICE OF INSPECTOR GENERAL

INTRODUCTION

Good afternoon. Thank you for inviting me to speak with you today. I am pleased to be here, and I hope that I can share some useful insight from our office's perspective to help you ensure that your programs are the best they can be and that you get the results you expect. The collective work of your organizations is essential to the mission of the U.S. Agency for International Development (USAID) and, as the Inspector General, I am particularly interested in preventing fraud, making sure that the programs the agency funds are well run, and seeing that government funds are spent wisely and appropriately.

As you are aware, USAID provides significant resources to nongovernmental and private voluntary organizations like yours. Since its inception over 25 years ago, the Inspector General's Office has worked to improve oversight mechanisms for USAID, as well as several other organizations, such as the African Development Foundation, the Inter-American Foundation, and the recently created Millennium Challenge Corporation.

BACKGROUND

I'd like to first give you some background about the work our office does and then talk about how we can help you manage an effective internal oversight process. Our mission, like that of other inspector general offices in the federal government, is to promote and preserve the effectiveness, integrity, and efficiency of the agencies we oversee by preventing fraud, waste, and abuse in their programs and operations.

We do this primarily by conducting audits and investigations of agency programs and operations. The activities we engage in are collaborative, proactive, and results-oriented. Our goal is to promote positive change within the organizations we oversee so that taxpayers are getting the most for their money and the funded programs are producing something tangible and worthwhile.

We have a workforce of approximately 180 direct-hire employees, as well as a number of Foreign Service national employees. About one-third of our employees work overseas in our regional offices in the Middle East, Africa, Europe, Asia, and Latin America.

FOREIGN ASSISTANCE TRANSITION

As many of you know, U.S. foreign assistance is undergoing a transition right now. Under Secretary Rice's leadership, the United States is looking to reform its organization, planning, and implementation of foreign assistance in order to promote transformational diplomacy. The primary goal of this effort is for each country receiving funds to build and sustain a well-governed, democratic state—a state that not only responds to the needs of its people but is able to conduct itself responsibly in the international community. To that end, the Department of State and USAID are working under joint strategic goals that articulate the U.S. foreign policy objectives shared by both agencies.

Along with this restructuring, the Administration has recommended—and Congress has appropriated—large increases in funding in several areas of the world where development assistance is most critical.

Much of these increases have been to rebuild both physical and human capacity following conflicts in Afghanistan, Iraq, and Lebanon; to help combat diseases like HIV/AIDS and malaria in Africa and Asia; and to provide humanitarian assistance in areas such as Sudan.

AUDIT ACTIVITIES

We conduct a variety of audit activities in accordance with government accounting standards issued by the Comptroller General of the United States. These include performance audits, financial audits, and information technology audits. During the last two reporting periods, we issued more than 500 audit reports that identified over \$137 million in questioned costs and \$11.5 million in funds that could be put to better use.

PERFORMANCE AUDITS

I'd like to highlight for you a few of our recent performance audits and talk about how our office helps improve programs and operations.

Some of the highest priorities we're addressing right now involve areas of conflict such as Iraq and Afghanistan, as well as the West Bank and Gaza.

The President's Emergency Plan for AIDS Relief, also known as PEPFAR, is another priority of the Administration, and we are actively working in the affected countries. We are also auditing other less well-known programs such as economic development programs in Latin America and Eurasia; food aid programs in Guatemala and Mozambique; and disaster reconstruction efforts in parts of Asia, along with Jamaica and Grenada.

In Iraq, our audits focus on a range of programs funded by USAID. These include the power sector, the educational system, the agricultural sector, and civil societies, to include civic education, women's advocacy, anticorruption efforts, and the promotion of human rights. Our recommendations in the Iraq program have resulted in better contracting procedures, improved coordination of equipment installation, and better planning processes for reconstruction activities.

We've directed our oversight in Afghanistan to projects involving road, school, and clinic reconstruction, as well as those that provide communities with work programs that encourage alternative livelihoods in key poppy-producing regions. Our audit of a \$108 million counter-narcotics program to provide economic alternatives to the production of opium poppy in Afghanistan found that the program had achieved significant results, such as training nearly 100,000 farmers in legal agricultural practices and accelerating legal business opportunities. However, we found that performance reporting procedures needed to be improved so that program results could be better monitored. USAID has since adopted those recommendations.

Significant resources are devoted to oversight of PEPFAR, a \$15 billion 5-year program that provides funding for HIV/AIDS-related prevention, care, and treatment services in 15 affected countries, such as in Zambia, Kenya, and Haiti, where infection rates are highest.

We have conducted a series of audits in four countries receiving USAID funding and again found problems with the reporting of progress, as well as the quality of performance data and the uniform reporting of achievements. Our office recommended closer coordination between USAID and the State Department to clarify reporting requirements and to improve the quality of performance data.

These are just a few examples of the performance audits our office conducts. These audit reports often include formal recommendations to agency managers to correct the detrimental conditions and causes identified during audit fieldwork. We monitor the recommendations to help ensure that they result in appropriate corrective actions by agency management, and we are required by law to report to Congress any audit recommendations that remain unresolved for more than six months.

FINANCIAL AUDITS

Another important element of our work is the oversight of financial audits. USAID is required by U.S. government regulations to obtain timely audits of its contractors and grantees. These audits are usually conducted by independent audit firms contracted either by USAID or the recipient organization, and are selected from a list of Inspector General-approved audit firms. We oversee these audits to help ensure that they are performed in accordance with appropriate standards and guidelines. We do desk reviews of audit reports and conduct periodic quality control reviews to determine whether the audits comply with U.S. government auditing standards. We also review reports submitted by the Defense Contract Audit Agency, which conducts financial audits of for-profit contractors.

IMPACT ON PVOS AND NGOS

How do our oversight responsibilities affect you specifically?

As most of you know, U.S.-based nonprofit organizations receiving more than \$500,000 in federal assistance during a fiscal year are subject to the financial audit requirements prescribed by the Office of Management and Budget's

Circular A-133. I should also note that this requirement relates to total federal financial assistance, which includes funds received through sub grants, as well as direct grants, from USAID and other federal agencies.

Additionally, our recipient-contracted audit guidelines require foreign nonprofit organizations spending more than \$300,000 of USAID funds during a fiscal year to have an annual financial audit performed. Final financial audits are required of all recipient organizations that expend more than \$500,000 of USAID funds throughout the life of an award regardless of whether they meet the \$300,000 threshold in any given year.

USAID contracts and grant agreements define the types of costs that are legitimate charges for supporting USAID programs. To increase awareness and compliance with cost principles, we conduct financial management training for overseas USAID staff, contractors, grantees, and others. This training presents a general overview of U.S. government cost principles and audit requirements. It also presents examples of concepts such as reasonableness of costs, the differences between allowable and unallowable costs, and compliance with applicable laws and regulations. During the last year, our staff has provided this training to more than 800 individuals in various countries throughout the world.

The vast majority of USAID-funded programs are carried out by hundreds of implementing partners, like you, who receive funding through numerous contracts, grants, and cooperative agreements. Consequently, many of our audit and investigative activities include organizations from the PVO and NGO community.

IMPORTANCE OF ACCOUNTABILITY

I know how important the issue of accountability is to each of you. Accountability and integrity are the pillars for effective leadership and oversight and the cornerstones of all financial reporting in government. The objectives of financial reporting for governments and for nonprofit organizations both stress the need for stakeholders to understand and evaluate the financial activities and management of these organizations. The public needs to be aware of the impact of the activities they are

supporting. The support the public provides privately to your organizations is voluntary, and—although you are nonprofit groups—you must compete with other organizations for resources. By ensuring that you have a transparent audit approach, you help convince would-be donors of the value, effectiveness, and efficiency of your services.

INTERNAL CONTROL MEASURES AND FRAUD AWARENESS

Therefore, it is important that your organizations have strong internal control measures, and I'd like to share with you some of the things you can do to mitigate your own internal risk. Specifically, I want to talk with you about some of the most common problems that our office uncovers when investigating contract fraud. I hope that, by making you aware of these occurrences, we can provide you with a tool to recognize suspicious activities, particularly in the overseas environment.

First, continually educating the contractors you deal with about U.S. contracting laws and regulations is an important step in preventing fraud. What may be acceptable business procedures in certain countries may not be acceptable when contractors are implementing projects funded by the United States.

I'm going to briefly speak about three of the most frequent problems we find when investigating contracts awarded to NGOs and PVOs to give you an idea of what you should look for in your own oversight process. What we see most often are fraudulent activities involving cost mischarging, progress payment fraud, and criminal and regulatory violations perpetrated by employees.

Cost mischarging occurs whenever a contractor charges the government for items that are not allowable, are not reasonable, or cannot be directly or indirectly allocated to the contract. The type of fraud we see most frequently is called an "accounting mischarge," which involves an individual's knowingly charging unallowable costs to the government, concealing them or misrepresenting them as allowable costs, or hiding them in accounts that aren't audited closely (such as office supplies).

Labor costs, as well as overhead expenses, are more susceptible to mischarging than material costs because the employees' labor can be readily charged to any contract. Some of the indicators you might look for are:

- Excessive or unusual labor charges by home office personnel.
- Abrupt changes in labor charge levels for no apparent reason.
- Labor time and charges that are inconsistent with the progress on the project.
- The inability of the contractor to supply time cards on demand.
- Time cards that are completed by the supervisor and not the individual employee, and
- Low-level work charged to high-level wage earners.

Sometimes we'll see contractors shifting costs, usually labor charges, from a less-profitable contract (such as a fixed cost or cost reimbursement type) to one or more other profitable cost-reimbursement contracts.

Another problem area, as I mentioned, is progress payment fraud. Progress payments are made as work progresses under a contract based on costs incurred, the percentage of work accomplished, or the completion of certain milestones. Fraud in progress payments occurs when a contractor submits a payment request based on falsified direct labor charges, on material costs for items the contractor does not possess, or on the falsified certification of a stage of completion attained. Some things to be aware of:

- Firms with cash flow problems are the most likely to request funds in advance of being entitled to them. Progress payments that don't seem to coincide with the contractor's plan and capability to perform the contract are suspicious and could suggest that the contractor is claiming payment for work not yet done.
- Another type of contractor fraud is submitting a progress payment claim for materials that have not yet been purchased. The contractor may issue a check to the supplier and then hold it until the government progress payment arrives. One way to confirm this irregularity is to check the cancellation dates on the

contractor's checks. If the bank received the check at about the same time or later than the contractor received the progress payment, then the check was probably held.

Some of the most egregious acts of fraud we encounter, however, are criminal and regulatory violations committed by employees responsible for overseeing or implementing contracts. Corruption and bribery, of course, are particularly problematic in many of the countries where the United States is providing aid, and we need to be vigilant for these types of acts. When I refer to employees, I'm including contractors and foreign nationals as well as oversight employees. Some of the warning signs that criminal or regulatory violations might be taking place are:

- Employees continually circumvent established procedures, including initiating actions without prior approval.
- Cash or commodities are handled carelessly, or cash is not turned in properly.
- Contracts are awarded that are outside the letter and spirit of established procedures.
- Employees have improper access to computer terminals and data.
- Employees exhibit unusual or extravagant behavior or spending (for example, an abrupt change in living style or carrying large amounts of cash).
- There is unusual or unauthorized interaction between an employee and a bidder or contractor.
- There is frequent or unusual travel.
- Actions are taken to obstruct an audit trail.

In short, anything that is contrary to regulation, good business practice, or common sense can indicate that something is wrong.

OTHER SERVICES PROVIDED BY OIG

These are just a few examples of the types of problems we see. We also have a detailed fraud indicators handbook that can be found on the USAID website, which provides many more examples of the types of fraud to look out for and common schemes that are employed.

It also provides information about the OIG hotline, where you can report suspected fraud. I encourage all of you to take advantage of that resource and to contact our office to provide clarification or to follow up with an investigation if necessary. In addition, we offer fraud awareness training to organizations like yours so that you can ensure your operations are functioning in compliance with the laws and regulations. In the last 5 years, our office conducted more than 300 of these training sessions in 50 countries, and we will be happy to brief your organization upon request.

Please feel free to call upon us if you have any questions or would like to request training for your organization in financial management or fraud awareness. I've brought some informational materials with me that provide contact numbers for our office, and we look forward to hearing from you.

Accountability and transparency are important to all of us. We recognize that supporting developing countries and eliminating corruption in government-funded programs require patience and diligence. To quote former United Nations Secretary-General Kofi Annan: "No one is born a good citizen; no nation is born a democracy. Rather, both are processes that continue to evolve over a lifetime." I appreciate the work that each of your organizations does to support developmental activities and to help ensure that government resources are spent in a manner that achieves the greatest good. Thank you again for inviting me to speak with you today.*



BIOGRAPHY

DONALD GAMBETESA
U.S. AGENCY FOR
INTERNATIONAL DEVELOPMENT
OFFICE OF INSPECTOR GENERAL



Donald Gambatesa began his tenure as the Inspector General at the U.S. Agency for International Development (USAID) on January 17, 2006, after more than 30 years of service in Federal law enforcement. Mr. Gambatesa serves concurrently as the Inspector General for the Millennium Challenge Corporation, the U.S. African Development Foundation, and the Inter-American Foundation.

In these capacities, Mr. Gambatesa oversees audit and investigative activities covering a wide range of foreign assistance programs and operations, including those devoted to economic development, disaster relief, global health, and reconstruction in areas of conflict. The Office of Inspector General helps improve foreign assistance programs through its recommendations and works to protect taxpayers' money by uncovering and investigating instances of fraud, waste, and abuse.

Previously, he served as the Special Agent in Charge of the Special Investigations Division in the Office of Inspector General at the USAID, and over 24 years as a special agent of the United States Secret Service (USSS). Mr. Gambatesa's career in the USSS included several leadership positions managing both protective security and investigative operations domestically and overseas. He has served as a special agent in charge in both field and headquarters offices.

Mr. Gambatesa has received numerous awards for outstanding performance and achievements during his law enforcement career. He is a graduate of John Carroll University and the Federal Bureau of Investigation's National Executive Institute. He is also a member of the International Association of Chiefs of Police and the National Executive Institute Associates.



PCIE and ECIE Membership



PCIE and ECIE Membership Members on Both Councils

Clay Johnson, III
Chair, PCIE and ECIE
Deputy Director of Management
OFFICE OF MANAGEMENT AND BUDGET
Eisenhower Executive Office Building
17th and Pennsylvania Avenue, NW, Room 113
Washington, DC 20503
(202) 456-7070

Gregory H. Friedman
Vice Chair, PCIE
Inspector General
DEPARTMENT OF ENERGY
1000 Independence Avenue, SW
Washington, DC 20585
(202) 586-4393
Web site <http://www.ig.energy.gov>
Hotlines (202) 586-4073
(800) 541-1625
Hotline E-mail ighotline@hq.doe.gov

Christine Boesz
Vice Chair, ECIE
Inspector General
NATIONAL SCIENCE FOUNDATION
4201 Wilson Blvd., Room 1135
Arlington, Virginia 22230
(703) 292-7100
Web site <http://www.nsf.gov/oig>
Hotline (800) 428-2189

Danny Werfel
Acting Controller
OFFICE OF FEDERAL FINANCIAL MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
Eisenhower Executive Office Building
17th Street and Pennsylvania Avenue, NW, Room 262
Washington, DC 20503
(202) 395-6059

Kenneth W. Kaiser
Assistant Director, Criminal Investigative Division
FEDERAL BUREAU OF INVESTIGATION
935 Pennsylvania Avenue, NW, Room 5012
Washington, DC 20535
(202) 324-4260

Robert I. (Ric) Cusick
Director
OFFICE OF GOVERNMENT ETHICS
1201 New York Avenue, NW, Suite 500
Washington, DC 20005
(202) 482-9300

Howard Weizmann
Deputy Director
OFFICE OF PERSONNEL MANAGEMENT
1900 E Street, NW, Room 5018
Washington, DC 20415-0001
(202) 606-1000

Scott Bloch
Special Counsel
OFFICE OF SPECIAL COUNSEL
1730 M Street, NW, Suite 300
Washington, DC 20036-4505
(202) 254-3610
Disclosure hotline (800) 872-9855
Whistleblower protection (800) 572-2249
Hatch Act information (800) 854-2824

PCIE Members

Donald A. Gambatesa
Inspector General
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT
Ronald Reagan Building
1300 Pennsylvania Avenue, NW
Washington, DC 20523-6600
(202) 212-1170
Web site <http://www.usaid.gov/oig>
Hotlines (202) 712-1023
(800) 230-6539

John L. Helgeson
Inspector General
CENTRAL INTELLIGENCE AGENCY
Room 2X30, New Headquarters Building
Washington, DC 20505
(703) 874-2555

Gerald Walpin
Inspector General
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
1201 New York Avenue, NW, Suite 830
Washington, DC 20525
(202) 606-9390
Web site <http://www.cnsig.gov>
Hotline (800) 452-8210

Phyllis K. Fong
Inspector General
U.S. DEPARTMENT OF AGRICULTURE
Jamie L. Whitten Building
1400 Independence Avenue, SW, Room 117-W
Washington, DC 20250-2301
(202) 720-8001
Web site <http://www.usda.gov/oig>
Hotlines (202) 690-1622 (800) 424-9121

Todd J. Zinser
Inspector General
DEPARTMENT OF COMMERCE
14th and Constitution Avenue, NW
HCHB 7898-C
Washington, DC 20230
(202) 482-4661
Web site <http://www.oig.doc.gov/oig>
Hotlines (202) 482-2495
(800) 424-5197
Hearing impaired (800) 854-8407

Claude M. Kicklighter
Inspector General
DEPARTMENT OF DEFENSE
400 Army Navy Drive
Arlington, Virginia 22202
(703) 604-8300
Web site <http://www.dodig.mil>
Hotline (800) 424-9098

Gregory H. Friedman
Inspector General
DEPARTMENT OF ENERGY
1000 Independence Avenue, S.W.
Washington, DC 20585
(202) 586-4393
Web site <http://www.ig.energy.gov>
Hotlines (202) 586-4073
(800) 541-1625

John P. Higgins, Jr.
Inspector General
DEPARTMENT OF EDUCATION
400 Maryland Avenue, SW
Washington, DC 20024
(202) 245-6900
Web site <http://www.ed.gov/about/offices/list/oig>
Hotline (202) 245-6911
E-mail oighotline@ed.gov

Daniel Levinson
Inspector General
DEPARTMENT OF HEALTH AND HUMAN SERVICES
330 Independence Avenue, SW, Room 5250
Washington, DC 20201
(202) 619-3148
Web site <http://oig.hhs.gov>
Hotline (800) 447-8477
E-mail hhstips@oig.hhs.gov

Richard L. Skinner
Inspector General
DEPARTMENT OF HOMELAND SECURITY
245 Murray Drive, Building 410
Washington, DC 20528
(202) 254-4100
Web site: <http://www.dhs.gov/xoig/index.shtm>
Hotline : (800) 323-8603
Hotline E-mail: dhsoighotline@dhs.gov

Kenneth M. Donohue
Inspector General
DEPARTMENT OF HOUSING AND URBAN
DEVELOPMENT
451 7th Street, SW
Washington, DC 20410
(202) 708-0430
Web site <http://www.hud.gov/offices/oig>
Hotlines (202) 708-4200
(800) 347-3735

Earl E. Devaney
Inspector General
DEPARTMENT OF THE INTERIOR
1849 C Street, NW, Mail Stop 5341
Washington, DC 20240
(202) 208-5745
Web site <http://www.doioig.gov/>
Hotline (800) 424-5081

Glenn A. Fine
Inspector General
DEPARTMENT OF JUSTICE
950 Pennsylvania Avenue, NW, Suite 4706
Washington, DC 20530
(202) 514-3435
Web site <http://www.usdoj.gov/oig>
Hotline (800) 869-4499
Hotline E-mail oig.hotline@usdoj.gov

Gordon S. Heddell
Inspector General
DEPARTMENT OF LABOR
200 Constitution Avenue, NW, Room S5502
Washington, DC 20210
(202) 693-5100
Web site <http://www.oig.dol.gov>
Hotlines (202) 693-6999
(800) 347-3756

William E. Todd
Deputy Inspector General
DEPARTMENT OF STATE AND THE BROADCASTING
BOARD OF GOVERNORS
2201 C Street, NW, Room 8100, SA-3
Washington, DC 20522-0308
(202) 663-0361
Web site <http://www.oig.state.gov>
Hotlines (202) 647-3320
(800) 409-9926

Calvin L. Scovell, III
Inspector General
DEPARTMENT OF TRANSPORTATION
400 7th Street, NW, Room 9210
Washington, DC 20590
(202) 366-6767
Web site <http://www.oig.dot.gov>
Hotlines (202) 366-1461
(800) 424-9071

Dennis Schindel
Acting Inspector General
DEPARTMENT OF THE TREASURY
Main Treasury Building, Room 4436
1500 Pennsylvania Avenue, NW
Washington, DC 20220
(202) 622-1090
Web site:
<http://www.ustreas.gov/inspector-general>
Hotline (800) 359-3898

J. Russell George
Inspector General
TREASURY INSPECTOR GENERAL FOR TAX
ADMINISTRATION
DEPARTMENT OF THE TREASURY
1125 15th Street, NW
Washington, DC 20005
(202) 622-6500
Web site <http://www.treas.gov/tigta>
Hotline (800) 366-4484

George Opfer
Inspector General
DEPARTMENT OF VETERANS AFFAIRS
810 Vermont Avenue, NW
Washington, DC 20420
(202) 565-8620
Web site <http://www.va.gov/oig>
Hotline (800) 488-8244
Hotline E-mail vaoighotline@va.gov

Bill Roderick
Acting Inspector General
ENVIRONMENTAL PROTECTION AGENCY
1200 Pennsylvania Avenue, NW, Mailcode 2410T
Washington, DC 20460-0001
(202) 566-0847
Web site <http://www.epa.gov/oig>
Hotlines (202) 566-2476
(888) 546-8740

Michael W. Tankersley
Inspector General
EXPORT-IMPORT BANK OF THE UNITED STATES
811 Vermont Avenue, NW.
Washington, D.C. 20571
(202) 565-3923
Web site <http://www.exim.gov/oig/index.cfm>
Hotline 1-866-571-1801

Jon T. Rymer
Inspector General
FEDERAL DEPOSIT INSURANCE CORPORATION
3501 N. Fairfax Drive
Arlington, VA 22226
(703) 562-2166
Web site <http://www.fdicoin.gov> E-mail: ighotline@fdic.gov
Hotline (800) 964-3342

Brian D. Miller
Inspector General
GENERAL SERVICES ADMINISTRATION
18th and F Streets, NW, Room 5340
Washington, DC 20405
(202) 501-0450
Web site <http://oig.gsa.gov/>
Hotlines (202) 501-1780
(800) 424-5210

Robert W. Cobb
Inspector General
NATIONAL AERONAUTICS AND SPACE
ADMINISTRATION
300 E Street, SW, Code W, Room 8V39
Washington, DC 20546
(202) 358-1220
Web site <http://oig.nasa.gov>
Hotline (800) 424-9183
Hotline Web site: <http://oig.nasa.gov/cyberhotline.html>

Hubert T. Bell
Inspector General
NUCLEAR REGULATORY COMMISSION
11545 Rockville Pike, Mail Stop T5-D28
Rockville, MD 20852
(301) 415-5930
Web site <http://www.nrc.gov/insp-gen.html>
Hotline (800) 233-3497

Patrick E. McFarland
Inspector General
OFFICE OF PERSONNEL MANAGEMENT
1900 E Street, NW, Room 6400
Washington, DC 20415-0001
(202) 606-1200
Web site <http://www.opm.gov/oig>
Hotline Fraud/waste/abuse (202) 606-2423
Hotline Healthcare fraud (202) 418-3300

Martin J. Dickman
Inspector General
RAILROAD RETIREMENT BOARD
844 North Rush Street, Room 450
Chicago, IL 60611
(312) 751-4690
Web site <http://www.rrb.gov/mep/oig.asp>
Hotline (800) 772-4258

Eric M. Thorson
Inspector General
SMALL BUSINESS ADMINISTRATION
409 3rd Street, SW, 7th Floor
Washington, DC 20416
(202) 205-6586
Web site <http://www.sba.gov/IG>
Hotlines (202) 205-7151 or (800) 767-0385

Patrick P. O'Carroll
Inspector General
SOCIAL SECURITY ADMINISTRATION
Room 300, Altmeyer Building
6401 Security Boulevard
Baltimore, MD 21235
(410) 966-8385
Web site <http://www.ssa.gov/oig>
Hotline (800) 269-0271

Richard Moore
Inspector General
TENNESSEE VALLEY AUTHORITY
400 West Summit Hill Drive
Knoxville, TN 37902-1499
(865) 632-4120
Web site <http://oig.tva.gov>
Hotlines (865) 632-3550
(800) 323-3835

ECIE Members

Fred E. Weiderhold, Jr.
Inspector General
AMTRAK
10 G Street, NE, Suite 3W-300
Washington, DC 20002
(202) 906-4600
Web site <http://www.amtrakoig.com>
Hotline (800) 468-5469

Clifford H. Jennings
Inspector General
APPALACHIAN REGIONAL COMMISSION
1666 Connecticut Avenue, NW, Suite 215
Washington, DC 20009-1068
(202) 884-7675
Web site:
<http://www.arc.gov/index.do?nodeId=2060>
Hotlines (202) 884-7667
(800) 532-4611

Carl W. Hoecker
Inspector General
U.S. CAPITOL POLICE
499 S. Capitol Street, SW, Suite 345
Washington, DC 20003
(202) 593-4642
Hotline (866) 906-2446
E-mail Oig@cap-police.senate.gov

A. Roy Lavik
Inspector General
COMMODITY FUTURES TRADING COMMISSION
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581
(202) 418-5110
Web site: <http://www.ignet.gov/internal/cftc/cftc.html>
Hotline (202) 418-5510

Christopher W. Dentel
Inspector General
CONSUMER PRODUCT SAFETY COMMISSION
4330 East West Highway
Bethesda, MD 20814-4408
(301) 504-7644
Hotline (301) 504-7906

Kenneth Konz
Inspector General
CORPORATION FOR PUBLIC BROADCASTING
401 9th Street, NW
Washington, DC 20004-2129
(202) 879-9660
Web site <http://www.cpb.org/oig>
Hotlines (202) 783-5408
(800) 599-2170

Michael Marsh
Inspector General
DENALI COMMISSION
Peterson Tower, Suite 410
510 L Street
Anchorage, Alaska 99501
(907) 271-1414

Curtis Crider
Inspector General
U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Avenue, NW, Suite 1100
Washington, DC 20005
(202) 566-3125
Web site <http://www.eac.gov/oig.asp>
Hotline (866) 552-0004

Aletha L. Brown
Inspector General
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
1801 L Street, NW, Suite 3001
Washington, DC 20507
(202) 663-4379
Web site:
<http://www.ignet.gov/internal/eeoc/eeoc.html>
Hotline (800) 849-4230

Carl A. Clinefelter
Inspector General
FARM CREDIT ADMINISTRATION
1501 Farm Credit Drive
McLean, Virginia 22102
(703) 883-4030
Web site <http://www.fca.gov/oig.htm>
Hotlines (703) 883-4316
(800) 437-7322

Kent R. Nilsson
Inspector General
FEDERAL COMMUNICATIONS COMMISSION
445 12th Street, SW, Room 2-C762
Washington, DC 20554
(202) 418-0470
Web site <http://www.fcc.gov/oig>
Hotline (202) 418-0473

Lynne A. McFarland
Inspector General
FEDERAL ELECTION COMMISSION
999 E Street, NW, Room 940
Washington, DC 20463
(202) 694-1015
Web site: <http://www.fec.gov/fecig/mission.htm>
Hotline (202) 694-1015

Edward Kelley
Inspector General
FEDERAL HOUSING FINANCE BOARD
1625 Eye Street, NW, Room 3095
Washington, DC 20006-4001
(202) 408-2544
Web site:
<http://www.fhfb.gov/Default.aspx?Page=100>
Hotlines (202) 408-2900
(800) 276-8329

Francine C. Eichler
Inspector General
FEDERAL LABOR RELATIONS AUTHORITY
1400 K Street, NW, Room 250
Washington, DC 20424
(202) 218-7744
Web site <http://www.flra.gov/ig/ig.html>
Hotline (800) 331-3572

Adam Trzeciak
Inspector General
FEDERAL MARITIME COMMISSION
800 North Capitol Street, NW, Room 1054
Washington, DC 20573
(202) 523-5863
Web site:
http://www.fmc.gov/bureaus/inspector_general/InspectorGeneral.asp
Hotline (202) 523-5865

Elizabeth A. Coleman
Inspector General
FEDERAL RESERVE BOARD
20th Street and Constitution Avenue, NW,
Stop 300
Washington, DC 20551
(202) 973-5005
Web site <http://federalreserve.gov/oig>
Hotlines (202) 452-6400
(800) 827-3340

Howard Sribnick
Inspector General
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2743
Web site <http://www.ftc.gov/oig/>
Hotline (202) 326-2800

Tony Ogden
Acting Inspector General
GOVERNMENT PRINTING OFFICE
North Capitol and H Streets, NW, Stop: IG
Washington, DC 20401
(202) 512-0039
Web site <http://www.gpo.gov/oig/>
Hotline (800)743-7574

Judith Gwynn
Acting Inspector General
U.S. INTERNATIONAL TRADE COMMISSION
500 E Street, SW, Room 515
Washington, DC 20436
(202) 205-3177
Web site <http://www.usitc.gov/oig>
Hotline (800) 500-0333

Ronald Merryman
Acting Inspector General
LEGAL SERVICES CORPORATION
3333 K Street, NW
Washington, DC 20007
(202) 295-1650
Web site <http://www.oig.lsc.gov/>
Hotline (800) 678-8868

Karl W. Schornagle
Inspector General
LIBRARY OF CONGRESS
101 Independence Avenue, Suite LM-30
Washington, DC 20540
(202) 707-2637
Web site <http://loc.gov/about/oig/>

Paul Brachfeld
Inspector General
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
8601 Adelphi Road
College Park, MD 20740-6001
(301) 837-1532
Web site <http://www.archives.gov/oig>
Hotlines (301) 837-3500
(800) 786-2551
Hotline E-mail oig.hotline@nara.gov

William A. DeSarno
Inspector General
NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street
Alexandria, Virginia 22314-3428
(703) 518-6351
Web site <http://www.ncua.gov/oig>
Hotlines (703) 518-6357
(800) 778-4806

Daniel L. Shaw
Inspector General
NATIONAL ENDOWMENT FOR THE ARTS
1100 Pennsylvania Avenue, NW
Washington, DC 20506
(202) 682-5402
Web site:
<http://www.nea.gov/about/OIG/Contents.html>
Hotline (202) 682-5402

Sheldon L. Bernstein
Inspector General
NATIONAL ENDOWMENT FOR THE HUMANITIES
1100 Pennsylvania Avenue, NW, Room 419
Washington, DC 20506
(202) 606-8350
Web site:
<http://www.neh.gov/whoweare/oig.html>
Hotline (202) 606-8423

Vacant
Inspector General
NATIONAL LABOR RELATIONS BOARD
1099 14th Street, NW, Room 9820
Washington, DC 20570
(202) 273-1960
Web site:
http://www.nlr.gov/About_Us/inspector_general/index.aspx
Hotline (800) 736-2983

Christine C. Boesz
Inspector General
NATIONAL SCIENCE FOUNDATION
4201 Wilson Boulevard, Room 1135
Arlington, Virginia 22230
(703) 292-7100
Web site <http://www.nsf.gov/oig>
Hotline (800) 428-2189
E-mail oig@nsf.gov

Geoffrey Johnson
Acting Inspector General
PEACE CORPS
1111 20th Street, NW
Washington, DC 20526
(202) 692-2916
Web site: [http://www.peacecorps.gov/index.cfm?shell=learn.
whatiscpc.management.inspcgen](http://www.peacecorps.gov/index.cfm?shell=learn.whatiscpc.management.inspcgen)
Hotline (800) 233-5874

Deborah Stover-Springer
Acting Inspector General
PENSION BENEFIT GUARANTY CORPORATION
1200 K Street, NW, Suite 470
Washington, DC 20005
(202) 326-4030 x3437
Web site <http://oig.pbgc.gov/>
Hotline (800) 303-9737

David C. Williams
Inspector General
U.S. POSTAL SERVICE
1735 Lynn Street
Arlington, Virginia 22209-2005
(703) 248-2300
Web site <http://www.uspsig.gov>
Hotline (888) 877-7644

H. David Kotz
Inspector General
SECURITIES AND EXCHANGE COMMISSION
100 F Street, NE
Washington, DC 20549-2736
(202) 551-6037
Web site <http://www.sec.gov/about/oig.shtml>
Hotline (202) 551-6060

Stuart W. Bowen, Jr
Inspector General
SPECIAL INSPECTOR GENERAL FOR IRAQ
RECONSTRUCTION
400 Army Navy Drive
Arlington, Virginia 22202
(703) 428-1100
Web site <http://www.sigir.mil/>
Hotline (866) 301-2003

A. Sprightley Ryan
Acting Inspector General
SMITHSONIAN INSTITUTION
MRC 12204, P.O. Box 37012
Washington, DC 20013-0712
(202) 633-7050
Web site <http://www.si.edu/oig/>
Hotline (703) 603-1894

Invitation to Contribute Articles

to

The Journal of Public Inquiry



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

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

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

**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;

