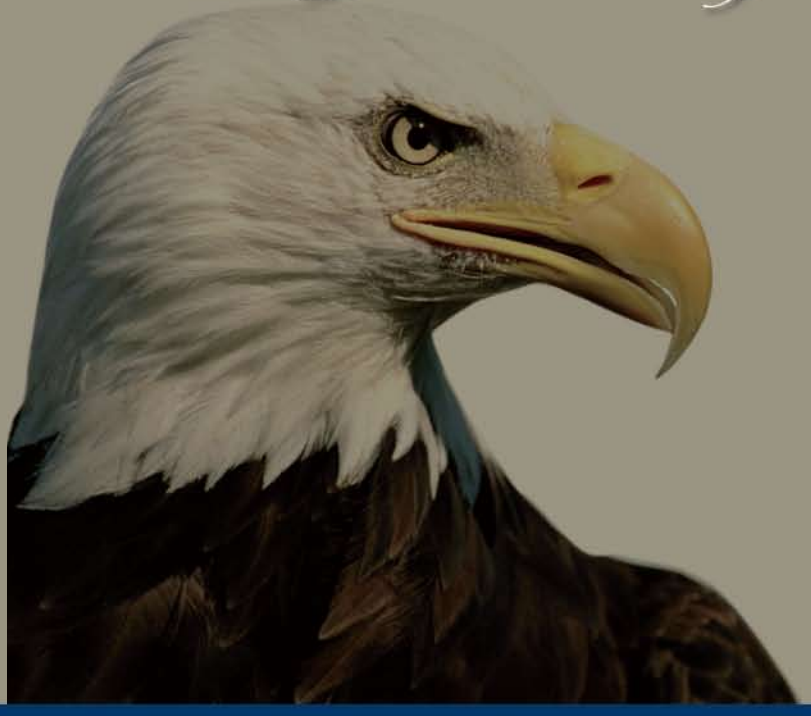
A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

The Journal of Public Inquiry



SPRING/SUMMER

2009

COUNCIL OF INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

Council of Inspectors General on Integrity and Efficiency

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

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

The CIGIE is led by Chair Phyllis K. Fong, Inspector General of the U.S. Department of Agriculture, and Vice Chair Carl Clinefelter, Inspector General of the Farm Credit Administration. The membership of the CIGIE includes 69 Inspectors General from the following federal agencies:

Members of the Council

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

LETTER FROM THE EDITOR-IN-CHIEF

Two words came to mind as I reviewed this issue of the *Journal of Public Inquiry*: "relevant" and "revealing." It is relevant because issues discussed involve topics currently making headlines. It is revealing because members of the Inspector General community were willing to share valuable insights. A great example of a relevant and revealing article is the feature involving real-time processes used by the Treasury Inspector General for Tax Administration to audit economic stimulus payments.

The *Journal* focuses on key challenges currently facing our community and ways to successfully turn those problems into solutions. The articles reveal timely information in regard to the following topics: whistleblower protections…desk audits...improving access to information...forensic auditing.

Our collective skills, talents, experiences, lessons learned, and best practices have combined to provide an influential forum. The *Journal* is a window into the IG world and has been a great reference that I have frequently referred to throughout my years as an Inspector General. One only needs to watch the news these days to see the contributions of the IG community. From audits to investigations to inspections – we are making a difference and adding value to our respective departments.

As members of the Inspector General community, we are charged with providing independent and objective oversight. In a single phrase, we "speak truth to power." One manner in which we do so is through congressional testimony.

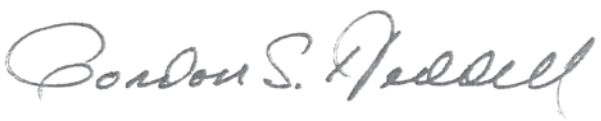
Congressional testimony is an important aspect of serving as an Inspector General. The *Inspector General Act of 1978*, as amended, states that we are "to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies related to the administration of such programs and operations and the necessity for and progress of corrective action."

The *Journal* includes six congressional testimonies related to a variety of current topics, such as Inspectors General: Independent Oversight of Financial Regulatory Agencies; Progress of the American Recovery and Reinvestment Act; Health Care Reform; U.S. Postal Service in Crisis; Small Business Innovation Research; and Hiring Practices.

In the words of President Franklin D. Roosevelt, "The truth is found when men are free to pursue it." The testimony we provide to Congress helps us bring important issues to light and provides transparency into the programs and operations of our agencies in an effort to make significant improvements.

Outreach is another important aspect of our work and this issue includes two speeches. The first is a speech I made this year to the graduates of the Combatant Command and Joint Inspectors General course. The second is a speech made by J. Russell George to the National Association of Tax Professionals at the 2009 Annual Conference.

I would like to thank the members of the Journal Editorial Board for their efforts, as well as the authors who shared their work with us. There is a great deal that can be learned each time so many experienced and dedicated individuals contribute collectively towards the betterment of the Inspector General community.



Gordon S. Heddell
Inspector General

Journal
of Public Inquiry

Feature Article

❧ Denotes the end of an article.

Economic Stimulus Payments Real-Time Auditing

The laws governing taxes frequently change and some of those changes can significantly affect both taxpayers and the economy

By Deann L. Baiza, John L. Hawkins, and Russell P. Martin

One thing is almost as certain as death and taxes…the laws governing taxes frequently change and some of those changes can significantly affect both taxpayers and the economy. As part of the Treasury Inspector General for Tax Administration's oversight of the Internal Revenue Service, we continually keep attuned to potential legislation that affects the tax laws, particularly those that can play a major role in the lives of taxpayers.

Several months before the financial meltdown and economic crisis gripped the country, the Congress and former President George W. Bush worked on ways to address a slowing economy and possible recession. In early December 2007, discussions of an economic stimulus package that included possible tax cuts began with a meeting of economists and business leaders.

We first learned of the possibility of economic stimulus legislation in January 2008 and our initial contact with the IRS occurred before the *Economic Stimulus Act* was passed. That contact was greeted with "Why are you here now?" The IRS was not expecting us to be involved quite this early in the process. Traditionally we look at an established program or process after it has been in place for some time. We explained that our approach was to look at the planning and implementation of the legislation as it happened with the hope that we could provide IRS with timely input that may prevent problems from occurring or at least minimize their impact. It was not long before the IRS saw the positive impact that this real-time audit approach provided as we began sharing valuable and timely information with the IRS throughout the audit process.

Using Lessons Learned to Develop an Audit Strategy Before Implementation Began

Once we learned of the possibility of economic stimulus legislation we immediately began evaluating the potential significance of the proposed legislation and how we could provide audit coverage should the legislation be enacted. Through monitoring news articles and other information from various sources, we soon realized this legislation would have a major impact on both IRS operations and taxpayers. Given both the significance and timeframe for implementation, we knew we needed an audit approach that would provide timely results and allow the IRS to make program corrections quickly to minimize the impact on taxpayers. We began laying out the framework for a multi-audit approach to assess the planning and implementation of the stimulus legislation once enacted.

The Act was signed into law on February 13, 2008. The Act's centerpiece was a tax cut in the form of an economic stimulus payment that would be paid as quickly as possible to U.S. taxpayers meeting certain qualifications.

While the tax credit was for Tax Year 2008, the legislation allowed for advance payment of the credit in the form of an economic stimulus payment based upon tax returns filed for Tax Year 2007. The IRS was tasked with the primary responsibility of identifying qualified individuals and issuing the economic stimulus payments. The IRS estimated more than 130 million households would qualify for what Congress estimated would total over $100 billion in economic stimulus payments.

However, further complicating the implementation of the legislation was the provision that qualified many retirees to receive a stimulus payment. Although qualifying, many of these individuals were no longer required to file an income tax return. How would the IRS identify and ensure retirees received their economic stimulus payment? Equally important, how would the IRS ensure millions received those payments at the same time the IRS was processing individual tax returns as part of its annual return filing season? Immediately after enactment, the IRS stated that the first payments would be issued to taxpayers in May 2008. That certainly did not leave the IRS or us much time to prepare. Despite the short time frame for payment issuance our planning efforts before the legislation was enacted ensured we were positioned to provide immediate oversight of the IRS' implementation of the legislation.

Now that we knew the details of the legislation, our first order of business was to finalize the scope of our multi-audit strategy. We drew on past experience to help identify the most significant areas of risk and define the scope of our audit strategy. The Congress had enacted similar legislation in June 2001 and again in May 2003, calling for the advance payment of a tax credit or refund. In both instances, we conducted audits to evaluate the IRS' efforts in issuing these advance payments. In both reviews we noted improvements that could be made in the way the IRS planned for or carried out the legislation. Because of the similarity of these laws and advance refunds, we knew that the prior TIGTA audits, and more importantly, the audit teams involved, would be a critical part of our determination of the best approach for reviewing the IRS' planning and implementation of the Act.

We evaluated the prior audit teams' approach to those reviews, the audit tests that were productive, the issues identified in those reviews, and how the Act's provisions were similar to or differed from the prior legislation. We held conference calls and meetings with those prior audit teams to discuss the testing and methodology used in the prior reviews as well as the issues previously reported that affected the IRS' ability to accurately issue the advanced refunds and the potential for the same problems occurring with this legislation. We also discussed the potential of fraudulent rebate claims and the need for the IRS to develop preventative controls. The lessons learned from those prior audits served as the cornerstone for the development of our economic stimulus audit strategy. The result was a strategy that provided real-time coverage of each stage of the Act from the planning of the economic stimulus payments in 2008 through the processing of the tax credits claimed on tax returns filed and processed in 2009.

Establishing a Coordinated Communication Strategy to Share Information Quickly

Because of the accelerated timeframe to implement the legislation, the substantial dollars at risk, and the number of taxpayers who could be impacted, we needed to develop a process to provide the IRS with immediate feedback relative to the concerns we were identifying to enable the IRS to take timely corrective action. In addition, the Act posed a unique audit challenge: implementation of the legislation crossed many IRS functional lines. How would we coordinate with all of the impacted functions so that there was two-way communications to ensure information was shared timely? Likewise, it was critical that we did not inhibit the IRS from devising and implementing numerous steps so economic stimulus payments could be issued as quickly as the legislation prescribed.

Communication with IRS was not our only concern. We also needed to communicate with our other TIGTA Audit divisions and groups that were involved with auditing various aspects of the legislation to ensure our coverage of the legislation was a coordinated cross-functional effort. As such we designated one audit team as the central communication point for requesting and sharing information with the IRS. This accomplished several things. It established "one voice" from TIGTA on the economic stimulus payments. Most importantly, this meant that the IRS heard from only one audit group on most of the legislation's provisions. Because of the high significance, the IRS was not bombarded with questions and issues coming from

so many different oversight groups.

The communication structure we established was instrumental in ensuring taxpayers received the stimulus payments they were entitled and helped us to timely accomplish our audit strategy.

Auditing as the Legislation Was Implemented to Minimize Errors

With our audit strategy developed and the communication lines established, it was time to get down to business. We initiated our multi-phase audit with the initiation of our first audit in late January 2008, two weeks before the Act was passed. While we knew these would be exciting audits with high visibility and importance, we also knew there would be stressful moments when audit results must be reported and delivered quickly.

Phase I – IRS Educates and Assists Millions of Taxpayers on the Economic Stimulus Payment

The first phase of our audit focused on the IRS' planning for and implementation of the economic stimulus payments. The review included an assessment of the IRS' efforts to implement the legislation and educate and assist taxpayers. The audit team for this phase included auditors who had worked on prior reviews of advance refunds, had knowledge of the IRS' fraud detection programs, or were experienced in the IRS' information technology modernization activities.

Our review identified that the IRS took extraordinary steps in planning for implementation of the legislation including a wide-reaching media campaign to educate individuals about what was required to receive an economic stimulus payment. While planning was generally sufficient, some IRS functions did not initially prepare action plans or had plans that missed key items to stop or deter fraudulent refunds.

Phase II – IRS Correctly Computed 99.6 Percent of the Economic Stimulus Payments Reviewed

Our coverage of the Act moved into the second phase designed to assess the accuracy of the IRS' computation of the payment and the adequacy of controls to ensure ineligible individuals did not receive an economic stimulus payment. To accomplish our objective, we partnered with a TIGTA information technology specialist to develop systemic programs to independently determine taxpayer eligibility for a payment and, if eligible, to calculate the amount of the economic stimulus payment for every taxpayer who had filed a Tax Year 2007 tax return prior to July 2008.

Once we computed the amount that an individual should receive, we compared the amount of our payment with the IRS' calculation. This analysis and comparison was done concurrently with the IRS' calculation of the economic stimulus payments and discrepancies were shared with the IRS before the payments were actually issued to the taxpayer. In many cases, that meant we only had two or three days to analyze hundreds of thousands of tax returns before payments were issued. We verified the accuracy of 129.1 million economic stimulus payments generated by the IRS as of June 13, 2008.

Audit Coverage Timeline

December 2007
Talk of an economic stimulus package begins.

January 25, 2008
TIGTA begins planning for coverage of the pending economic stimulus legislation.

January 30, 2008
TIGTA initiates Phase I assessing IRS' planning for and implementation of legislation.

February 13, 2008
The Economic Stimulus Act of 2008 is enacted.

April 3, 2008
TIGTA initiates Phase II assessing the accuracy of payment calculation and processes to ensure ineligible individuals did not receive payments.

April 22, 2008
Testing for Phase I ends.

April 28, 2008
Dept. of Treasury issues the first economic stimulus payments.

July 3, 2008
Testing for Phase II ends.

July 31, 2008
TIGTA issues Phase I audit report.

Phase III – IRS Ensured Eligible Individuals Received Their Economic Stimulus Payments

The third phase of our strategy determined if IRS' processes and procedures ensured all eligible individuals received their economic stimulus payment and that no payments were issued after December 31, 2008, which was the last date allowed by the legislation. By this time, the IRS had issued the majority of the stimulus payments for taxpayers who had timely filed their Tax Year 2007 tax return by April 15, 2008.

We monitored the IRS' efforts to correct error conditions identified by both the IRS and TIGTA where taxpayers did not receive the correct amount of the payments to which they were entitled. In addition, we evaluated the IRS' implementation of legislation passed subsequent to the Act that modified the economic stimulus payment eligibility rules for military taxpayers.

Phase IV – IRS Correctly Calculated 99.6 Percent of the Recovery Rebate Credits Reviewed Though Taxpayer Confusion Presented Challenges

The fourth and final phase in our strategy evaluated the planning, computation, and issuance of the recovery rebate credit. As previously mentioned, the economic stimulus payment was calculated based on Tax Year 2007 tax returns in an effort to release funds to individuals as quickly as possible. Although most individuals received the correct economic stimulus payment, there were individuals who did not receive an economic stimulus payment in 2008 who may have been entitled to receive a payment based on the filing of their Tax Year 2008 tax return in the form of a recovery rebate credit (generally filed between January and April 2009). In addition, some individuals could have received an additional amount when comparing information on their Tax Year 2007 and Tax Year 2008 tax returns.

Keeping in line with our real-time auditing approach, we began this phase of our audit in September 2008, months before the IRS would begin processing Tax Year 2008 tax returns claiming the credit. This allowed us to evaluate the IRS' planning and implementation efforts as they were occurring. Like the first phase of our strategy, we reviewed drafts of IRS documents, including tax forms, instructions, and other related publications for taxpayer use. We also reviewed IRS procedures and computer programming documents to ensure necessary programming changes for the recovery rebate credit were planned or had been made. As we drew closer to the start of the IRS' 2009 tax return filing season, we again worked with our TIGTA information technology specialist to expand our systemic programs to again independently determine taxpayer eligibility and compute the recovery rebate credit. As a result, we were able to verify the recovery rebate credit for over 102 million tax returns through April 17, 2009, as they were processed by the IRS.

"Using real-time auditing ensured millions of individuals received the economic stimulus payment and recovery rebate credit to which they were entitled and prevented billions of dollars in erroneous recovery rebate credits from being issued."

Audit Coverage Timeline (Cont'd)

- August 4, 2008 TIGTA initiates Phase III assessing process to ensure eligible individuals received payments.
- September 4, 2008 TIGTA issues Phase II audit report.
- September 8, 2008 TIGTA initiates Phase IV of its Audit assessing the planning, computation and issuance of recovery rebate credit.
- October 15, 2008 Last day to file a tax return to receive an economic stimulus payment in 2008.
- December 31, 2008 IRS stops issuing economic stimulus payments.
- January 16, 2009 IRS begins processing recovery rebate credits.
- February 27, 2009 Testing for Phase III ends.
- April 24, 2009 TIGTA issues Phase III audit report.
- June 11, 2009 Testing for Phase IV ends.
- September 9, 2009 TIGTA issues Phase IV audit report.

Overall, the IRS was able to achieve the intent of the Economic Stimulus Act. The IRS issued more than $104.8 billion in economic stimulus payments and recovery rebate credits to over 140 million taxpayers. Over the 18-month period from January 2008 to June 2009, we were able to provide the IRS with real-time input allowing the IRS to make improvements to informational notices and tax form instructions before they were sent to taxpayers. The IRS was also able to correct errors in its calculation of the economic stimulus payment and recovery rebate credit as well as its manual tax return processing procedures before the errors could negatively affect a significant number of taxpayers.

We were able to provide members of Congress with current information regarding the status and success of the IRS' economic stimulus and recovery rebate efforts. Our efforts identified over 533,000 eligible individuals who had not received economic stimulus payments or recovery rebate credits totaling approximately $190.1 million to which they were entitled. This included more than 56,000 individuals on social security that had not yet received but were entitled to an economic stimulus payment. In addition, our work prevented almost $1.6 billion in recovery rebate credits from being issued to almost 6.4 million taxpayers who were not entitled to receive a recovery rebate credit.

Deann L. Baiza

Deann L. Baiza is the Audit Manager of the TIGTA office in Kansas City, Missouri. Ms. Baiza audit group is part of the Electronic Tax Administration, Returns Processing and Accounts Services directorate and conducts multi-faceted reviews of IRS return processing and account settlement activities.

Most recently, her staff was received the PCIE Award for its work on the *Economic Stimulus Act of 2008*. Ms. Baiza started her career with the IRS Inspection Service as a Staff Auditor in 1989 in Kansas City, Mo. and joined TIGTA in 1998 before becoming an audit manager in 2000.

Ms. Baiza received a bachelor's degree in accounting with a minor in economics from Northwest Missouri State University.

John L. Hawkins

John L. Hawkins is a Senior Auditor in TIGTA's Kansas City, Mo. office. John started his career as an accountant in private industry and joined the IRS Inspection Service in 1977. In 1984, Mr. Hawkins joined the IRS as a Revenue Agent in the IRS Examination Division. Mr. Hawkins later returned to the Inspection Service and transitioned to TIGTA in 1998. During his time with TIGTA, Mr. Hawkins participated in many high impact audits of the IRS and served as the Lead Auditor on two of TIGTA's reviews of the *Economic Stimulus Act of 2008*.

Mr. Hawkins graduated Magna Cum Laude from Avila University in 1975 where he received a bachelor's degree in accounting with a minor in economics. He is a Certified Public Accountant and a member of the Association of Government Auditors.

Russell P. Martin

Russell P. Martin is the Director, Electronic Tax Administration, Returns Processing and Accounts Services, located in Stoneham, Mass. Mr. Martin is responsible for managing and directing audits of IRS individual tax return processing. Mr. Martin oversees three offices located in Cincinnati, Ohio, Kansas City, Mo. and Austin, Texas.

Mr. Martin began his federal career in 1989 working as an Auditor with the Inspection Service in Andover, Mass. Mr. Martin then joined TIGTA in 1998 and held positions including senior auditor and audit manager before being promoted to director in 2008. Mr. Martin received a bachelor's degree in accounting from Nichols College.

[OUTREACH]

Marshalling Whistleblower Protection

Protecting the whistleblower process is one of the most important duties of an Inspector General

By Eric B. Kempen and Andrew P. Bakaj

The Department of Defense Inspector General has a mission to promote integrity, accountability, and improvement of the Department of Defense personnel, programs, and operations in supporting our warfighters. Critical in achieving this is providing a method of communication for Defense employees who witness "wrongdoing." The IG provides this avenue. Whistleblower complaints arrive through a myriad of avenues such as whistleblower stakeholders, IG hotlines, component IG referrals, and congressional inquiries. The importance of whistleblowing, especially in the DoD context, in supporting and protecting warfighters from inefficient, ineffective, and often illegal activities that disrupt their operations is best illustrated by the story of Ernest "Ernie" Fitzgerald, a DoD whistleblower whom Senator Charles E. Grassley of Iowa once described as "the father of all whistleblowers."[1]

Mr. Fitzgerald worked as a management systems deputy for the Department of the Air Force where he was responsible for the development of improved management controls. In 1968, Mr. Fitzgerald reported a $2.3 billion cost overrun in the Lockheed C-5 aircraft program. As a congressional witness before the Joint Economic Committee, he rejected the advice of Air Force officials and testified with candor and transparency about billions of dollars in avionics program cost overruns and other technical problems. In response to Mr. Fitzgerald's testimony, President Richard M. Nixon directed that he be fired. "It was reported that Nixon told aids to, 'get rid of that son of a bitch.'" In executing the president's order, Mr. Fitzgerald was ultimately terminated by Defense Secretary Melvin Laird.[2]

Senator Charles Grassley and Mr. Ernie Fitzgerald

Because of his candor and commitment to the truth, Mr. Fitzgerald was a driving force for whistleblower protections. Mr. Fitzgerald continued to fight a four-decade long campaign against fraud, waste, and abuse within the Department. Consequently, he was instrumental in the enactment of the *Civil Reform Act of 1978*, a precursor to the *Whistleblower Protection Act of 1989*.

The WPA exists to ensure that federal employees are free from prohibited personnel practices, including retaliation for whistleblowing. Pursuant to the *Inspector General Act* and Executive Order 12674, executive branch employees have a positive obligation to report fraud, waste, abuse, and corruption. Further, for making such a disclosure, federal managers are prohibited from taking or threatening to take any adverse personnel action as reprisal.[3]

Protecting the whistleblower

1 152 Cong. Rec. S1780 (daily ed. March 06, 2006) (statement of Sen. Grassley).

2 Vest, Jason, Maverick Moves On, Government Executive (April 15, 2006), http://www.govexec.com/features/0406-15-/0406-15na2.htm

3 Executive Order 12731 (October 17, 1990). See also Whistleblower Protection Act of 1989.

process is one of the most important duties of an IG. It is a means of supporting the sourcing of administrative and criminal investigations and audits. With respect to civilian DoD employees, the DoD IG's Civilian Reprisal Investigation Directorate is committed to supporting and training its employees in whistleblower rights and responsibilities. CRI facilitates this through the Office of Special Counsel's Section 2302 (c) Certification Program. DoD component IGs are encouraged to explore the OSC certification process because, as Mr. Fitzgerald demonstrated, whistleblowers are an invaluable resource in the oversight of warfighter operations. Accordingly, IGs must set the example in protecting its sources of those individuals who report "wrongdoing."

Critical in protecting whistleblowing is raising awareness. CRI promotes this through three methods: outreach, investigations, and training. Each of these is interrelated and all support the investigative mission. Without "investigations" marked by independence and integrity, outreach and training cannot modify management behavior. Outreach is conducted in order to educate strategic stakeholders about the mission of CRI, the basics of whistleblowing and whistleblower reprisal, and to ultimately generate complaint referrals. CRI actively investigates whistleblower reprisal complaints not only to educate witnesses and responsible management officials alike in whistleblowing rights and responsibilities, but also to ensure that DoD civilian employees who blow the whistle are protected from reprisal. CRI actively trains DoD IG supervisors, managers, and new employees though the Section 2302 (c) Certification Program.

Congress enacted Title 5 Section 2302 (c) of the United States Code in 1994 as a response to reports of widespread ignorance in the federal workforce concerning employees' right to be free from retaliation as a result of whistleblowing. The provision states that the head of each agency has the responsibility to ensure "that agency employees are informed of the rights and remedies available to them" for making a protected disclosure. Accordingly, the DoD IG is responsible for "the prevention of prohibited personnel practices" and the creation of a workplace environment in which retaliation against employees for making a protected disclosure is prohibited.[4]

OSC's 2302 (c) Certification Program allows federal agencies to meet their statutory obligation to educate their workforce about the rights, responsibilities, and remedies available to them under the WPA. The DoD IG has participated in the certification process since September 2002. As a result, both new and current IG employees are informed of their rights under the WPA.

Failure to inform federal employees of their whistleblower rights and obligations hurts the DoD, our warfighters, and the federal government as

4 Title 5 USC § 2302(c).

Certification Program

OSC will certify an agency Section 2302 (c) compliant if the agency meets the following five requirements:

1. Place informational posters in all personnel and EEO offices and in other prominent places throughout the agency;

2. Provide written materials to new employees as part of the orientation process on PPPs, the WPA, and the OSC (OSC has created informational materials, including an outline of PPP rights and remedies);

3. Provide annual notification to current employees about PPPs, the WPA, and OSC's role in enforcing these laws (OSC has made available examples of letters sent to agency employees by agency heads, outlining rights and remedies under the WPA);

4. Train managers and supervisors to ensure their understanding of responsibilities under the PPPs and whistleblower protection provisions of Title 5. (OSC can provide speakers for training and a Power Point presentation); and

5. Provide an OSC Web site link via the agency's intranet and/or Web site.[1]

1 www.osc.gov/outreach.htm (Accessed on May 15, 2009).

a whole. We see the importance of this in today's current Global War on Terror operations whereby the Defense Hotline provides an avenue to report fraud, waste, and abuse. Defense whistleblowers have prompted investigations and audits into numerous mission critical functions and activities that directly impact the war-fighter.

For instance, the Defense Criminal Investigative Service vigorously investigates GWOT-related allegations involving matters such as bribery, theft, and procurement fraud. In addition to investigating allegations of fraud, waste, and abuse; in 2008 DCIS launched a proactive project, which is analyzing over $14 billion in payment vouchers related to U.S. Army purchases in Iraq. Moreover, the DoD IG has numerous ongoing Iraq-related audits including contract surveillance, contract payments, and acquisition of armored vehicles.

Compliance with Section 2302 (c) certification provides federal employees with the understanding that:

1. It is their responsibility to come forward when they witness a violation of a law, rule, or regulation;
2. There is a place, such as an IG, for federal employees to turn to when they witness fraud, waste, or abuse; and
3. Mechanisms are in place to both: protect their identity after disclosing a violation of law, rule, or regulation; and investigate reprisal actions against them by management.

Further, compliance with Section 2302 (c) certification achieves three goals:

1. Allows source protection;
2. Alerts and prevents potential systematic agency issues; and
3. Corresponds with the Obama Administration's policy and practice for openness and transparency.

As Mr. Fitzgerald demonstrated, whistleblowers are critical in reporting wrongdoing and we, as federal agencies, have a responsibility to educate our employees of their rights. Employees who are educated in whistleblower rights and responsibilities, and particularly of the protections afforded to whistleblowers, will be more confident in reporting possible violations of law, rule or regulation, gross mismanagement, gross waste of funds, abuse of authority, or a substantial danger to public health and safety.

As a former Defense official once said, the actions of an Inspector General are to "reinforce the message that we will vigilantly protect our soldiers, airmen, and marines from those who seek to defraud them and will hold accountable anyone who betrays the public trust." We, therefore, urge other DoD organizations and federal agencies alike to become Section 2302 (c) compliant and consider the OSC as a valuable resource for achieving this important goal.

Eric B. Kempen

Eric B. Kempen is an Investigator on the Procurement Fraud Reprisal Team, Civilian Reprisal Investigations for the DoD IG. He graduated Summa Cum Laude with a bachelor's degree from the University of Maine in 2005. Mr. Kempen earned his Master in Public Administration from Syracuse University Maxwell School of Citizenship and Public Affairs in 2008.

Andrew P. Bakaj

Andrew P. Bakaj is an Investigator and the team leader of the National Security Reprisal Team, Civilian Reprisal Investigations for the DoD IG. Mr. Bakaj provided oversight over the National Security Agency's first substantiated reprisal investigation resulting in the agency's first disciplinary action against an NSA official for reprisal. Mr. Bakaj earned his bachelor's degree in International Affairs at George Washington University and attended Syracuse University College of Law to earn a J.D.

[INVESTIGATIONS]

The Desk Audit: How a Supervisor Can Help the Struggling Investigator

Just how much time does the investigator have to work on any one case?

By Inspector General Randy D. Scott

As a supervisor I find it frustrating when an investigation is stalled and appears to be going nowhere. If it is not a particularly difficult category of investigation, I have to be concerned about the investigator. Is the case an anomaly or is it typical of the majority of cases carried by the investigator? One method I use to help make such a determination is the desk audit process. When using the desk audit, I need to keep the limitations of what I call the "investigative box" in mind. Certain unavoidable factors impose limits, (the sides of the box).

- Box Side 1: There is a limited amount of time to conduct a criminal, administrative, or civil inquiry.
- Box Side 2: There are a limited number of personnel who can be assigned to any one case.
- Box Side 3: There is a limited amount of money that can be spent on any one case.
- Box Side 4: There are laws, regulations, and policies that limit how an investigation can be conducted.

Time

The amount of time an investigation is taking may be the biggest discussion item I have with an investigator. New cases are reported and need to be assigned. Certain cases have a higher level of visibility inside and outside the organization. As a supervisor, I am expected to keep things moving and to guide or push investigators as needed. When I conduct a desk audit I need to know if the investigator has a realistic understanding of the amount of time it will take to successfully resolve the case. Is the time estimate realistic given the number of leads to be completed? My experience as a case agent and as a supervisor should allow me to make a good estimate. Do I have a good understanding of the limited number of hours that are available to the investigator? Just how much time does the investigator have to work on any one case? Do I remember all of the demands placed on a case agent?

Let's look at a possible work schedule for a three month period of time for a federal investigator working a 10 hour investigative day. Three months represents about 60 workdays, multiplied by 10 hours per day, yields 600 potential work hours per quarter. Now let's begin reducing those potential work hours with the other time demands placed on the investigator.

Scheduled annual leave of one week	-40
Scheduled court appearance estimated by the AUSA to be one week	-40
Quarterly required legal training	-8
Quarterly required firearms and unarmed self-defense training	-8
Physical fitness incorporated with lunch hour three times per week	-36
Planned surveillance in support of a major investigation	-40
Total available hours	428

If the investigator has 428 available hours for 25 assigned cases that represents about 17 hours, or roughly two days per case per quarter. Not all that much time and it includes those administrative hours for documenting interviews and assembling reports. Also, this assumes there are no

special assignments from the front office, sick leave, or any other unplanned events to interfere with the work schedule.

Personnel

Normally, I assign a new investigation to one investigator to see it through to completion. To successfully complete a case or to move a stalled investigation forward, the investigator may need more personnel to assist.

Is surveillance required? Are there a large number of witnesses to be interviewed? Will a search warrant be executed and multiple investigators needed for several days? If so, where will I find those personnel to help in the investigation?

Unlike popular British detective dramas, there is usually not a chief constable, multiple detective sergeant constables, and several shifts of detective constables devoted to a single investigation. Even if extra personnel are available for short periods of time, very quickly they have to return to their own case load.

Money

There are always budget limitations in any organization and for every case. If the investigator and I believe 24 hours of surveillance of a suspect is required and the surveillance team requires an airplane, is funding available? While the investigator is enthusiastic about the case, can I convince the front office that expensive air surveillance is a good investment?

What other less expensive investigative techniques might I suggest to help resolve the case or move it forward?

Laws, Regulations, and Policies

Does the investigator understand the elements of the offense under investigation or the allegations? I need to remember if this is the first time the case agent has worked on this category of crime or if the investigator has worked, for example, only on major fraud cases for the last five years. Is the investigator making full use of the laws, rules, regulations, and procedures available? For example, could a federal grand jury subpoena provide needed records if probable cause for a search warrant has fallen short? If a suspect is in custody, has the investigator prioritized the remaining work to meet speedy trial requirements?

All investigators have to deal with the limits imposed by the investigative box. But sometimes, these day-to-day challenges can be overwhelming for an investigator. As a supervisor, I become concerned when deadlines are missed. What do I need to do when it appears cases do not seem to be moving toward completion? When other investigators start to complain that they are always getting the new cases coming through the door, what is my response? If the AUSA calls and wants to know why subpoenas have not been delivered or key witnesses interviewed, how do I respond?

As a supervisor, I get a variety of clues from a variety of sources that I have an unproductive investigator. They may come from other members of the squad, my boss, outside sources or even from the investigator. Every once in a while, a case agent says "I'm overloaded and I need help. I don't know what I should be doing on these cases."

The Desk Audit Process

Rather than waiting for the clues to come my way, I have found that use of the desk audit process is the best early warning system to identify the unproductive investigator. It helps me start the process of figuring out why there might be a problem.

The desk audit can provide the mechanism to help an investigator navigate around the fours sides of the investigative box. I schedule the average productive investigator for a desk audit on an average of 90-120 days, just to make sure the assigned cases are moving towards completion. This is the opportunity for me to make sure the investigator is working toward the goals and objectives of the squad, the office, or the organization overall.

For an unproductive investigator, I find that 90-120 days is too long. Here is where the standard file review technique is modified for use as a performance improvement or development plan. I schedule a development plan file review at least every 60 days. If problems persist, I could schedule it at a 45 or 30 day interval depending on the investigator and my comfort level with his or her work.

Just like the regular desk audit process, the development plan desk audit starts with the investigator. The case agent creates a list of all assigned cases with the date the investigation was opened and assigned. The investigator lists the major allegation (such as fraud against the government over $50,000). The case agent then writes a one to three sentence summary of the investigation to date along with a summary of the planned investigative activity. The investigator estimates the amount of time that will be devoted to that particular investigation during the next review period of 60, 45, or 30 days. This time estimate cannot exceed the available hours for the next desk audit time period and must include all of the other time commitments required such as annual leave and training.

In theory, each investigation should have some investigative activity during the review period. As a practical matter, that is not always possible. Some cases will have had no investigative activity during the review period. There may be a logical explanation for the lack of activity. It is nonetheless an opportunity for me to discuss with the investigator

what is happening especially if there has been no activity for more than one review period.

Now back to the investigative box. When a case is apparently stalled, I must examine the four sides of the box for that particular investigation. Has there been sufficient time for the investigator to work on a particular case?

Is surveillance required but other personnel have not been able to participate? Do I need to assign additional personnel for specific days to assist in the investigation? Is there another investigative agency with potential interest in the case that could contribute personnel even for a period of time? Are specialized forensic personnel needed, which requires that I talk with another supervisor from another squad regarding scheduling?

If funding is an issue, what are the specific requirements? Are funds needed for a short-term light undercover operation or a sting operation? Are special rental vehicles needed? Does a subpoena request require extra funds to pay for copying expenses for the case file, prosecutor, and eventually for the defense in a major white collar crime case? Has the investigator started the funding request process and completed the necessary paperwork to obtain funding? Do I need to intervene with the administrative office to get the request moving?

Has the case agent run into an unusual legal situation that I need to discuss with the legal advisor for the office or a supervisor in the U.S. Attorney's Office? Do I need to remind the case agent of a change in the law or an organizational policy that either authorizes or prohibits certain investigative techniques?

As the investigator and I work our way through each case during the desk audit process, I develop a better understanding of exactly what is happening. A pattern forms. I may decide the investigator is overloaded and some cases need to be reassigned or closed. Or, I may decide the agent is not working to full capacity and I need to provide specific guidance for each case.

Keeping in mind the time limits imposed by the investigative box, the case agent and I agree on milestones and deadlines that are set or adjusted from a prior desk audit. At the end of the desk audit, the investigator will have a clear understanding of exactly what needs be done for each case. The investigator and I have developed a workable and agreed upon action plan.

Since the goal of the development plan desk audit process is to provide the investigator an opportunity to improve, I should see progress over a series of desk audit meetings. Once sufficient progress has been made and all investigations are back on track, I can resume the 90-120 day routine or standard desk audit schedule.

Not every series of development plan desk audits quickly moves the unproductive investigator back to the totally productive stage. Sometimes backsliding takes place. Sometimes the process never takes at all.

In such cases, a second option I can use is the intensive or daily audit. Unproductive days can become unproductive weeks and roll into a problem desk audit. The intensive or daily audit allows for my daily interaction with the investigator for a short but useful period of time. As with the other reviews, the process starts with the investigator.

At the beginning of each day, the investigator takes the first 15 to 20 minutes and prepares a summary of what investigative activity was conducted the day before with reference to the specific cases involved. Next, the investigator lists a summary of what is planned for the upcoming workday, again with reference to specific cases. This can best be done by an e-mail sent to me.

However, the investigator is not done. The process is followed by a 5 to 10 minute discussion with me that allows me to quickly review and provide any needed clarification. Since the planned work references specific investigations, I can review the last desk audit worksheet, as needed. After our brief discussion, I can make comments in a reply e-mail, send it for confirmation to the case agent, and file it under the name of the investigator for future documentation.

Most investigators, being investigators, can follow the trail at this point and realize I am documenting their work on a daily basis. At this point, the investigator should be making a serious attempt at work improvement to get out from under the daily audit.

Admittedly, the daily audit adds to the burden of an already busy supervisor. Nonetheless, it is an investment that pays off in the future when I have a more productive investigator who requires less supervision.

The development plan desk audit process and the daily audit are designed to restore an investigator to full productivity, but if required, the audits can also provide me with a well documented record for future personnel action.

The desk audit process allows for the regular review of investigative work that ensures the goals and objectives of the unit are being met. The supervisor and the investigator have an agreed upon strategy for the next review period whether it is 120 days, 60 days, or tomorrow. It allows for periodic fine-tuning of investigations or daily mentoring and training for improved performance of a struggling investigator.

Sample Desk Audit Summary

1. **Case name and number**: Smith, John A. #123-456-789
2. **Offense**: Fraud against the government over $50,000
3. **Allegation**: An employee and cooperating witness alleged that over the last six months, Smith filed false claims in excess of $10,000-$12,000 per month against the government for work not done as part of a contract for electrical repairs at a government installation.
4. **Investigation completed since last desk audit**: The cooperating witness and three additional witnesses interviewed. Contract obtained and reviewed. Invoices submitted by Smith to date being assembled by accounts payable office but some invoices appear to be missing. Some invoices signed by persons other than Smith.
5. **Planned investigation**: The cooperating witness is willing to hire an undercover investigator posing as administrative assistant in the accounting office of the company to work on a part-time basis. Liaison being conducted with AUSA to establish limits on undercover activity. Interview of witnesses and cooperating witness to be continued. Search warrant affidavit for main office company records to be discussed with assigned AUSA.
6. **Time Estimate**:
   a. 2 -hours- Finalizing undercover operation with AUSA
   b. 45-60 hours- daily telephone contact with undercover investigator and summary of investigative activity for the next 30 days
   c. 16-24 hours- interviews of company personnel
   d. 4-8 hours- final debrief of cooperating witness
   e. 8-hours- preparation, legal review, and meeting with AUSA regarding possible search warrant for documents.

   75-102 estimated total hours of investigative work
   and written instructions from supervisor on desk audit:

Cancel plans for undercover operation. (Undercover person not currently available.) Concentrate on finishing interviews and seeking search warrant. Conduct trash cover of business dumpster with new agent on squad and include results in search warrant application. Estimate how many investigators will be needed for search warrant execution and interviews of suspect company officials. Recalculate time estimate for case for review period.

Randy D. Scott

Randy D. Scott is the Inspector General of the Human Services Department in Santa Fe, N.M. His office is responsible for statewide investigations, audits, and financial recovery operations regarding public assistance programs and professional standards investigations of department employees.

Prior to his current assignment, Mr. Scott was a security consultant for the Northrop Grumman Corporation in Albuquerque, New Mexico. He retired from the Federal Bureau of Investigation having served as a Special Agent in Seattle and a Supervisory Special Agent in San Francisco (Oakland Resident Agency). He subsequently was assigned to FBI Headquarters in Washington D.C. working at the National Counterintelligence Center in Langley, Va. Prior to his transfer to the FBI, Mr. Scott was a Special Agent of the Naval Investigative Service assigned to Memphis, Tenn., Agana, Guam, the USS Forrestal, Charleston S.C., and Orange County Calif.

[OUTREACH]

Three Ideas to Improve Effective Inspector General Access to Both Information and Individuals

It has been said that knowledge is power; today, access is power

By Inspector General Brian D. Miller

Renewed interest in oversight and accountability, highlighted by implementation of the *American Recovery and Reinvestment Act of 2009*, Pub. L. No. 111-5, has focused sharply on the need for transparency, effective oversight, and the roles of Inspectors General across the federal government. Transparency compels IGs to conduct robust oversight and thus commands federal officials to give IGs access to documents, individuals, and information systems. It has been said that knowledge is power. Today, access is power. IGs without access are powerless and cannot ensure transparency. The ideas presented below would help to improve oversight and transparency by improving IG access.

Congressional interest in the role of IGs was shown in the ARRA provisions giving IGs, among other things, additional authorities and responsibilities, in matters involving ARRA funds, to interview contractor employees and conduct whistleblower investigations. Congressional support for the IG function was demonstrated through enactment of the *Inspector General Reform Act of 2008*, which implemented several proposals suggested by the Legislation Committee of the National Procurement Fraud Task Force, such as expanding (1) coverage of the *Program Fraud Civil Remedies Act* and law enforcement authority to all IGs; and (2) IG subpoena authority to include electronically stored information and tangible things. In addition, discussions are ongoing regarding other proposals put forth by the Task Force, such as additional amendments to the PFCRA and enhancement of Office of Inspector General authority to conduct computer matches.

With respect to effective access to information and individuals, however, some hurdles still remain that are not being addressed. Those hurdles are impeding the ability of the IG community to ensure that oversight is as fully transparent and efficient as possible. Access to both information and individuals is essential for effective oversight. When access is delayed or denied, auditors and investigators may not find important material and results may be attenuated and incomplete. Denial of access to employees of contractors, for example, can pose unnecessary challenges as IGs attempt to understand what really happened with a contractor's billing practices. On the other hand, having to notify the target of the existence of an investigation in order to get his/her financial records can impede the conduct of that investigation.

In this article, I advance two new ideas not previously offered by the Task Force, and a third new idea to modify the Task Force's suggestion on IG subpoena authority. These ideas, individually or collectively, would help to ensure IGs and their staff have access to the data and individuals necessary to

perform their work. The first idea concerns timely access to financial records, an issue that arises frequently in investigations, without having to tell the target about the investigation. The second idea involves removing procedural roadblocks to OIG access to electronic information systems, which can create needless delays. The third idea focuses on ensuring proper access to individuals who work for federal contractors, by giving IGs additional authority, without raising the concerns that testimonial subpoena authority seems to raise. Taken together, these ideas would be valuable aids to improving the work of IGs as they strive to protect the American public from fraud, waste, and abuse.

1.) "Don't Tip Off the Target" Amendment to the Right to Financial Privacy Act

Basic investigative techniques include not "tipping off" a subject about an investigation. Premature disclosure can lead to destruction of evidence, intimidation of witnesses, or flight. It can also preclude undercover work and provide an opportunity for the subject to manipulate his finances to frustrate the government's interests. As an illustration, telling someone like Bernie Madoff that he was under investigation would only give him an opportunity to hide or transfer ill-gotten gains before the government had an opportunity to understand the full extent of his crimes or freeze his assets.

Current RFPA Requirements Pose a Problem

The RFPA currently requires IGs to provide notice to the subject of an investigation when issuing a subpoena for that person's financial records, absent a court order delaying such notice for 90 days, before the IG can obtain those records. This notice requirement could harm the investigation and cause unnecessary and undue delay. Inspector General subpoenas should be treated the same as grand jury subpoenas, which are exempt from the requirement to give the subject notice.

The RFPA, which does not apply to state or local governments, was adopted to create a statutory Fourth Amendment protection for bank records primarily in response to *United States v. Miller,* 425 U.S. 435 (1976), where the Court held there was no such protection. Grand jury subpoenas were excepted from the customer notice and challenge provisions in the RFPA because of the secrecy surrounding grand juries and a concern that notice and challenge rights might in fact harm the privacy of those under investigation. As stated by the Supreme Court, the purposes served by grand jury secrecy include preventing escape, preventing tampering with witnesses, encouraging free disclosures by witnesses, and protecting the innocent. *United States v. Procter & Gamble Co.,* 356 U.S. 677 (1958).

These factors apply equally well to IG investigations, which also can be harmed by premature disclosure. Investigation records are covered by the *Privacy Act*, which protects the confidentiality of those records. In addition, timing suggests that when Congress adopted the RFPA, they did not consider the effect on IG investigations. The IG Act was enacted on October 12, 1978 (P.L. 95-452), while the RFPA was enacted on November 10, 1978 (P.L. 95-630). With the passage of the IG Act and the more recent Reform Act, perhaps it is time to correct that apparent oversight.

The requirement for notice to the subject prior to obtaining his financial records can be detrimental to an investigation in several ways:

- Providing notice to a target can provide him an opportunity to destroy or tamper with evidence, flee, or intimidate witnesses.
- Such premature disclosure can also prevent legitimate undercover work and make recovery of misspent funds more problematic. These financial transactions can be extremely complicated to trace and unravel, and advance notice can impede the government's forfeiture and other civil remedies that are designed to ensure the minimization of unlawful losses of federal dollars.
- The notice requirements can also cause undue delay. As an initial matter, if the government does not know all the names on the account, the government must issue a subpoena to the bank to identify the account holders. Then, after obtaining the identities of the account holders, the government must issue another subpoena and comply with the notice provisions for each account holder. There is an additional minimum 15-day delay between sending the notice to the customer and obtaining the records, or a potentially longer delay if the Department of Justice decides to seek a court order, which delays notice for 90 days. If the Department of Justice seeks a delay or the customer files a challenge in court, the law enforcement agency cannot obtain the records until the court issues a decision, a process that could take a significant amount of time during which the subject would be free to move assets and otherwise hamper the investigation.

The RFPA also requires notification to the subject within 14 days when records obtained under the RFPA are transferred to another agency, which would apparently include records transferred from an IG to the Department of Justice in furtherance of a criminal investigation. I know of no other law that requires notifying the subject when records are transferred to a prosecuting authority.

Because of the similarity in the interests served by grand jury and IG investigations, and the protections afforded the records, I suggest that Congress consider giving IGs the same exemption from the RFPA notice requirement that grand jury subpoenas currently have, such that an IG does not have to notify a target when a subpoena for his financial records is issued.

Proposed Language for "Don't Tip Off the Target"
Amend 12 U.S.C. 3413(i) and 3420 to read as follows:

Title 12. Banks and Banking

§ 3413(i) Disclosure pursuant to issuance of subpoena or court order respecting grand jury proceeding or law enforcement investigation
Nothing in this chapter (except sections 3415 and 3420 of this title) shall apply to any subpoena or court order issued in connection with (1) proceedings before a grand jury or (2) a law enforcement investigation by an Inspector General pursuant to the Inspector General Act of 1978, as amended; except that a court shall have authority to order a financial institution, on which a grand jury or Inspector General subpoena for customer records has been served, not to notify the customer of the existence of the subpoena or information that has been furnished to the grand jury or in response to the IG Subpoena, under the circumstances and for the period specified and pursuant to the procedures established in section 3409 of this title.

§ 3420. Grand jury information; notification of certain persons prohibited
(a) Financial records about a customer obtained from a financial institution pursuant to a subpoena issued under the authority of a Federal grand jury or by an Inspector General as part of a law enforcement investigation—

1. ***in the case of a grand jury subpoena, shall be returned and actually presented to the grand jury unless the volume of such records makes such return and actual presentation impractical in which case the grand jury shall be provided with a description of the contents of the records;***
2. ***in the case of a grand jury subpoena, shall be used only for the purpose of considering whether to issue an indictment or presentment by that grand jury, or of prosecuting a crime for which that indictment or presentment is issued, or for a purpose authorized by rule 6(e) of the Federal Rules of Criminal Procedure, or for a purpose authorized by section 3412 (a) of this title;***
3. ***in the case of an Inspector General subpoena, shall be used only for a legitimate law enforcement purpose, and any subsequent disclosure or transfer of records obtained pursuant to that subpoena to the Department of Justice shall be exempt from the provisions of section 3412(a) and (b) of this title;***
4. ***shall be destroyed or returned to the financial institution if not used for one of the purposes specified in paragraphs (2) or (3); and***
5. ***shall not be maintained, or a description of the contents of such records shall not be maintained by any government authority other than in the sealed records of the grand jury or by an Inspector General, unless such record has been used in the prosecution of a crime or to further a legitimate agency administrative purpose consistent with the Privacy Act.***

(b)(1) No officer, director, partner, employee, or shareholder of, or agent or attorney for, a financial institution shall, directly or indirectly, notify any person named in a grand jury or Inspector General subpoena served on such institution in connection with an investigation relating to a possible—
(A) crime against any financial institution or supervisory agency or crime involving a violation of the Controlled Substance Act [21 U.S.C. 801 et seq.], the Controlled Substances Import and Export Act [21 U.S.C. 951 et seq.], section 1956 or 1957 of title 18, sections 5313, 5316 and 5324 of title 31, or section 6050I of title 26; or
(B) conspiracy to commit such a crime, about the existence or contents of such subpoena, or information that has been furnished to the grand jury or Inspector General in response to such subpoena.
(2)Section 1818 of this title and section 1786 (k)(2) of this title shall apply to any violation of this subsection.

2.) Explicit Access to Agency Information Systems by Oversight Authorities

Providing IGs with explicit, unrestricted read-only access to agency information systems would remove a current roadblock to effective oversight of agency programs. The *Federal Information Security Management Act* and implementing procedures, such as the controls prescribed in *National Institute of Standards and Technology Special Publication 800-53A,* require federal agencies to control access to their information systems. The IG Act, in turn, provides that IGs are to have access to all agency "records, reports, audits, reviews, documents, papers, recommendations, or other material" related to the programs and operations of the agency. Systems owners' understanding of the types of access controls required can result in limiting or delay-

ing IGs' access to material, impeding the unrestricted access contemplated by the IG Act. The lack of an explicit provision for access by IGs as oversight bodies has caused confusion and inconsistency in information security management and can result in unnecessary delays to IG reviews and oversight.

The required systems controls include "least privilege" and "need to know," which allow authorized accesses only for users who are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. To implement this requirement, system owners have implemented protocols that require the requesting organization to provide information such as a limited timeframe for access, the security clearance level of each person requesting access, and the justification for access, which can be interpreted to require a statement as to the specific project purpose. Because the system owner controls access, moreover, that owner can require the IG to provide specific details as to the purpose of access before granting that access, and the system owner can, in fact, deny access.

In my view, these controls, as implemented, may place too many restrictions on the IG access contemplated in the IG Act. Frequently, the IG may want to conduct various reviews on information in agency IT systems simply to look for potential weaknesses or problems. To have to explain to the agency in each case why the IG wants access, and obtain the agency's permission, seems to contradict the intent of the IG Act. I believe the interests of IG oversight and IT security can be better balanced by providing explicit guidance on IG access to IT systems, and providing that IGs themselves must ensure that any access by their employees complies with applicable requirements, rather than leaving that determination to the system owners.

I suggest an amendment to the *Federal Information Security Management Act of 2002*, as follows:

Section 3544 of title 44, United States Code, is amended—

by striking "and" at the end of paragraph (a)(4);

by striking a period and inserting a semicolon at the end of paragraph (a)(5); and

by adding at the end of subsection (a) the following:

"(6) if the agency has an Inspector General appointed under the Inspector General Act of 1978 or any other law, ensure that the Office of Inspector General has unrestricted "read-only" access for review and analysis to all agency information systems from the Inspector General's accredited system. The Director of the Office of Management and Budget and the National Institute of Standards and Technology shall promulgate guidance to implement this paragraph."

3.) Access to Contractor Employees

Often issues that may arise in the course of an audit or investigation can be resolved or disposed of simply by talking to the people who were involved. When those people are federal employees, there is ample precedent for the expectation that they will be available to talk with IGs and their staffs as needed subject to the usual constitutional and *Privacy Act* protections. There is no similar expectation, however, with regard to people who work for federal contractors. Since so much of the government's work is currently accomplished with contractors, it stands to reason that contractor employees have a wide range of knowledge of and experience with activities that likely will become the subjects of audits or investigations. Not being able to talk to them presents a significant problem for ensuring effective oversight.

There has been discussion between the IG community and Congress regarding expanding IG subpoena authority to include testimonial subpoena authority, as suggested by the Task Force. However, Congress has not introduced legislation to accomplish this purpose, and concerns about that recommendation include implications for the Fifth Amendment, and questions regarding whether the DOJ should be involved in the decision to issue the subpoena, since DOJ would have to seek a court order to enforce the subpoena in the case of a refusal to comply. In light of those concerns, I am proposing an alternative, based on language in the ARRA and in the recent amendment to the Federal Acquisition Regulation requiring contractors to self-report certain crimes and violations, to give IGs statutory authority to interview contractor employees without the procedural hurdles of issuing a subpoena.

Section 1515 of ARRA provides that OIGs, with respect to each contract or grant awarded using ARRA funds, are authorized to examine any records that pertain to and involve transactions relating to the contract, subcontract, grant, or subgrant, and "to interview any officer or employee of the contractor, grantee, subgrantee, or agency regarding such transactions." This provision as applicable to contractors has been implemented via an interim rule published at *74_Fed. Reg. 14646* (March 31, 2009), which amended FAR section 52.212-5, Contract Terms and Conditions Required to implement Statutes or Executive Orders – Commercial Items, to provide that Inspectors General shall have access to and the right to (1) examine a contractor's or subcontractor's records that pertain

to, and involve transactions relating to, contracts using Recovery Act funds, and (2) "[i]nterview any officer or employee regarding such transactions."

Similarly, the FAR now requires, in all contracts with a value expected to exceed $5 million and a performance period of at least 120 days, a clause that defines "full cooperation" as providing "government auditors and investigators" with "access to employees with information." 48 CFR 52.203-13(a). These provisions illustrate the movement toward requiring those who obtain federal money to cooperate with oversight bodies. I believe that same logic should be applied to all those who receive federal funds.

Because the ARRA provision authorizing IGs to interview contractor employees is more definitive than the FAR provision – although their intent appears to be the same – I would suggest that extending this ARRA provision to apply to all contracts, not just contracts using Recovery Act funds, would as a practical matter, provide IGs with a statutory basis to interview contractor employees. I believe that most contractors would not act in direct contravention of a statutory requirement; therefore this approach should make it simpler for IGs to interview those contractor employees they need to talk to. This approach would move the issue of interviewing contractor employees out of the subpoena arena to contract enforcement, which presumably would limit or eliminate the concerns about testimonial subpoena authority. Moreover, the logic of granting this authority to IGs for contracts using ARRA funds would apply equally well to all other contracts.

While there are many arguments for extending this approach to subcontractor employees as well, Congress chose, in the ARRA, to give the Government Accountability Office, but not IGs, the authority also to interview any officer or employee of a subcontractor receiving Recovery Act funds. Based on ARRA, I am not proposing extending this authority to subcontractor employees at this time.

I suggest an amendment to the IG Act as follows:

Section 6 of the Inspector General Act, 5 U.S.C. App. 3, is amended—

By adding at the end of subsection (a) the following:

"(10) Whenever in the judgment of the Inspector General it is necessary in the performance of the functions assigned by this Act, (a) to examine any records of any contractor or grantee, and of its subcontractors or subgrantees, or any State or local agency administering a contract, that pertain to, and involve transactions relating to, the contract, subcontract, grant, or subgrant; and (b) to interview any officer or employee of the contractor, grantee, subgrantee, or agency regarding such transactions."

Conclusion

For IGs, access is power. In general, it remains true that knowledge also is power. In our technological age, however, access is necessary for knowledge. Obtaining access to records without delay and not having to "tip off the target," clearly providing for unrestricted read-only access for IGs to all agency information systems, and clarifying the expectation that IGs will have access to contractor employees will go a long way to improving the effectiveness of oversight and protecting the interests of the American taxpayers.

Brian D. Miller

Brian D. Miller was confirmed by the U.S. Senate as the Inspector General of the General Services Administration on July 22, 2005.

As Inspector General, Mr. Miller directs nationwide audits and investigations of federal procurement involving GSA. Mr. Miller is also a member of the Council of the Inspectors General on Integrity and Efficiency and participated in the Department of Justice Hurricane Katrina Task Force. On October 10, 2006, Mr. Miller was named Vice-Chair of the National Procurement Fraud Task Force. Mr. Miller played a leading role in developing a new requirement for contractors to report overpayments and crimes, included in the *Close the Contractor Fraud Loophole Act of 2008*.

In 2007, Mr. Miller was recognized by Ethisphere magazine as the 12th "most influential person in business ethics" by a worldwide panel of experts. In July 2008, Mr. Miller was named among "Those Who Dared: 30 Officials Who Stood Up for Our Country," a special report of Citizens for Responsibility and Ethics in Washington, D.C. a national advocacy organization. In October 2008, Mr. Miller received the Attorney General's Distinguished Service Award.

Mr. Miller earned his law degree from the University of Texas.

[AUDIT]

A Conceptual Framework for Forensic Audit and Automated Oversight

Forensic audit specifically looks for financial misconduct, abusive or wasteful activity using automated audit tools and techniques

By Brett M. Baker

Federal Offices of Inspector General have a significant statutory oversight responsibility of the programs and financial operations administered by their respective agencies. Risk-based audits, evaluations, and investigations are designed to provide coverage of federal outlays exceeding $2 trillion annually. Traditional performance, financial, and financial-related audits provide taxpayers and Congress with greater visibility and transparency of federally funded programs and government operations and reasonable assurance that they are meeting their statutory mission; however, an increasingly automated financial management environment present significant challenges to government managers delivering programs and to Offices of Inspector General providing oversight. Financial and operational processes produce large volumes of data; however, federal agencies have difficulty extracting information and knowledge necessary for decision-makers. The amount of data increases two-fold every year though the capability to transform data into useful decision support information has not kept pace. In addition, OMB estimates that there is $75 billion in improper and erroneous payments made annually which is almost 4 percent of the $2 billion in federal outlays.

Predictive analytics and automated oversight can facilitate a more thorough extraction of information and knowledge for government managers as well as enhance the oversight capabilities of the federal Offices of Inspector General.

Forensic auditing is a discipline available within the Inspector General community that can complement and support traditional audit approaches that commonly use statistical sampling to identify and test a representative group of transactions and project the results to the universe under study. Forensic audit specifically looks for financial misconduct, abusive or wasteful activity using automated audit tools and techniques against financial and operational transaction-level data. In contrast to traditional audit approaches, forensic audit uses a 100 percent review approach where every transaction is examined in an automated manner against pre-defined business rules and fraud indicators.

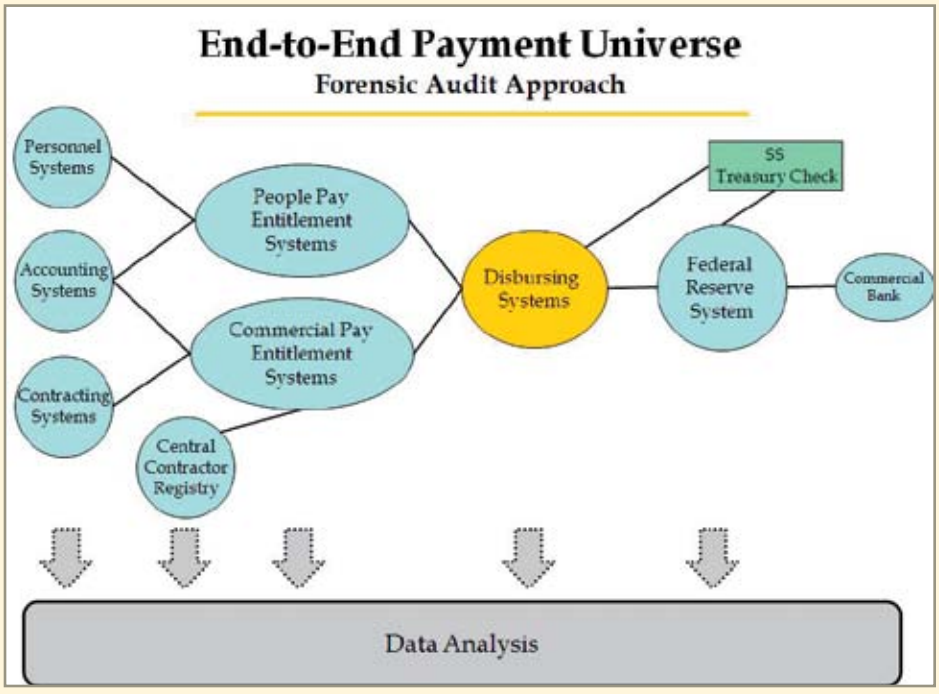
Tools and Techniques

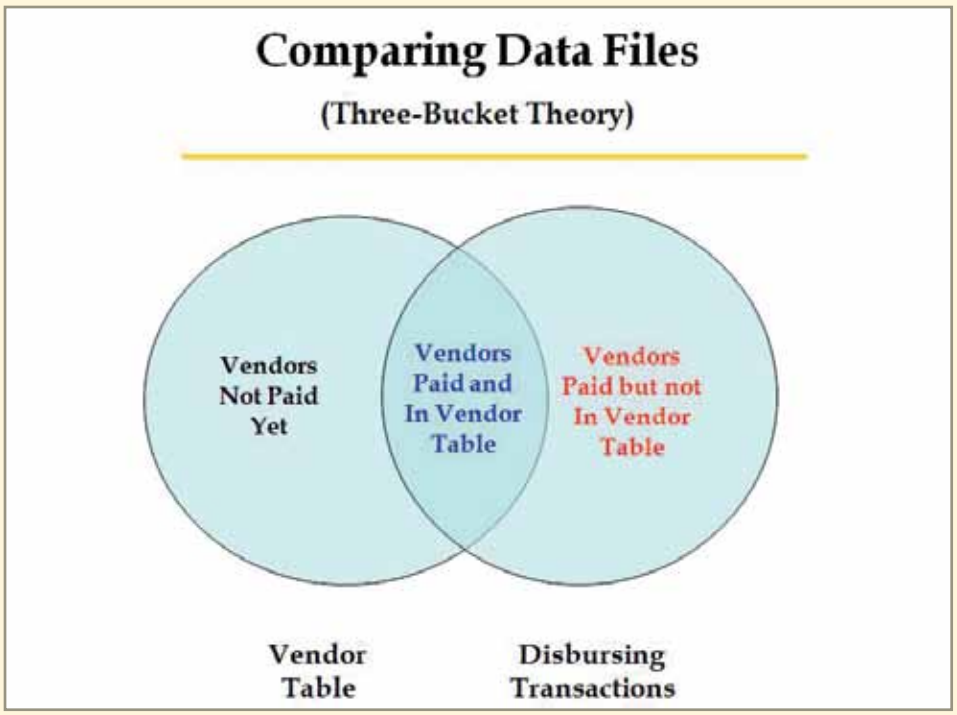
Data analysis software used in audit and investigative organizations have the capability to perform sophisticated comparisons and analyses against a large volume of financial and operational transactions. Forensic data analysis tools are commonly used in the Inspector General community to examine financial and operational transactions. They allow auditors and investigators to identify anomalous activity within a data file and between data files. The tools can provide the users with information about the underlying transactions without applying business rules or fraud indicators. Within a data file users can summarize large volumes of data into more meaningful groups of transactions. For example, millions of purchase card transactions can be summarized to show how many transactions are in each of the merchant category codes to quickly show

groups of potentially improper transactions with prohibited types of vendors. Summarizing financial information on date can help the auditor and investigator show trends in activity over time. Frequency distribution is another powerful tool that can show outliers in financial data that auditors and investigators can target their reviews. Most data have a normal distribution of values, i.e., has the appearance of a Bell Curve. Activity on the ends of the normal distribution of financial activity would show high dollar amounts and zero or even negative values.

Tools such as IDEA and ACL also allow the user to build business rules or fraud indicators to apply against transaction level data. Business rules are calculated fields where the user interrogates and compares various data fields for specific conditions and can be later extracted into a separate data file for more in-depth analysis. For example, in government purchase card transactions, the user can build a business rule into the data analysis tool to flag transactions that are just under the normal purchase card transaction limit of $2500. Another business rule could be to look for credit transactions which normally are for refunds but may be an indicator of potentially inappropriate use by the card holder. Another common feature of data analysis tools is to examine transaction data for duplicates. In a commercial payment environment, business rules can be coded to look for transactions that have the same invoice number, same posting date, same dollar amount, and same contract number to reduce a very large volume of transactions to a much smaller number that can be further researched by the auditors and investigators. Data analysis tools can also extract any discrete portion of a text field so that transactions can be more thoroughly analyzed such as the 4th through 12th characters of a long code that would be the Social Security number. Another example could be for a line of accounting for a commercial payment transaction that can be over 100 characters in length and include contract, payment type, and funding information. Breaking out the specific types of information that is built into a line of accounting allows the user to perform more sophisticated comparative and analytical tests.

Another powerful capability of data analysis tools is the ability to compare separate data files. A common feature to the tools is the join option where two data files can be combined using a linking field. This commonly produces an output file that has transactions that meet one of the following three possibilities: 1) a transaction is in both files, which would be normal if the two data files being compared were from within an end-to-end process; 2) a transaction is in the first file, but not in the second; and 3) the opposite where the transaction is in the second file but not the first. I refer to this as the "three bucket theory." In most financial management processes transactions will pass through the various systems in an end-to-end manner. In comparing two files along the end-to-end process the auditor or investigator would normally find transactions that are in both files under comparison (joined). This is particularly true in a commercial payment environment; however, joining files together will also surface transactions that are in one file but not the other, which may warrant further attention by the auditors and investigators. An example of this can be found in comparing payment files that include vendor identification numbers against a vendor file of valid contractors to ensure improper payments have not been introduced later in the financial process. Again, most transactions in the joined files would be represented in both files. If a vendor is only in the vendor file of valid contractors but not in the payment file then it would normally mean they didn't submit an invoice in the payment file under review. However, if the payment file has a vendor or entity in it that is not in the vendor file of valid contractors then it would likely warrant further research by the auditors or investigators. This can also be done





for bank account information to show changes in bank accounts for a vendor. A sequence of payments to a vendor where the bank account changes from 12345 to 67890 back to 12345 may indicate payments have been redirected by someone other than the vendor without the knowledge of the vendor. Comparing several files in an end-to-end process can help reduce the number of false positives that can arise in forensic analyses. Analysis of only a payment file for duplicate invoices or payment amounts might show a large number of false positives (e.g., transactions that look like duplicates but are actually not.) Comparing the payment file against file extracts from initiating contract and accounting systems can reduce the likelihood of false positives. Beneford's Law can also identify potentially abusive transactions by isolating patterns in numbers that are outside a statistical norm.

Data Analysis vs. Predictive Analytics

Data mining is a set of sophisticated techniques that can find patterns and relationships in data that have not previously been identified. This is a much more advanced level of analysis than the previously described techniques. It is a subset of knowledge discovery in databases, which is the process for preparing data, selecting data mining techniques, and evaluating knowledge discovered through analysis. The extracted knowledge and information can be used by researchers to predict future outcomes or develop ways to classify data, explain existing data, or summarize the contents of voluminous databases that will aid in the overall decision making process.

Data mining is a more knowledge-based, variable application discipline that requires some level of data preparation and cleansing for effective results. SPSS' Clementine, Silicon Graphics' Mineset, IBM's Intelligent Miner, and the SAS Institute's Enterprise Miner are very powerful tools that allow less technical users to perform complex data analysis tasks that would have required an advanced computer science degree to perform only a decade ago – classification, clustering, and visualization. The graphical user interface provided a user-friendly platform for less technical users to take advantage of powerful tools without submitting a data request to a technical computer staff. The visual advantage of the GUI provided even the most technical data mining experts with better analysis options than the text-based predecessors.

Artificial neural networks are information processing techniques that work in a manner similar to the way biological nervous systems process information. The information processing system includes a large number of highly interconnected processing elements (neurons) that can address very targeted analyses. Artificial neural networks "learn" by continuously comparing the processing results against historical patterns and profiles. Neural networks are designed to attack a business problem in a specific manner through a learning process – e.g., pattern recognition or data classification. Neural networks are adaptive in nature in much the same way as biological life forms learn. The most common form of neural networks is supervised learning networks which include a retrieving phase and a learning phase. In contrast, unsupervised learning rules include training data that consists only of input training profiles. The neural networks train in an iterative manner learning and modifying weightings in their algorithms continuously. In addition, obtaining clean data is important to successfully using neural network technology. Missing data values can have a damaging effect on the quality of data mining output. Researchers must engage in time-consuming data cleanup to ensure that the information being mined and analyzed does not contain corrupt data.

Neural networks are designed with three layers of processing – the input layer, hidden layer, and output layer with each layer interconnected, inner woven with its neighbor. Raw data and

information are read into the input layer. The hidden layer activity is driven by the weighting of the connections between the input and hidden layers. Similarly, the weighting of the hidden and output layer interconnections also has bearing on the results. There are two manners in which to architect a neural network – single layer and multi-layer. In the single layer architecture, every node within the neural network is interconnected. In the multi-layer architecture, nodes are numbered by layer. .

Neural networks use an unconventional approach to analyzing data in that instructional algorithms are not known in advance. The application does not follow a set of instructions to perform the analyses. Traditional computer applications follow preprogrammed instructions based on predefined knowledge of the programmers. This is not the case with neural network analyses as the researcher generally does not know what the outcome of the analyses will be (e.g. neural networks learn by continuously self reviewing the results and refining the algorithm weightings and therefore cannot be designed to address a specific business problem.) The examples must be carefully isolated or the neural network may not function properly. Regardless, the neural network process is unpredictable. The power of a neural network is its ability to learn through the training trials (e.g. constant improving and refining.) A common reference to neural networks is the researcher does not need to know the questions to obtain the answers.

"An organization should strive to develop a base level of forensic capability for all auditors and investigators..."

Traditional computer applications use an approach for solving business problems where the instructions must be clear and definable for the program to work properly and receive good results. The results are predictable and in the event that the results are not quite what the researcher anticipated, he or she can review the coding for program inaccuracies that generated the incorrect results. Neural networks do now work in this manner. A common practice is to combine the traditional analysis approaches with neural network analysis where the traditional approach performs a supervised role. Another form of neural network technology is a Kohonen network which include feature maps to imitate brain activity. Kohonen networks perform mostly unsupervised learning and cluster analyses that do not include a hidden layer – there is simply an input layer and an output layer.

Building a Forensic Audit Capability

Building a forensic audit capability within an Office of Inspector General can be thought of on two levels – building an organization-wide forensic capability as well as a more specialized forensic unit. An organization should strive to develop a base level of forensic capability for all auditors and investigators where any team can readily perform data analyses, such as, summarization, file joins, and trend analyses with transaction level data within and between data files as part of an audit or investigation. This requires training on the use of data analysis tools and more importantly to use them on a consistent basis in performing the work. It is helpful to the organization if the tools are available for every auditor and investigator in their workstation. Training opportunities are readily available for the common data analysis tools, including hands-on instruction and professional conferences. Recruiting, training and developmental opportunities for auditors and investigators that promote system savvy, critical thinking, analytical, and business process skills are essential to developing an organization-wide forensic approach. It is also beneficial to develop a more sophisticated forensic

audit capability in an organization that uses sophisticated data mining tools and powerful hardware, such as SQL servers, and access to mainframe applications, to perform the more in-depth data analysis and data mining. Forensic units can also develop a capability to perform continuous monitoring of key financial systems and processes through periodic extractions of data from the systems or embedding query capabilities within the systems.

Forensic Audit Approach

The general approach for performing forensic audit is not dramatically different than a traditional audit approach. Teams develop audit objectives, identify the audit universe, map out the process under review, identify key control points, develop the audit program, collect and test evidence, report the results. The forensic audit approach makes greater use of transaction level data and employs a 100% review process based on data analysis with targeted business rules. A coordinated effort with subject matter experts and investigators provides an integrated approach to examining a process from a forensic perspective. It also important to note that getting data from the financial and operational systems is one of the greatest challenges of forensic auditing. Requests for data should be made very early in the effort and include record layouts and data dictionaries. Mapping the process in forensic auditing is important and should be first done at a high level to show the key processes, controls, and systems in the financial and operational environment under review. This will help the auditors and investigators more readily identify necessary data and show its place in the overall process. When getting data from systems it is best to first obtain a small data file with the necessary fields to review before making a request for larger data files. The forensic audit approach will identify ways to see anomalous activity in management processes using automated oversight techniques. In reporting the results of forensic audit it is beneficial to recommend to management consideration of using those techniques to improve their financial management oversight of a financial or operational area.

Conclusion

The federal financial management and operational environment is increasingly more complex and system oriented at the same time taxpayers and Congress are also seeking a government that is more transparent and accountable. Forensic audit is an approach that integrates audit, evaluation, and investigations in manner that provides Offices of Inspector General with a powerful capability to meet and exceed our statutory oversight mission and help improve government.

Brett M. Baker

Dr. Brett M. Baker is the Assistant Inspector General for Audit with the U.S. Department of Commerce Office of Inspector General with oversight of financial statement, financial-related, acquisition, performance, and forensic audit work of agency operations. Prior to joining Commerce OIG, he was the Director of the Defense Finance and Accounting Service Office of Internal Review with oversight of financial-related, performance, systems, and forensic audits, and investigations of DFAS operations. Before joining DFAS in 2000, Dr. Baker held leadership positions with the U.S. Department of Education OIG. He also served as an instructor with the Inspector Generals' Auditor Training Institute and developed/taught its first Windows-based computer-assisted audit techniques course.

Dr. Baker is a Certified Public Accountant and Certified Information Systems Auditor and the recipient of two President's Council on Integrity and Efficiency Awards for Excellence (1999, 2003). Dr. Baker holds a B.S. in Sociology from Iowa State University and a B.A. in Accounting from the University of Northern Iowa. He also holds an Master's degree in Information Resource Management from Central Michigan University and a doctorate in Information Technology and Systems Management from the University of Maryland. He began his government career with service in the U.S. Army Signal Corps.

[TESTIMONY]

Inspectors General: Independent Oversight of Financial Regulatory Agencies

Congressional testimony before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittee on Government Management, Organization, and Procurement (March 25, 2009)

By Gary L. Kepplinger

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss H.R. 885, *Improved Financial and Commodity Markets Oversight and Accountability Act*. As you know, this proposed legislation recently referred to your subcommittee is intended to enhance the independence of Inspectors General in key financial regulatory agencies including the Board of Governors of the federal Reserve System, the Commodity Futures Trading Commission, the National Credit Union Administration, the Pension Benefit Guaranty Corporation, and the Securities and Exchange Commission. In numerous reports and testimonies over the last several years, we have discussed the key role that IGs play in federal agency oversight.[1]

The *Inspector General Act of 1978*,[2] created offices of Inspector General at major departments and agencies with IGs who are appointed by the President, confirmed by the Senate, and may be removed only by the President with notice to the Congress stating the reasons. The IGs are to prevent and detect fraud and abuse in their agencies' programs and operations; conduct audits and investigations; and recommend policies to promote economy, efficiency, and effectiveness. In 1988, the 1978 IG Act was amended to establish additional IG offices in designated federal entities defined by the Act.[3] Generally, the DFE IGs have the same authorities and responsibilities as those originally established by the IG Act but there is a clear distinction—they are appointed and may be removed by their agency heads rather than by the President and are not subject to Senate confirmation. In the now more than three decades since passage of the IG Act, the IGs have been instrumental in enhancing government accountability.

Our nation is currently in the midst of one of the worst financial crises ever. As we recently reported, the current U.S. financial regulatory system regulators—put into place over the last 150 years—that has not kept pace with major developments in financial markets, products, and associated risks in recent decades.[4] It has become apparent that the U.S. financial regulatory system is ill suited to meet the nation's needs in the 21st century, and significant reforms to the U.S. financial regulatory system

1 GAO, *Inspectors General: Opportunities to Enhance Independence and Accountability*, GAO-07-1089T (Washington, D.C.: July 11, 2007); GAO, *Inspectors General: Proposals to Strengthen Independence and Accountability*, GAO-07-1021T (Washington, D.C.: June 20, 2007); GAO, *Highlights of the Comptroller General's Panel on Federal Oversight and the Inspectors General*, GAO-06-931SP (Washington, D.C.: September 11, 2006); GAO, *Inspectors General: Enhancing Federal Accountability*, GAO-04-117T (Washington, D.C.: October 8, 2003), GAO, *Inspectors General: Office Consolidation and Related Issues*, GAO-02-575 (Washington, D.C.: August 15, 2002).

2 Pub. L. No. 95-452, 92 Stat. 1101 (Oct. 12, 1978) (codified, as amended, at 5 U.S.C. App.).

3 Pub. L. No. 100-504, 102 Stat. 2515 (Oct. 18, 1988) (5 U.S.C. App.).

4 GAO, *Financial Regulation: A Framework for Crafting and Assessing Proposals to Modernize the Outdated U.S. Financial Regulatory System*, GAO-09-216 (Washington, D.C.: Jan 8, 2009).

are critically and urgently needed. We have included modernization of the outdated U.S. financial regulatory system as a high-risk area in our recent report of high-risk designations across the federal government.[5]

Currently, both the administration and the Congress are considering many options aimed at strengthening the financial regulatory system. H.R. 885 would provide for the inspectors general for selected financial regulatory agencies to be appointed by the President with Senate confirmation. Those IGs currently are appointed by their agency heads and may be removed by their agency heads.

Today, I will discuss (1) the legislative proposals in H.R. 885, (2) the key principles and importance of auditor and IG independence, and (3) current coordination mechanisms in place for IG offices. My testimony today draws primarily on prior GAO reports and testimonies conducted in accordance with generally accepted auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Provisions of H.R. 885

Currently, the IGs at the federal Reserve Board, Commodity Futures Trading Commission, Securities and Exchange Commission, National Credit Union Administration, and the Pension Benefit Guaranty Corporation are appointed to their offices by their agency heads and may be removed from office by their respective agency heads. H.R. 885, *Improved Financial and Commodity Markets Oversight and Accountability Act*, would provide for the conversion of these IGs from appointment by their respective agency heads to appointment by the President with confirmation by the Senate. Likewise, after this conversion, these IGs may be removed only by the President with advance notification to the Congress of the reasons. We believe that the differences in the appointment and removal processes between presidentially appointed IGs and those appointed by their agency heads result in a clear difference in the level of independence of the IGs. A general tenet to keep in mind is that the further removed the appointment source is from the entity to be audited, the greater the level of independence.

In the past, the Congress has taken actions to convert IGs from appointment by their agency heads to appointment by the President with Senate confirmation as a way to enhance IG independence. For example, on the heels of the savings and loan and banking crisis, over two decades ago, the role of the federal Deposit Insurance Corporation's IG became increasingly important in providing oversight. Due to the perceived limitation of the FDIC IG's independence resulting from agency appointment, the Congress converted the IG from agency appointment to appointment by the President with Senate confirmation.[6] In another example, the Congress took action to convert the Tennessee Valley Authority IG to appointment by the President with Senate confirmation because of concerns about interference by TVA management.[7] In both cases, Congress recognized that the IG's independence would be enhanced by the presidential appointment. The change from agency appointment to appointment by the President has been recognized by Congress since the advent of the IG concept as strengthening the critical element of IG independence. As we have noted in prior reports and testimony, we believe independence is one of the most important elements of an effective IG function.

Auditor and IG Independence

We believe that the differences in the appointment and removal processes between presidentially appointed IGs and those appointed by agency heads result in a clear difference in the organizational independence of the IGs. The IG Act, as amended (IG Act),[8] requires IGs to perform audits in compliance with *Government Auditing Standards*[9] and authorizes IGs to conduct inspections and investigations.[10] These standards recognize the methods for external appointment and removal of the IG as key independence considerations to enable internal IG offices to report their work externally. Those offices with IGs appointed by the President are more closely aligned with the independence standards for external audit organizations,[11] while those offices with IGs appointed by the agency head are more closely aligned with the independence standards for internal audit

5 GAO, High –Risk Series: An Update, GAO-09-271 (Washington, D.C.: January 2009).

6 Resolution Trust Corporation Completion Act, Public Law 103-204, Dec. 17, 1993.

7 Pub. L. No. 106-422, 114 Stat. 1872 (Nov. 1, 2000).

8 Codified at 5 U.S.C. App.

9 GAO, *Government Auditing Standards, July 2007 Revision*, GAO-07-731G (Washington, D.C.: July 2007), issued by the Comptroller General of the United States.

10 Professional standards for the IGs have been issued by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency.

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

organizations.[12]

In 1988, IG Act amendments created the DFE IGs, including those covered by H.R. 885, with a clear distinction in their appointment—they are appointed and removed by their entity heads rather than by the President and are not subject to Senate confirmation. Organizational independence differs between the offices of presidentially appointed IGs and other IGs who are agency appointed. The DFE IGs, while generally covered by many of the same provisions of the IG Act as the IGs appointed by the President with Senate confirmation, are more closely aligned to independence standards for internal auditors than to those for external auditors. At the statutory safeguards exist for DFE IG independence for reporting externally. These safeguards include establishment of the IG by statute, communication of the reasons for removal of the head of an audit organization to the cognizant legislative oversight body, statutory protections that prevent the audited entity from interfering with an audit, statutory requirements for the audit organization to report to a legislative body on a recurring basis, and statutory access to records and documents related to agency programs.

Independence is one of the most important elements of an effective IG function. In fact, much of the IG Act provides specific protections to IG independence that are unprecedented for an audit and investigative function located within the organization being reviewed. These protections are necessary in large part because of the unusual reporting requirements of the IGs, who are both subject to the general supervision and budget processes of the agencies they audit, and also expected to provide independent reports of their work externally to the Congress and the public.

Independence is also the cornerstone of professional auditing. Without independence, an audit organization cannot fully provide independent audits, perspectives, and assessments. Likewise, an IG who lacks independence cannot effectively fulfill the full range of requirements for the office. Lacking this critical attribute, an audit organization's work might be classified as studies, research, consulting, or reviews, rather than independent audits.

Government Auditing Standards states, "In all matters relating to the audit work, the audit organization and the individual auditor, whether government or public, must be free from *personal, external, and organizational* impairments to independence, and must avoid the appearance of such impairments to independence. Auditors and audit organizations must maintain independence so that their opinions, findings, conclusions, judgments, and recommendations will be impartial and be viewed as impartial by objective third parties with knowledge of the relevant information."

- **Personal independence** applies to individual auditors at all levels of the audit organization, including the head of the organization. Personal independence refers to the auditor's ability to remain objective and maintain an independent attitude in all matters relating to the audit, as well as the auditor's ability to be recognized by others as independent. The auditor needs an independent and objective state of mind that does not allow personal bias or the undue influence of others to override his or her professional judgments. This attitude is also referred to as intellectual honesty. The auditor must also be free from direct financial or managerial involvement with the audited entity or other potential conflicts of interest that might create the perception that the auditor is not independent.
- **External independence** refers to both the auditor's and the audit organization's freedom to make independent and objective judgments free from external influences or pressures. Examples of impairments to external independence include restrictions on access to records, government officials, or other individuals needed to conduct the audit; external interference over the assignment, appointment, compensation, or promotion of audit personnel; restrictions on funds or other resources provided to the audit organization that adversely affect the audit organization's ability to carry out its responsibilities; or external authority to overrule or to inappropriately influence the auditors' judgment as to appropriate reporting content.
- **Organizational independence** refers to the audit organization's placement in relation to the activities being audited. Professional auditing standards have different criteria for organizational independence for external and internal audit organizations. The IGs, in their statutory role of providing oversight of their agencies' op-

12 Under internal auditing standards, internal auditors are generally limited to reporting internally to the organization that they audit, except when certain conditions are met, such as when mandated by statutory or regulatory requirements. (See the Institute of Internal Auditors, International Professional Practices Framework (Almonte Springs, Fla: Jan. 2009).Internal audit organizations are organizationally placed within the organization they audit and are defined as being organizationally independent under professional auditing standards if the head of the audit organization (1) is accountable to the head or deputy head of the government entity or to those charged with governance; (2) reports audit results both to the head or deputy head of the government entity and to those charged with governance; (3) is located organizationally outside the staff or line-management function of the unit under audit; (4) has access to those charged with governance; and (5) is sufficiently removed from political pressures to conduct audits and report findings, opinions, and conclusions objectively without fear of political reprisal.

erations, represent a unique hybrid of external and internal reporting responsibilities. The implementation of the IGs' reporting relationships with their respective agency heads can also significantly affect the independence of the IGs. Generally, the IGs represent a hybrid of external auditing and internal auditing in their oversight roles for federal agencies. The IG offices, having been created to perform a unique role in overseeing federal agency operations, have characteristics of both external audit organizations and internal audit organizations. For example, the IGs have external reporting requirements consistent with the reporting requirements for external auditors, while at the same time they are part of their respective agencies.

IGs also have a dual reporting responsibility to the Congress and their agency heads. The IGs' external reporting requirements in the IG Act include reporting the results of their work in semiannual reports to the Congress. Under the IG Act, the IGs are to report their findings without alteration by their respective agencies, and public reports are to be made available on each IG's website. The IG Act also directs the IGs to keep agency heads and the Congress fully and currently informed of any problems, deficiencies, abuses, fraud, or other serious problems relating to the administration of programs and operations of their agencies. Also, the IGs are required to report particularly serious or flagrant problems, abuses, or deficiencies immediately to their agency heads, who are required to transmit the IG's report to the Congress within 7 calendar days.

The IG Act also provides specific protections to IG independence, including a prohibition on the ability of the agency head to prevent or prohibit the IG from initiating, carrying out, or completing any audit or investigation. This prohibition is directed at helping to protect the IG office from external forces that could compromise independence. The IG's personal independence and the appearance of independence to knowledgeable third parties is also critical when the IG makes decisions related to the nature and scope of audit and investigative work performed by the IG office. The IG must determine how to utilize the IG Act's protection of independence in conducting and pursuing the audit and investigative work. The IG's personal independence is necessary to make the proper decisions in such cases.

The IG Act provides the IGs with protections to external independence by providing access to all agency documents and records; prompt access to the agency head; the ability to select and appoint IG staff; the authority to obtain services of experts; and the authority to enter into contracts. The IG may choose whether or not to exercise the Act's specific authority to obtain access to information that is denied by agency officials. Again, each IG must make decisions regarding the use of the IG Act's provisions for access to information, and the IG's personal independence becomes key in making these decisions.

The *IG Reform Act of 2008*, enacted on October 14, 2008, amends the IG Act to further enhance the independence of the IGs, among other things.[13] To illustrate, the 1978 IG Act requires that the IGs nominated by the President be selected without regard to political affiliation and solely on the basis of integrity and defined abilities. However, these criteria were not included as a provision in the legislation that created the DFE IGs. The Reform Act extends these qualification criteria to apply also to the selection of the DFE IGs. In addition, the enhanced by changes to the timing of notification to Congress of an IG removal or transfer—to at least 30 days before any planned removal of an IG under the IG Act, rather than merely an after-the-fact notice of prior removal.

IG Coordination

Prior to the passage of the IG Reform Act in 2008, the IGs' coordinating structure included two separate administratively established organizations: the IGs appointed by the President with Senate confirmation belonged to the President's Council on Integrity and Efficiency, and the DFE IGs formed the Executive Council on Integrity and Efficiency. Both councils have been chaired by the Deputy Director for Management in the Office of Management and Budget and were established by Executive Order to coordinate the IGs' activities across the government.[14] In our 2002 report, we had suggested that the Congress consider establishing an IG council by statute that includes stated roles and responsibilities, designated funding sources, and provisions for coordination with other federal oversight organizations.[15]

The IG Reform Act created an independent establishment in the executive branch, called the Council of IGs on Integrity and Efficiency, to replace the PCIE and ECIE, and to aid the IG community and foster government wide efforts to coordinate and improve oversight. This includes the establishment of a revolving fund to be used for council functions and duties with amounts in the fund coming from executive branch agencies. This new IG coordinating

13 Many of the provisions in the Reform Act were discussed by a panel hosted by the Comptroller General during May 2006. The discussion included the appointment and removal of IGs, an IG council established by statute, and areas related to IG independence and effectiveness. See GAO-06-931SP.

14 The IG Act has required IGs to coordinate with the Comptroller General to avoid duplication and ensure effective coordination and cooperation. 5 U.S.C. App. § 4(c).

15 GAO, *Inspectors General: Office Consolidation and Related Issues*, GAO-02-575 (Washington, D.C.: Aug. 15, 2002).

structure is to become effective 180 days after the date the Reform Act became law.

Other recent efforts involve the coordination of financial regulatory IGs. On October 3, 2008, the President signed into law the *Emergency Economic Stabilization Act of 2008*, which established the Office of Financial Stability within the Department of the Treasury and authorized the Troubled Asset Relief Program. The Special IG for TARP, created by EESA, who is appointed by the President with Senate confirmation, has announced efforts to coordinate with other IGs who operate in areas related to TARP activities. The coordination group referred to as the TARP-IG Council was established administratively by the SIG TARP and includes the IGs at the federal Reserve Board, the federal Deposit Insurance Corporation, the federal Housing Finance Agency, the Securities and Exchange Commission, the Department of Housing and Urban Development, the Department of the Treasury, and the Treasury IG for Tax Administration, as well as representatives from GAO. The TARP-IG Council seeks to coordinate the activities of the IGs, establish protocols, and share ideas for comprehensive audits and investigations, while avoiding unnecessary or duplicative burdens on those charged with managing TARP.

The SIG TARP also announced the formation of a broad, multi agency task force designed to deter, detect, and investigate instances of fraud in the federal Reserve's Term Asset-Backed Securities Loan Facility program, which is intended to make credit available to consumers and small businesses. The task force was created in coordination with the federal Reserve Board IG and will include the federal Bureau of Investigation, the Financial Crimes Enforcement Network, U.S. Immigration and Customs Enforcement, the Internal Revenue Service's Criminal Investigation, the Securities and Exchange Commission, and the U.S. Postal Inspection Service.

With the growing complexity of the federal government, the severity of the problems it faces, and the fiscal constraints under which it operates, it is important that independent, objective, and reliable IG structures be in place at federal agencies to ensure adequate audit and investigative coverage of federal programs and operations. The current crisis in the financial markets is illustrative of the significant challenges facing the federal government. As the administration and the Congress continue to take actions to address the immediate financial crisis, creating a regulatory system that reflects new market realities is a key step to reducing the likelihood that the United States will experience another financial crisis and enhancing oversight of the direction and implementation of current initiatives. As a result, considerable debate is under way over whether and how the current regulatory system should be changed, including calls for consolidating regulatory agencies, broadening certain regulators' authorities, or subjecting certain products or entities to more regulation. Strong independent oversight and accountability functions of the inspectors general at the regulatory agencies will be an important element of this reform.

Coordination of the financial regulatory agencies' IGs is especially important during the current financial crisis. The fragmented and complex arrangement of federal and state regulators makes the communication and coordination of IGs at the regulatory agencies challenging but critical to providing effective oversight as significant reforms in the U.S. financial regulatory system evolve.

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

Gary L. Kepplinger

Gary L. Kepplinger was appointed General Counsel of the U.S. Government Accountability Office in 2006 and retired from GAO in May 2009. He served as the Deputy General Counsel from 2001 to 2006 and the Managing Associate General Counsel responsible for GAO's accounting, appropriations, information management, and special investigations matters from 1988 to 2001.

Since joining GAO's Office of General Counsel in 1975, Mr. Kepplinger had a distinguished career working on a wide variety of issues ranging from public land and environmental issues to supporting the Comptroller General as a member of the Chrysler Loan Guarantee Board and the United States Railway Association (Conrail). In addition, Mr. Kepplinger had served as the editor for the second edition of GAO's four-volume publication, *Principles of Federal Appropriations Law*. He had been a frequent speaker, writer, and instructor on appropriations law matters. His latest contribution was an analysis of the appropriation and accounts clause of the Constitution in *The Heritage Guide to the Constitution*.

Mr. Kepplinger received a B.A. degree from George Washington University and his law degree magna cum laude from DePaul University College of Law. He is a member of the bars of Illinois, Virginia and the United States Supreme Court.

[TESTIMONY]

Progress of the American Recovery and Reinvestment Act

Congressional testimony before the U.S. Senate, Committee on Homeland Security and Governmental Affairs (April 2, 2009)

By Inspector General Earl E. Devaney

Mr. Chairman and members of the Committee, I want to thank you for the opportunity to testify today. I have had the honor of testifying before this Committee in the past as the Inspector General of the Department of the Interior. As you all know, the President has recently appointed me to chair the Recovery Accountability and Transparency Board (the Board), and it is in that capacity that I appear before you today. My testimony will address the current status and mission of the Board, and after I make my opening remarks, I will be glad to answer any questions you have for me.

I am pleased to tell you that the Board has recently obtained office space and continues to acquire a staff of highly skilled oversight and IT professionals. Our first Board meeting was held last week, and we have set in motion a number of initiatives to ensure that the Board fulfills all of its responsibilities under the *American Recovery and Reinvestment Act of 2009* (the Recovery Act or Act).

The Members of the Board and I view the Board as having a dual mission. First, the Board is responsible for establishing and maintaining a website, the purpose of which is not only to foster historic levels of transparency of Recovery funds but to do so in a user-friendly manner. Second, the Board will coordinate and conduct oversight of Recovery funds to prevent fraud, waste or abuse.

Even before the Recovery Act was signed into law by the President, the Office of Management and Budget and the General Services Administration had begun designing the architecture and creating the implementation plan for the website. A great deal of credit must be extended to OMB and GSA for their efforts to launch this website. Because of their efforts, all Americans can visit the website today at Recovery.gov. However, I think it is important to point out that the creation of this website is an evolving process with multiple phases. It is not a single event.

As you know, the Recovery Act vests the Board with the authority to maintain this website. Now that the first phase of getting Recovery.gov up and running has ended, I am eager for the Board to start the second phase of development: The Board will begin to manage the Web site's design and content, OMB will retain responsibility for the reporting guidance and the collection and verification of data, and GSA will continue to host the website. I am confident that this division of labor will provide the best opportunity to maximize Recovery.gov's use as a transparency and accountability tool, and I am equally confident that we will also have the opportunity to achieve an unprecedented level of citizen participation.

The Board is in the process of obtaining an outside source to conduct an Independent Verification and Valida-

tion – referred to as an IV&V – to assess the current state of Recovery.gov. We have also tentatively decided to hold an electronic town hall where the Board and OMB will be able to solicit advice and ideas from the public on new technologies that can help us collect and array data regarding Recovery funds in an innovative way. Soon after this public event, we will conduct a competitive process to select a vendor or vendors to help us build the type of historic website envisioned under the Recovery Act.

Mr. Chairman, I believe James Madison was correct when he said, "A popular government without proper information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or, perhaps, both." The words of Madison lead me to conclude that the information on Recovery.gov must be easily retrievable and understood by taxpayers, lawmakers and watchdog groups alike and that citizens must be given the opportunity to provide feedback to their government. Indeed, I am excited about the prospect of heightened citizen participation being a force multiplier for Inspectors General along with the likely benefit of it helping to drive self-correcting behavior.

Regarding the other half of the Board's dual mission – accountability – there is also recent news. IGs across the federal government have developed multiple strategies to help prevent fraud, waste or abuse of Recovery funds. In fact, the Committee recently heard testimony about some of these preventive strategies from the Chair of the Council of the Inspectors General on Integrity and Efficiency, Phyllis Fong. While it is not my intention to repeat them all again today, I can tell you that the IGs are quickly transforming those strategies into real action. For example, at least six IGs have already conducted reviews of previously unimplemented IG or Government Accountability Office recommendations. These reviews will allow their departments to take corrective actions to ensure that effective controls are in place for handling Recovery funds.

The Department of the Interior Office of Inspector General has developed a risk-based model to use in conjunction with Recovery funds going into grants and is now assisting that Department to develop its own risk model for grants, with the hope of extending the model to contracts and cooperative agreements. The Department of Energy Office of Inspector General has completed 30 fraud awareness briefings nationwide involving more than 2,000 attendees. Several other IGs have audits and evaluations that are about to be released which will include recommendations that will be particularly helpful to their departments for Recovery Act activities.

At our first Board meeting last week, both Phyllis Fong and I supported the Board's decision to form a new Recovery Funds Working Group which will be co-chaired by Board Member Calvin Scovel, the IG at the Department of Transportation, and a member of the Board's staff, former IG John Higgins. The purpose of this Working Group will be to ensure the maximum level of coordination and cooperation among IGs necessary to prevent fraud, waste and abuse.

Mr. Chairman, you and the Members of the Committee may have noticed that I have been using the word "prevent" to help describe the Board's mission of accountability. That is very deliberate on my part.

Most IGs, including myself, generally spend considerable time detecting fraud or waste and then examining such fraudulent or wasteful activities through either a traditional audit or criminal investigation. It strikes me that, although those traditional tools will undoubtedly serve an essential purpose once Recovery funds have been awarded and as they are being spent, IGs may be better able to maximize their value to the accountability goal of the Recovery Act by first concentrating their efforts on prevention. The language of the Recovery Act strongly suggests that IGs and other oversight entities are being asked to minimize the risks inherent in distributing such an extraordinary amount of

money and to maximize the opportunities to prevent waste or fraud in the first instance, before it happens.

I foresee the Board actively detecting fraud trends, identifying best practices for conducting reviews, and designing risk-based strategies to help focus the oversight community's limited resources. The new Recovery Funds Working Group will also serve as a catalyst for an unprecedented leveraging of resources. We will also work closely with the Department of Justice to ensure that when fraud is detected - a swift, coordinated process will follow.

In addition, I can assure each of you that the Board will strive to be as helpful as possible to state and local governments. To that end, the Board's staff will include audit, investigative, procurement and intergovernmental professionals who, as a key part of their job descriptions, will be responsible for fostering a close working relationship with all of our oversight partners. Clearly, for the Board to accomplish its mission of accountability, we will need to ensure open communications and frequent interactions with state and local auditors, as well as with the GAO.

Finally, I would like to present some of the impending challenges that I see as having the most impact upon the Board and its missions of transparency and accountability. First and foremost is the matter of data quality. Simply stated, the federal government's systems have never been fully successful at producing timely and reliable data. Add to that problem the difficulty of transmitting and reporting data up through multiple layers of government, as the Recovery Act contemplates, and you begin to understand the basis for my concern.

Second to data quality is the lack of an adequate number of procurement professionals at all levels of government. Federal agencies, in particular, will have great difficulty attracting and hiring enough procurement professionals to minimize the risks associated with moving this amount of money quickly to accomplish the Act's goals. As you may know, the Act calls for the Board to review whether or not there are sufficient qualified acquisition and grant personnel overseeing Recovery funds and whether they have received adequate training. My staff has already begun the process of doing this review, and I was particularly encouraged by the news that the Office of Personnel Management has tentative plans to hold a multi-agency job fair to help agencies with their human resource needs in this arena.

Finally, I am concerned there may be a naïve impression that, given the amount of transparency and accountability called for by this Act, little to no fraud or waste will occur. I am afraid that my 38 years of federal enforcement experience informs me that some level of waste or fraud is, regrettably, inevitable. Obviously, the challenge for those of us charged with oversight will be to significantly minimize any such loss. My promise to this Committee today is that my staff, the members of the Board, and I will work tirelessly to reduce those losses to the lowest level possible.

Mr. Chairman and members of the Committee, that concludes my prepared testimony. Thank you for this opportunity. I will be glad to answer any questions you might have.

Earl E. Devaney

Earl E. Devaney is the Chairman of the Recovery Board, which is charged with overseeing spending under the $787 billion program. In announcing Devaney's appointment, the President said: "Earl has doggedly pursued waste, fraud and mismanagement. He has the reputation of being one of the best [Inspectors General] that we have in this town…. I can't think of a more tenacious and efficient guardian of the hard-earned tax dollars the American people have entrusted us to wisely invest."

President Bill Clinton appointed Mr. Devaney as the Inspector General of the Department of the Interior in 1999.

Before becoming the Inspector General of the Department of the Interior, Mr. Devaney spent eight years as the Director of the Office of Criminal Enforcement, Forensics and Training for the Environmental Protection Agency. In 1998, he received the Meritorious Presidential Rank Award for outstanding government service.

Mr. Devaney began his federal law enforcement career with the Secret Service in 1970, following his graduation from Franklin and Marshall College. At the time of his retirement from the Secret Service in 1991, Mr. Devaney was Special Agent in Charge of the fraud division and was recognized as an international expert in white collar crime.

[TESTIMONY]

Health Care Reform: Opportunities to Address Waste, Fraud, and Abuse

Congressional testimony before the U.S. House of Representatives , Energy and Commerce Committee, Subcommittee on Health (June 25, 2009)

By Inspector General Daniel R. Levinson

Good morning Chairman Pallone, Ranking Member Deal, and distinguished members of the Subcommittee. I am Daniel Levinson, Inspector General of the U.S. Department of Health and Human Services. In the context of current discussions about health care reform, it is critical that the Government pursue a comprehensive strategy to combat fraud, waste, and abuse to ensure that federal health care programs remain solvent and best serve the needs of beneficiaries. I thank you for the opportunity to discuss the Office of Inspector General's work in this area.

OIG has devoted considerable resources toward fighting fraud, waste, and abuse involving HHS's federal health care programs. We have performed evaluations, investigations, and audits on a wide variety of issues, including fraudulent activity by health care providers; excessive payments for medical services, equipment, and prescription drugs; and financial conflicts of interests within the institutions charged with protecting the health of the American public.

Through this work, we have helped identify and recover billions of dollars in fraudulent, abusive, or wasteful payments and also raised awareness of these critical issues among policy makers, government agencies, and the health care community at large. We have recommended improvements to program safeguards and payment methodologies to prevent fraud, waste, and abuse and to ensure health care quality and beneficiary safety. We have also reached out to the health care community to promote compliance. Moving forward, OIG is committed to building on our successes and achieving even greater results in protecting the integrity of government health care programs and the health and welfare of people served by them.

In my testimony this morning, I will begin by describing OIG's unique role in combating fraud, waste, and abuse in Medicare and Medicaid. I then will provide an overview of vulnerabilities in these programs and discuss current initiatives that expand our efforts to identify, investigate, and prosecute health care fraud. Finally, I will discuss OIG's "Five Principles" strategy for combating fraud, waste, and abuse, which we believe are applicable to any health care program.

OIG's Role and Partners in Combating Fraud, Waste and Abuse

OIG is an independent, nonpartisan agency committed to protecting the integrity of the more than 300 programs administered by HHS. OIG's mandate is to protect the integrity of the programs ohms, as well as the health and welfare of the beneficiaries of those programs. Thanks to the work of our 1,500 employees and our law enforcement partners, from FY 2006 through FY 2008, OIG's investigative receivables averaged $2 billion per year and our audit disallowances resulting from Medicare and Medicaid oversight averaged $1 billion

per year. The result was a Medicare and Medicaid-specific return on investment of $17 to $1 for OIG oversight. In addition, in FY 2008, implemented OIG recommendations resulted in $16 billion in savings and funds put to better use.

Further, as reflected in OIG's Semiannual Report to Congress released earlier this month, OIG's expected recoveries for the period of October 2008 through March 2009 include $274.8 million in audit disallowances and $2.2 billion in investigative receivables, which includes nearly $552 million in non-HHS receivables resulting from OIG work (e.g., the States' share of Medicaid restitution).

It comes as no surprise that the large federal government expenditures on health care programs attract individuals and entities seeking to exploit the health care system for their own financial gain. The National Health Care Anti-Fraud Association estimates conservatively that at least 3 percent of health care spending is lost to fraud. In FY 2009, Medicare is expected to cover an estimated 45.5 million beneficiaries at a total cost of$486 billion to the federal government and Medicaid is expected to cover an estimated 51 million beneficiaries and cost the federal government over $217 billion. Though the vast majority of health care providers and suppliers are honest and well intended, even a small percentage of providers and suppliers intent on defrauding the programs can have significant detrimental effects. Although it is not possible to measure precisely the extent of fraud in Medicare and Medicaid, virtually everywhere we look OIG continues to find fraud, waste, and abuse in these programs. Therefore, OIG works closely with HHS officials, the Department of Justice, other agencies in the Executive Branch, Congress, and States to bring about systemic changes in program operations, successful prosecutions, negotiated settlements, and recovery of funds.

Collaboration and innovation are essential in the fight against fraud. On May 20, 2009, HHS Secretary Kathleen Sebelius and Attorney General Eric Holder announced a new initiative to marshal significant resources across the Government to prevent health care waste, fraud, and abuse; crack down on fraud perpetrators; and enhance existing partnerships between HHS and DOJ to reduce fraud and recover taxpayer dollars. To further this effort, the Secretary and Attorney General created the Health Care Fraud Prevention and Enforcement Action Team joint task force consisting of senior level leadership from both departments.

Among other activities, HEAT is building on the successful OIG-DOJ Medicare Fraud Strike Force initiated in south Florida, discussed in greater detail later, by expanding Strike Forces to other metropolitan areas across the country. These Strike Forces use advanced data analysis techniques to identify criminals operating as health care providers and detect emerging or migrating fraud schemes.

HEAT is also focusing on prevention strategies to combat health care fraud. For example, HEAT will expand a Centers for Medicare and Medicaid Services demonstration project in south Florida that uses site visits to potential durable medical equipment suppliers to ensure that applicants are legitimate businesses, not criminals. HEAT also plans to enlist health care providers in the fight against fraud by increasing training about program requirements and effective compliance measures that help ensure integrity of billing practices.

Strike Force activities are one part of the government's enforcement efforts; OIG also works with our law enforcement partners to pursue other criminal cases as well as civil and administrative cases. In FY 2008, OIG investigations resulted in 455 criminal actions against individuals or entities that engaged in crimes against departmental programs and 337 civil and administrative actions, which included *False Claims Act* and unjust enrichment lawsuits filed in federal district court, Civil Monetary Penalties Law settlements, and administrative recoveries'
related to provider self-disclosure matters. Also in FY 2008, OIG excluded from the federal health care programs 3,129 individuals and entities for fraud or abuse that affected federal health care programs and/or beneficiaries.

The collaborative antifraud efforts of HHS and DOJ are rooted in the *Health Insurance Portability and Accountability Act of 1996*, P. L. 104-191, which directed the Secretary of HHS, acting through OIG and the Attorney General, to promulgate a joint Health Care Fraud and Abuse Control Program. The HCFAC Program and Guidelines went into effect on January 1, 1997. HIP AA requires HHS and DOJ to report annually to Congress on HCFAC Program results and accomplishments. HCFAC activities are supported by a dedicated funding stream within the Hospital Insurance Trust Fund.

In its 11th year of operation, the HCFAC continues to demonstrate the success of a collaborative approach to identify and prosecute health care fraud, prevent future fraud and abuse, and protect Medicare and Medicaid beneficiaries. Since its inception, HCFAC activities have returned over $11.2 billion to the Medicare Trust Fund. As I will discuss, the Government's efforts to address DME and infusion fraud in south Florida illustrate the benefits of a collaborative approach. Although I will highlight efforts focused on DME and infusion fraud in particular geographic hot spots, fraud, waste, and abuse occur

among all types of health care providers and suppliers and can affect all types of services covered by Medicare and Medicaid in all geographic areas.

Vulnerabilities in Federal Health Care Programs

Strike Force Activities Have Uncovered Numerous Program Vulnerabilities

OIG and our law enforcement partners are focusing antifraud efforts in geographic areas at high risk for Medicare fraud. In 2007, OIG and DOJ launched a Strike Force effort in south Florida consisting of staff from OIG, DOJ, the U.S. Attorney's Office for the Southern District of Florida, the Federal Bureau of Investigation, and CMS to identify, investigate, and prosecute DME suppliers and infusion clinics suspected of Medicare fraud. Building on the success in south Florida, the Strike Force was expanded to Los Angeles in March 2008 and to Houston and Detroit in May 2009 in connection with the HEAT initiative.

The Strike Force model has proven highly successful. To date, the south Florida Strike Force has opened 161 cases, convicted 151 of its targets, and secured $187 million in criminal fines and civil recoveries. In addition to prosecuting criminals and recovering funds for the Medicare Trust Fund, the south Florida Strike Force has had a powerful sentinel effect. Medicare claims data show that during the first 12 months of the Strike Force (March 1,2007, to February 29, 2008), claim amounts submitted for DME in south Florida decreased by 63 percent to just over $1 billion from nearly $2.76 billion during the preceding 12 months.

In March 2008, DOJ and OIG established a second Strike Force in Los Angeles. Since operations began, the Los Angeles Strike Force has opened 48 cases and is targeting individuals and organizations that have submitted fraudulent claims to the Medicare program. The schemes include false claims for wheelchairs, orthotics, and other DME that was medically unnecessary and/or was not provided to the beneficiaries identified in claims.

The recent Strike Force investigation and prosecution of Medcore Group LLC and M&P Group of South Florida illustrate key vulnerabilities in the Medicare program. Medcore and M&P operated as Miami-based HIV clinics from approximately 2004 through 2006, billed approximately $5.3 million to the Medicare program, and received payments of more $2.5 million. From their inception, Medcore and M&P were set up as criminal enterprises designed to defraud Medicare. The scheme was to submit claims for medically unnecessary HIV infusion and injection treatments. The three owners of Medcore and M&P included a former gas station attendant, a trained cosmetologist, and an individual currently incarcerated for Medicare fraud involving a separate DME company he operated from 2001 to 2003. None had a medical background.

At trial, one of Medcore's owners, Tony Marrero, testified that the scheme was so profitable so quickly that he became concerned about getting caught and decided to set up a second fraudulent clinic, M&P, in the name of his wife. M&P was located in the same building as Medcore, had the same employees, submitted claims under the Medicare provider number of the same physician, and submitted claims on behalf of six of the same patients. In fact, the same physician was associated with other Miami-area infusion clinics, which billed Medicare for more than $60 million between 2004 and the end of 2005.

Mr. Marerro also testified at trial that he had an arrangement with a pharmaceutical wholesale company to buy invoices that showed the purchase of large amounts of medications, when only small amounts were actually purchased. One of the medical assistants testified that she manipulated the patients' blood samples to ensure that laboratory results would appear to support the Medicare claims.

Like many infusion fraud schemes, Medcore and M&P gained the cooperation of patients by giving them kickbacks of up to $200 per visit. Four patients testified that they took kickbacks and never received any medication at the clinics. One patient testified that he used his payments from the clinics to support his cocaine addiction. Another patient testified that he did not have HIV, even though the clinics' documents showed that he was being infused with medication to treat HIV. By the patients' own admission, they had been receiving kickbacks from numerous Miami clinics for many years. On March 17, 2009, a federal jury in Miami convicted two physicians and two medical assistants who worked for Medcore and M&P in connection with the fraud scheme. The Government obtained 6 pleas before trial, resulting in 10 convictions in total.

OIG's fraud-fighting efforts in south Florida also draw on the expertise of our auditors and evaluators. For example, OIG identified weaknesses in Medicare's supplier enrollment process and its supplier oversight activities. In 2006, OIG conducted unannounced site visits to 1,581 DME suppliers in south Florida and found that 31 percent, i.e., 491 suppliers, did not maintain physical facilities or were not open and staffed during business hours, contrary to Medicare requirements. The 491 suppliers were referred to CMS so that CMS could consider revoking their billing privileges, which it subsequently did. Billing privileges were reinstated by hearing officers for 222 of the 243 suppliers who appealed. Subsequently, 74 percent of the suppliers whose billing privileges were reinstated by hearing officers (165 of

222) had their privileges revoked again or inactivated by CMS. Between April and September 2007, the U.S. Attorney's Office indicted 18 individuals connected to 15 of the 222 reinstated suppliers. As of April 2008, 10 of the 18 individuals had been convicted, sentenced to jail terms, and ordered to pay restitution. Six of the eight remaining individuals have since been sentenced to jail terms and ordered to pay restitution. Two of the eight individuals are currently fugitives. OIG's work demonstrates how important it is to strengthen the enrollment screening process and improve program safeguards.

As a further result of OIG's work in south Florida, our analysis of Medicare billing patterns for inhalation drugs used with DME has uncovered evidence of abusive billing. Despite CMS's efforts to address inappropriate payments, problems persist. For example, in 2007, Medicare paid almost $143 million for inhalation drugs in Miami-Dade County alone-an amount 20 times greater than the amount paid in Cook County, Illinois, the county (outside south Florida) with the next highest total payments. However, according to Medicare enrollment data, Cook County is home to almost twice as many Medicare beneficiaries as Miami-Dade County. Medicare's average per-beneficiary spending on inhalation drugs was five times higher in south Florida than in the rest of the country. Further, 75 percent of south Florida beneficiaries who received a particular inhalation drug, budesonide, had Medicare-paid claims that exceeded Medicare utilization guidelines, compared to 14 percent of beneficiaries in the rest of the country. For 62 percent of south Florida inhalation drug claims, the beneficiaries on these claims did not have a Medicare-billed office visit or other service in the past 3 years with the physician who reportedly prescribed the drug. Finally, 10 south Florida physicians were each listed as the ordering physician on more than $3.3 million in submitted inhalation drug claims in 2007, or an average of $12,000 per day.

Similarly, OIG found that CMS has had limited success controlling aberrant billing by infusion clinics. In the second half of 2006, claims originating in three south Florida counties accounted for 79 percent of the amount submitted to Medicare nationally for drug claims involving HIV/AIDS patients and constituted 37 percent of the total amount Medicare paid for services for beneficiaries with HIV/AIDS. However, only 10 percent of Medicare beneficiaries with HIV/AIDS lived in these three counties.

Other Program Vulnerabilities

As part of its core mission, OIG identifies vulnerabilities that put programs and beneficiaries at risk and makes recommendations to address these vulnerabilities. OIG reviews have identified payments for unallowable services, improper coding, and other types of improper payments. Improper payments range from reimbursement for services not adequately documented and inadvertent mistakes to payments that result from outright fraud and abuse. We have identified program integrity risks and vulnerabilities in every part of Medicare, as well as Medicaid. These vulnerabilities affect services ranging from inpatient hospital and skilled nursing services to outpatient services provided by physicians and other health professionals, to payment for prescription drugs and medical equipment. Examples include:

Durable Medicare Equipment

OIG has an extensive body of work identifying Medicare fraud, waste, and abuse related to DME. Problems include DME suppliers circumventing enrollment and billing controls, high payment error rates, kickbacks, and excessive reimbursement rates for certain DME. OIG has made recommendations to CMS to strengthen program integrity and DME oversight. OIG also has recommended stronger enrollment safeguards and payment reforms to align Medicare reimbursement for DME more closely with widely available market prices.

OIG has long identified several types of DME that are particularly vulnerable to billing abuses. For example, an investigation of a large wheelchair supplier found that the company had submitted false claims to Medicare and Medicaid, including claims for power wheelchairs that beneficiaries did not want, did not need, or could not use. In 2007, the company agreed to pay $4 million and relinquish its right to approximately $13 million in claims initially denied for payment by CMS. Nationally, in 2004, OIG estimated that Medicare and its beneficiaries paid $96 million for claims that did not meet Medicare's coverage criteria for any type of wheelchair or scooter and that they overspent an additional $82 million for claims that could have been billed using a code for a less expensive mobility device.

In addition, OIG has identified reimbursement rates for certain

items and services that are too high. For example, in 2006, OIG reported that Medicare had allowed, on average, $7,215' for the rental of an oxygen concentrator that costs approximately $600 to purchase new. Additionally, beneficiaries incurred, on average, $1,443 in coinsurance charges. We determined that if home oxygen payments were limited to 13 months rather than the current 36 months, Medicare and its beneficiaries would save $3.2billion over 5 years.

Further, in March 2009, OIG reported that Medicare reimbursed suppliers for negative pressure wound therapy pumps based on a purchase price of more than $17,000, but that suppliers paid, on average, approximately $3,600 for new models. Negative pressure wound therapy pumps are a type of DME used to treat ulcers and other serious wounds.

When Medicare first started covering wound pumps in 2001, it covered only one model, which was manufactured and supplied by one company. Medicare paid for this pump based on the purchase price as identified by that company. In 2005, Medicare expanded its coverage to include several new pump models manufactured by other companies. However, Medicare reimburses suppliers for these new pumps based on the original pump's purchase price, which is more than four times the average price paid by suppliers.

Home Health/ Personal Care Services

In general, OIG has identified fraud, waste, and abuse vulnerabilities in home health and personal care services similar to those described above for DME.

In a report released this month, OIG estimated that New York State improperly claimed over $275 million in federal Medicaid reimbursement during our January 1, 2004, through December 31, 2006, audit period for personal care services from providers in New York City that did not meet coverage requirements. These improper payments occurred because the State did not adequately monitor New York City's personal care services program for compliance with certain federal and State requirements. In addition, we identified quality and safety concerns. Cases are being pursued involving allegations that beneficiaries were physically abused by personal care aides, and their property was stolen. In addition, we have investigated complaints from beneficiaries that aides have abandoned them.

Prescription Drugs

OIG has an extensive body of work identifying fraud, waste, and abuse related to prescription drug coverage under Medicaid, Medicare Part B, and Medicare Part D. Fraud concerns include pharmaceutical companies misreporting pricing information that is used as the basis of reimbursement and/or Medicaid rebates; illegal marketing tactics, including kickbacks and off label/off-compendium promotion; pharmacies switching drugs to maximize reimbursement; and drug diversion. OIG also is concerned that Medicaid reimbursement for prescription drugs, particularly generic drugs, does not accurately reflect drug costs. For Medicare Part D, OIG has identified vulnerabilities related to sponsors' bids and the resulting payments and premiums to plan sponsors, as well as deficiencies in Part D integrity safeguards.

Medicaid Services

Medicare and Medicaid share many of the same vulnerabilities, including DME, home health, and prescription drugs. Medicaid-specific vulnerabilities include improper payments for school based health services, case management services, and disproportionate share hospital payments.

For example, in 2006, OIG found that a State Medicaid agency claimed federal Medicaid funding totaling $86 million for unallowable targeted case management services. In a series of reviews in several States, OIG consistently found that schools had not adequately supported their Medicaid claims for school-based health services and identified almost a billion dollars in improper Medicaid payments.

Other Outpatient Services

OIG also continues to identify vulnerabilities related to certain types of services provided by physicians and other health professionals, including services related to advanced imaging, pain management, mental health services, clinical labs, and transportation services. For example, OIG found that from 1995 to 2005, advanced imaging paid under the Medicare Physician Fee Schedule grew more than fourfold, from 1.4 million to 6.2 million services. Allowed charges and utilization rate per beneficiary grew by a similar magnitude, to $3.5 billion and 163 services per 1,000 beneficiaries. Services provided by independent diagnostic testing facilities accounted for nearly 30 percent of this growth. OIG work has found problems with IDTFs, including noncompliance with Medicare requirements and billing for services that were not reasonable and necessary.

Inpatient Services

Expenditures for inpatient services, including those provided by inpatient hospitals and skilled nursing facilities, account for one-third of all Medicare expenditures. Problems identified by OIG include hospitals taking advantage of enhanced payments by improperly manipulating billing; hospitals reporting in-

accurate wage data, which affects future Medicare payments; inpatient facilities that may be gaming prospective payment reimbursement systems by discharging or transferring patients to other facilities for financial rather than clinical reasons; and kickback schemes.

OIG Recommendations

In addition to pursuing those who violate the law, we also alert program administrators and other departmental officials to problems and offer solutions. These recommendations for corrective action are found in OIG's audit and evaluation reports, management implication reports resulting from OIG's investigative work, and other communications. In 2008, implemented OIG recommendations resulted in an estimated $16 billion in program savings and funds put to better use. In addition, OIG recommendations have resulted in substantial improvements in efficiency, effectiveness, and quality, as well as fraud prevention, whose impacts are more difficult to quantify.

To preserve its independence and objectivity, OIG is not authorized to implement or operate the HHS programs it oversees, nor can OIG compel the Department to implement our recommendations. However, we take several steps to follow up with program officials on the status of OIG recommendations and to encourage actions to address the vulnerabilities that we have identified. For example, the Principal Deputy Inspector General and I meet regularly with the CMS Administrator and other senior CMS officials to discuss unimplemented recommendations and other program integrity concerns. OIG is implementing a new recommendations management system that will further enhance our ability to track and follow up on OIG recommendations.

Each year we issue a Compendium of Unimplemented OIG Recommendations. The Compendium consolidates significant unimplemented monetary and nonmonetary recommendations addressed to the Department that we expect would, if adopted, result in cost savings, improved program integrity, and/or greater program efficiencies. These recommendations require legislative, regulatory, and/or administrative action. While implementation of monetary recommendations would have fiscal impacts, implementation of nonmonetary recommendations would improve program operations in other ways. In some cases, the agency agrees with our recommendations but has not yet fully implemented them; in others, the agency disagrees with our recommendations.

OIG's unimplemented recommendations provide a useful roadmap for focusing efforts to safeguard and improve the efficiency and effectiveness of the HHS programs OIG oversees. However, it is difficult to draw conclusions about overall savings from these recommendations. Estimates of potential monetary benefits listed in the Compendium are unique to each recommendation and are not comparable. These are typically point-in-time estimates and are often specific to the scope and timing of OIG's underlying work. When OIG reports implemented recommendations and resulting savings in our Semiannual Reports to Congress, we typically rely on savings estimates produced by the Congressional Budget Office or other HHS sources. However, with respect to unimplemented recommendations, CBO or other sources for scoring potential savings frequently are not available. Therefore, OIG may use findings from our reports or other sources, as available, to estimate potential savings. Several of our recommendations that we expect would produce savings do not include estimates of those savings. Notwithstanding the limitations in estimating potential savings, the Compendium is an important tool for identifying program vulnerabilities and improvements.

Ensuring the Integrity of Federal Health Care Programs

OIG's Five-Principle Strategy to Combat Health Care Fraud, Waste, and Abuse

For federal health care programs to best serve beneficiaries and remain solvent for future generations, the government must pursue a comprehensive strategy to prevent, detect and remediate fraud, waste, and abuse. Based on OIG's extensive experience in combating health care fraud, waste, and abuse, we have identified the following five principles that we believe should guide the development of any national health care integrity strategy.

1. Enrollment - Scrutinize individuals and entities that want to participate as providers and suppliers prior to their enrollment in health care programs.
2. Payment - Establish payment methodologies that are reasonable and responsive to changes in the marketplace.
3. Compliance - Assist health care providers and suppliers in adopting practices that promote compliance with program requirements, including quality and safety standards.
4. Oversight - Vigilantly monitor programs for evidence of fraud, waste, and abuse.
5. Response - Respond swiftly to detected fraud, impose sufficient punishment to deter others, and promptly remedy program vulnerabilities.

We believe that these principles provide a useful framework for designing and implementing program benefits and integrity safeguards. Consistent with these principles, OIG offers the following recommendations to strengthen the integrity of federal health care programs.

Enrollment

Scrutinize individuals and entities that want to participate as providers and suppliers prior to their enrollment in health care programs.
Medicare and Medicaid provider enrollment standards and screening should be strengthened, making participation in federal health care programs as a provider or supplier a privilege, not a right. It is more efficient and effective to protect the programs and beneficiaries from unqualified, fraudulent, or abusive providers and suppliers up front than to try to recover payments or redress fraud or abuse after it occurs. Greater transparency in the enrollment process will help the Government know with whom it is doing business.

For example, as the Medcore and M&P case described above demonstrates, a lack of effective screening measures gives dishonest and unethical individuals access to a system they can easily exploit. Even after Medcore had billed Medicare for $4 million in fraudulent claims, it was easy for the clinic's owner to obtain a provider number in his wife's name for a second clinic, M&P, operating in the same building as Medcore, with the same medical director, employees, and patients. One of the owners, Mr. Marrero, testified that when he ultimately sold M&P for $100,000 in cash, he went to a lawyer's office so the lawyer could fill out paperwork to put ownership of the clinic in the name of two nominee owners. The sale was structured as a stock sale so that the new "owners" would have 90 days to notify Medicare of the change in ownership, allowing a window of time for the fraud to continue under new "ownership." In our experience, it is too easy for unscrupulous individuals to recruit nominee owners of fraudulent companies.

Providers and suppliers applying for enrollment in Medicare or Medicaid should be screened before they are granted billing privileges. Heightened screening measures for high-risk items and services could include requiring providers to meet accreditation standards, requiring proof of business integrity or surety bonds, periodic recertification and onsite verification that conditions of participation have been met, and full disclosure of ownership and control interests. The cost of this screening could be covered by charging application fees. New providers and suppliers should also be subject to a provisional period during which they are subject to enhanced oversight, such as prepayment review and payment caps.

Payment

Establish payment methodologies that are reasonable and responsive to changes in the marketplace.
We support efforts to pay appropriately for the items and services covered by federal health care programs. Medicare and Medicaid payments should be sufficient to ensure access to care without wasteful overspending. Payment methodologies should also be responsive to changes in the marketplace, medical practice, and technology. Although CMS has the authority to make certain adjustments to fee schedules and other payment methodologies, for some changes, congressional action is needed.

OIG has conducted extensive reviews of Medicare and Medicaid payment methodologies and has determined that the programs pay too much for certain items and services. As OIG's reviews of home oxygen equipment and wound therapy pump payments demonstrate, when reimbursement methodologies do not respond effectively to changes in the marketplace, the program and its beneficiaries bear the cost. As the experience of south Florida illustrates, excessive payments also are a lucrative target for criminals. These criminals can reinvest some of their profit in kickbacks for additional referrals, thus using the program's funds to perpetuate the fraud scheme.

All payment methodologies create incentives and fraud risks that should be identified and addressed. For example, fee-for-service payments create financial incentives to maximize the number and complexity of services provided, even when such services are not medically necessary. Conversely, under a fixed, prospective payment system, financial incentives encourage fewer services and patients may not receive all of the care that they need and for which the program is paying. In considering any payment structure, it is imperative to identify the incentives that it creates and associated risks and to implement necessary safeguards to remediate the negative incentives and reduce fraud risks.

Compliance

Assist health care providers and suppliers in adopting practices that promote compliance with program requirements.
Health care providers and suppliers must be our partners in ensuring the integrity of federal health care programs and should adopt internal controls and other measures that promote compliance and help prevent, detect, and respond to health care fraud, waste, and abuse. To this end, OIG has published on its Website extensive resources to assist industry stakeholders in understanding the fraud and abuse laws and designing and implementing effective compliance programs. These resources include sector-specific Compliance Program Guidance that describes the elements of an effective compliance program and identifies risk areas, advisory opinions, and fraud alerts and bulletins.

In many sectors of the health care industry, such as hospitals, compliance programs are widespread and often

very sophisticated; other sectors have been slower to adopt internal compliance practices. Compliance programs not only benefit the federal health care programs; they also benefit industry stakeholders by improving their business practices, by fostering early detection and correction of emerging problems, and by reducing the risk that they will become the subject of a whistleblower complaint or fraud prosecution.

States also have begun to recognize the value of compliance systems. For example, New York now requires providers and suppliers to implement an effective compliance program as a condition of participation in its Medicaid program. Medicare Part D also requires that prescription drug plan sponsors have compliance plans that address certain required elements. Although compliance programs do not guarantee reduced fraud and abuse, they are an important component of a comprehensive government-industry partnership to promote program integrity. We advocate that providers and suppliers be required to adopt compliance programs as a condition of participating in the Medicare and Medicaid programs. Further, the obligation of providers and suppliers to repay overpayments they discover through compliance efforts or otherwise should be made explicit in the statute. There should be no question that providers and suppliers must return taxpayer dollars they should not have received in the first place.

Oversight

Vigilantly monitor the programs for evidence of fraud, waste, and abuse.
As fraud schemes become more sophisticated and migratory, access to real time data and the use of advanced data analysis to monitor claims and provider characteristics are critically important. OIG is using innovative technology to detect and deter fraud, and we continue to develop and implement cutting edge initiatives to enhance our technology infrastructure and support a data driven antifraud approach. More must be done to ensure that agencies government-wide are able to use 21st century information technology effectively in the fight against health care fraud. This data-driven approach should underpin the development of fraud enforcement and prevention activities. The health care system compiles an enormous amount of data on patients, providers, and the delivery of health care items and services. However, federal health care programs often fail to use claims-processing edits and other information technology effectively to identify improper claims before they are paid and to uncover fraud schemes. For example, Medicare should not pay a clinic for HIV infusion when the beneficiary has not been diagnosed with the illness, pay twice for the same service, or process claims that rely on the provider identifiers of deceased physicians. Better collection, monitoring, and coordination of data would allow Medicare and Medicaid to detect these problems earlier and avoid making improper payments. Moreover, effective use of data would enhance the government's ability to detect and respond to fraud schemes more quickly.

Needed improvements in program oversight include real-time access to data for law enforcement; uniform, comprehensive data elements; more timely collection and validation of data; robust reporting of data by States and others; interoperability of systems; consistent data extraction methods; and the ability to draw and analyze claims and provider data across Medicare Parts A, B, C, D, and Medicaid. CMS is building an Integrated Data Repository that will, when completed, contain a wealth of data across several programs. Although the system is still under development, the prospect of such a comprehensive data warehouse holds considerable promise for detecting and preventing fraud and abuse. In addition, we advocate the consolidation and expansion of the various provider databases, including the Health Care Integrity and Protection Data Bank, the National Practitioner Data Bank, and OIG's List of Excluded Individuals/Entities. Providing a centralized, comprehensive, and public database of adverse actions and other sanctions -- including a national registry of patient abuse and neglect -- would be an effective means of preventing providers and suppliers with problem backgrounds from moving from State to State unnoticed by licensing, government, and health plan officials.

Response

Respond swiftly to detected fraud, impose sufficient punishment to deter others, and promptly remedy program vulnerabilities.
To ensure the integrity of federal health programs, law enforcement is working to accelerate the government's response to fraud schemes by reducing the time needed to detect, investigate, and prosecute fraud. The government's Strike Force model has proven highly successful in this regard, and although resource intensive, is a powerful antifraud tool and represents a tremendous return on investment. In addition to prosecuting criminals and recovering funds for the Medicare Trust Fund, the Strike Forces have had a strong sentinel effect, as evidenced by the 63 percent decrease in DME claims submitted in south Florida over the first 12 months of Strike Force operations there.

Even the best antifraud efforts are ineffective if fraud is not promptly detected and, once detected, promptly punished and deterred. For example, our investigations have found evidence of an increase in organized crime in health care. Health care fraud is attractive to or-

ganized crime because the penalties are lower than those for other organized-crime-related offenses (e.g., offenses related to illegal drugs); there are low barriers to entry (e.g., a criminal can easily obtain a supplier number, gather some beneficiary numbers, and bill the program); schemes are easily replicated; and detection efforts often are hampered by lack of access to real-time data. We need to alter the cost-benefit analysis by increasing the risk of swift detection and the certainty of punishment.

In addition, it is currently difficult to stop the flow of Medicare dollars to criminals who are under investigation for known health care fraud schemes. An explicit payment suspension authority would enable Medicare to keep taxpayer dollars out of the pockets of criminals in cases where the government has credible evidence of fraud. These criminals often take the money and disappear before the government can complete an investigation and prosecute them. An explicit payment suspension authority is a critical, money-saving tool in these situations.

OIG currently uses a range of administrative sanctions, including civil monetary penalties and program exclusions, as an adjunct to criminal and civil enforcement. However, OIG has identified a number of enhancements to these administrative authorities that would increase our ability to address emerging schemes, such as authorizing CMPs for false provider enrollment applications and for the ordering or prescribing of items or services by an excluded entity. Amending the law to align our CMP authorities with the recent *False Claims Act* amendments would also be helpful.

In addition, in the course of our investigations, audits, and evaluations, OIG often identifies program vulnerabilities that have been or could be exploited and recommends corrective actions. Program administrators and policy makers have important roles in responding quickly to address these vulnerabilities and reduce the risk of future fraud, waste, and abuse.

Conclusion

In conclusion, in the context of health care reform, it is an especially important time to consider how to best safeguard health care programs from fraud, waste, and abuse to protect beneficiaries and taxpayer dollars. OIG's mission is to protect the integrity of HHS programs, including the Medicare and Medicaid programs, and the well-being of program beneficiaries. In fulfilling our mission, OIG has identified tor recovery billions of dollars lost to fraud, waste, and abuse; helped remove thousands of fraudulent providers from federal health care programs; pinpointed numerous items and services for which the government is substantially overpaying; and recommended actions to better protect programs and beneficiaries. These experiences and results have applicability to the current discussions of health care reform. It is critical that the government pursue a comprehensive strategy to combat fraud, waste, and abuse. We believe that our "Five Principles" strategy provides the framework to identify new ways to protect the integrity of the programs, meet the needs of beneficiaries, and keep federal health care programs solvent for future generations. We look forward to working with the Committee on these issues, including providing you with information and technical assistance. This concludes my testimony, and I would be pleased to answer any questions.

Daniel R. Levinson

Daniel R. Levinson has headed the Office of Inspector General for the U.S. Department of Health and Human Services since September 8, 2004. HHS is among the largest departments in the federal government, encompassing Medicare, Medicaid, public health, medical research, food and drug safety, welfare, child and family services, disease prevention, Indian health, and mental health services. It also exercises leadership responsibilities in public health emergency preparedness and combating bio-terrorism.

As Inspector General, Mr. Levinson is the senior official responsible for audits, evaluations, investigations, and law enforcement efforts, relating to HHS programs and operations.

Mr. Levinson has devoted most of his career to government service. Prior to his appointment at HHS, he served as Inspector General of the U. S. General Services Administration, where he oversaw the integrity of the federal civilian procurement process.

Mr. Levinson is a Phi Beta Kappa graduate of the University of Southern California, and earned a J.D. from Georgetown University, where he served as notes and comments editor of the *American Criminal Law Review*. He is a Certified Fraud Examiner and a member of the California, New York, and District of Columbia Bars.

[TESTIMONY]

U.S. Postal Service in Crisis

Congressional testimony before the U.S. Senate, Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security (August 6, 2009)

By Inspector General David C. Williams

Mr. Chairman and members of the subcommittee, I appreciate the opportunity to discuss the Postal Service's retiree health care liabilities. The Postal Service's financial stability is currently threatened by the disruptive effects of new communication technologies and the massive and sudden economic downturn.

This situation has turned into an immediate crisis because of the significant diversion of cash to pay for future retiree health care benefits. For example, the first 6 months of this year's payment to the Postal Service Retiree Health Benefits Fund was $2.7 billion. If not for this payment, the Postal Service would have made $400 million instead of losing $2.3 billion in the first half of 2009.

The *Postal Accountability and Enhancement Act of 2006* requires the Postal Service to make 10 annual payments of over $5 billion each in addition to the $20 billion already set aside for prefunding its retiree health benefits. The size of the $5 billion payments has little foundation, and the current payment method is damaging to the financial viability of the Postal Service even in profitable times.

- The payment amounts were not actuarially based. Instead, the required payments were built to ensure that the Postal Act did not affect the federal budget deficit. This seems inexplicable since the Postal Service is not part of the federal budget, does not receive an appropriation for operations, and makes its money from the sale of postal services.
- The payment amounts are fixed through 2016 and do not reflect the fund's earnings or estimates of the Postal Service's liabilities as a result of changing economic circumstances, declining staff size, or developments in the health care and pharmaceutical industries.
- The payments do not take into account the Postal Service's ability to pay and are too challenging even in normal economic times. In the current economic climate, the Postal Service is forced to borrow and place its solvency at risk. Borrowing to pay a debt that will be incurred in the future is a controversial practice — not seen in business or government.

Beyond the problems with the payments, we believe it is important to know if the Postal Service's obligation is reasonably estimated. My office asked an actuarial consulting firm, the Hay Group, to:

- Benchmark OPM's assumptions against those commonly used in the public and private sector;
- Review OPM's estimates of the Postal Service's liabilities;
- Estimate how well the Postal Service will have funded its retiree health obligations when the mandated payments end; and
- Estimate proper funding levels given adjustments to assumptions.

In brief, the actuaries found that:

- OPM's assumption that health care inflation will average 7 percent indefinitely is unreasonably high when compared to the 5 percent health care inflation rate commonly used by Fortune 100 companies, state and local governments, and public utilities.
- The payments are aggressive, reducing the Postal Service's unfunded liabilities more quickly than typical prefunding plans.
- When the broadly accepted 5 percent for growth of health care costs is used, the estimates show the Postal Service will have overfunded its obligations by an extravagant $13 billion at the end of 2016.

By the end of 2016, the current payments will have essentially created an accidental annuity. At 5 percent interest, the $104 billion fund will earn more than $5 billion a year. This is a significant amount of money to cover retiree premiums, which are predicted to be $2 billion this year.

The punishing payments threaten Postal Service solvency in the current crisis. Because the Postal Service has been forced to borrow during its profitable years, borrowing levels are now stressed during times of need.

Resetting the annual payments from over $5 billion to $1.57 billion will leave only $26 billion unfunded by the end of 2016.

- Resetting payment levels will provide a more achievable financial goal.
- New payments will take into account the substantial annual earnings of the fund. Last year, the fund earned $1.3 billion.
- Payments should be reset periodically to recognize factors such as
  - Medical/technical innovations and breakthroughs;
  - Current efforts to reduce inflation within the medical sector; and
  - Changing interest rates on the fund.

The Postal Service must meet its retiree benefit obligations, while acting like a business and paying its expenses from the sale of postal services. As a result, retiree health benefit obligations and all other Postal Service liabilities should be derived mathematically and not politically. I am aware that there were voices on your committee and in the House that called for the proper payment level to be set at the time that the payments were distorted. I am hopeful that these voices will now be heard to correct this debilitating problem. If this distortion is corrected, the Postal Service can more realistically address the remaining serious challenges and opportunities before it. Thank you.

David C. Williams

David C. Williams was sworn in as the second independent Inspector General for the U.S. Postal Service on August 20, 2003. His organization's mission is preventing, detecting, and reporting fraud, waste, and misconduct, and promoting efficiency in Postal Service operations.

Mr. Williams' staff of more than 1,100 employees—located in offices nationwide—independently audits and investigates the largest civilian federal agency with $75 billion in annual revenues, a workforce of more than 760,000 employees and contractors, and 37,000 postal facilities.

In his last position, Williams served as the Deputy Assistant Administrator for Aviation Operations at the Transportation Security Administration from August 2002 until August 2003, where he managed the Aviation Inspection Program at federalized airports.

Williams served in the U.S. Army Military Intelligence and began his civilian federal career as a Special Agent with the Secret Service.

A Bronze Star and Vietnamese Medal of Honor recipient, Mr. Williams previously served as Inspector General for five federal agencies: the U.S. Nuclear Regulatory Commission, Social Security Administration, Department of the Treasury, Tax Administration of the Department of Treasury and acted as IG for the Department of Housing and Urban Development.

[TESTIMONY]

Small Business Innovation Research

Congressional testimony before the U.S. Senate, Committee on Commerce, Science and Transportation (August 6, 2009)

By Inspector General Allison C. Lerner

Mr. Chairman and Members of the Committee, I appreciate this opportunity to discuss my office's work related to the Small Business Innovation Research program at the National Science Foundation.

Background

The *Small Business Innovation Development Act of 1982* created the Small Business Innovation Research program to stimulate technological innovation; use small businesses to meet federal research and development needs; foster and encourage participation by minority and disadvantaged persons in technological innovation; and increase private sector commercialization innovations derived from federal research and development. Under the SBIR program, the National Science Foundation and ten other federal agencies currently allocate 2.5% of their extramural R&D budgets for awards to small businesses.

Each SBIR agency uses the program to address the unique needs of its mission. At NSF, the primary objective of the SBIR program is to increase the incentive and opportunity for small firms to undertake cutting-edge, high-risk, high-quality scientific, engineering, or education research that would have a high potential economic payoff if the research is successful. The SBIR program is part of NSF's Engineering Directorate, and the ultimate goal of each project is a commercially viable product, process, device, or system. The program is funded

by the government in two phases, followed by a privately-funded third phase. Phase I is a 6-month grant to assess an idea's feasibility, currently supported by NSF up to $150,000. If the Phase I project is successful, the company can apply for a Phase II award, which runs for up to 2 years and is funded up to $750,000.

Since 1990, NSF has awarded more than 6,600 Phase I and Phase II SBIR awards totaling more than $1.1 billion. The vast majority of the companies receiving SBIR awards spend their SBIR funds properly to carry out the research they proposed to do, and they report accurately to the agency about the results they obtained under the SBIR award. However, since my office's inception, we have conducted a number of investigations of companies that have allegedly committed fraud involving their SBIR awards.

Specifically, since 1989 we have opened 64 cases involving SBIR companies. Of those 64 cases, 16 have resulted in significant criminal, civil, or administrative action to date, and 5 are currently under investigation. While these numbers are not large, it is likely that they do not reflect the full extent of fraud in the program due to under-reporting and other issues which I will discuss later in my statement.

It is important to note that NSF's SBIR program staff has strongly supported my office's efforts to prevent, detect, and prosecute fraud in the SBIR program. SBIR program officers regularly inform my office when they receive allegations of wrongdoing or become aware

of information that indicates a possible problem within the program, and those valuable leads have been the source of many of our successful investigations.

As requested by the Committee, the following summarizes the types of fraudulent activity our office has found in NSF's SBIR program. I will also discuss processes that my office has developed and NSF has implemented that have enabled us to prevent and, if necessary, prosecute fraud in the SBIR program. Finally, I will conclude by noting some problems my office has encountered in investigating this type of fraud.

Types of Fraudulent Activity in the National Science Foundation's SBIR Program

The primary type of fraudulent activity we encounter in the SBIR program involves duplicative funding, which results in false statements, false claims, and criminal misuse of grant funds. We have also investigated cases in which research misconduct has resulted in fraud against the SBIR program. I will briefly describe our work in these areas.

Duplicative Funding

Duplicative funding, in which companies obtain payments from multiple SBIR agencies for the same work, is the most frequent violation we have found in NSF's SBIR program. This problem arises because, in order to maximize their opportunities for receiving SBIR funding for their proposals, companies may submit the same proposal to more than one of the eleven federal agencies that have SBIR programs. At NSF, these multiple submissions must be disclosed, and it is a violation of program policy for companies to accept funding from multiple agencies for the same work. NSF's proposal preparation guidance makes it clear to potential recipients that receiving duplicate SBIR funding for the same or overlapping research is prohibited, and the NSF program announcement clearly states that:

> NSF will not make awards that duplicate research funded or expected to be funded by other agencies . . . . If a proposer fails to disclose equivalent or overlapping proposals . . . , the proposer could be liable for administrative, civil or criminal sanctions.

Since its inception, my office has investigated approximately 34 cases of alleged duplicative funding. We have substantiated the charge in 10 cases. Examples of our work in this area include a case in which, in addition to receiving duplicate funding from NSF's and other agencies' SBIR programs, the recipient used the SBIR funds to pay for renovations to his home and to overpay vendors so he could pocket the reimbursements. Ultimately, he paid $1.4 million in restitution, civil damages, taxes, and penalties, and pled guilty to mail fraud and tax evasion to resolve these charges.

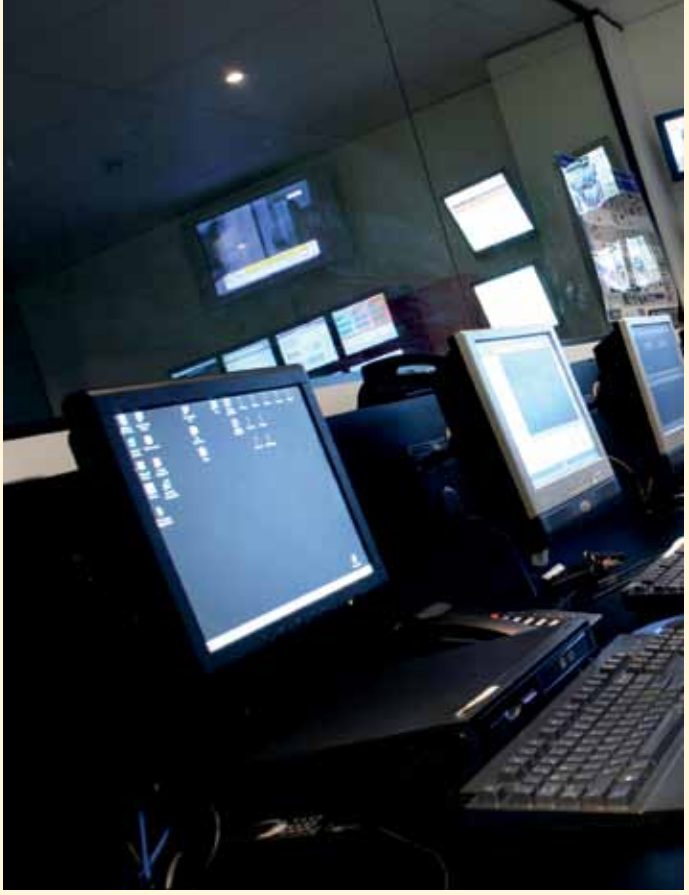
A second such case involved two companies with the same owner that received duplicate SBIR awards from several agencies for the same work. The companies paid $3.45 million in restitution and civil damages, and open SBIR awards to the companies totaling $909,000 were terminated.

Finally, we also investigated a case in which the company received funding from NSF and other federal agencies for duplicate research. The defendants were accused of knowingly and repeatedly applying for and receiving SBIR grants from agencies for research that had already been completed under grants awarded to other agencies. They were also accused of charging the government for the cost of engineering work that was not performed. As a result of our investigation, $530,000 of the company's and the owner's bank accounts and assets, which had been frozen during the investigation, were paid to the federal government, and $1.4 million in open SBIR awards were terminated.

Research Misconduct

We have also encountered situations where research misconduct under some of NSF's SBIR awards resulted in the program being defrauded. Research misconduct occurs when data or results are fabricated, falsified, or plagiarized. We have found some instances where companies fabricated, falsified, or plagiarized their Phase I final reports in order to obtain Phase II funding. Such misconduct in research amounts to fraud against the SBIR program because in order to obtain Phase II funding, the company's Phase I project must be successful.

In one such case we investigated, a university professor obtained an NSF Phase I award for a proposal he submitted in his wife's name on behalf of a nonexistent company she allegedly owned. The professor converted all of the Phase I funds to his personal use, and then plagiarized the final Phase I report from a former student's thesis. On the basis of



that report, the non-existent company received a Phase II award. As a result of our investigation, the professor pled guilty to making false statements, and he and his wife paid $214,000 in restitution and fines.

Best Practices

As a result of our investigations involving SBIR program fraud, my office has identified two best practices that are valuable tools in preventing and prosecuting such fraud. A summary of these practices—required disclosures and certifications and mandatory attendance at awardee briefings—follows.

Required Disclosures and Certifications

In 1994, as a result of problems we had noted in our investigations involving SBIR recipients, our office made several recommendations intended to improve administration of NSF's SBIR program. The majority of those recommendations focused on strengthening existing disclosures and certifications, and on adding such disclosures and associated certifications in areas that had previously had no such coverage. NSF accepted all of these recommendations, and the resulting disclosures and certifications have helped the agency deter fraud at the outset, by making clear what the agency's expectations are. They have also helped us prosecute cases of fraud, as they make it clear to recipients that the provision of false information is a criminal offense.

Pursuant to our recommendations, NSF requires proposers seeking SBIR funding to disclose if the proposal has been submitted to another agency and to state that: (1) the company is a small business; (2) the company will perform at least two-thirds of the work under Phase I or at least half under Phase II; and (3) the Principal Investigator will be primarily employed by the company during the term of the award. The authorized organizational representative is then required to sign the following certification (referred to as a "1001 certification"):

> I understand that the willful provision of false information or concealing a material fact in this report or any other communication submitted to NSF is a criminal offense (U.S. Code, Title 18, Section 1001).

When an SBIR proposal is awarded, before the company can receive its first payment, NSF requires SBIR recipients to disclose whether:

1. The principal investigator and the small business firm have accepted funding for the same or overlapping work except as stated in the underlying proposal,
2. All proposals describing the same or overlapping work have been withdrawn from other agencies,
3. The primary employment of the principal investigator is with the firm at the time of the award and will continue during the conduct of the research, and
4. The grantee is a small business.

After making these disclosures, the authorized company officer is required to sign a 1001 certification.

Finally, SBIR awardees are required to submit reports to NSF about their projects' accomplishments to receive interim and final payments. Phase I awardees submit a final report when the project is over, and Phase II awardees submit interim reports every 6 months and a final report at the end. NSF requires SBIR recipients submitting such reports to disclose whether:

1. The Principal Investigator is primarily employed by the company;
2. The work under the project has not been submitted for funding to another federal agency and has not been funded under any other federal award;
3. The work for which payment is requested was performed in accordance with the award terms and conditions;
4. The statements in the report (excluding scientific hypotheses and scientific opinions) are true and complete; and
5. The text and graphics in the report are the original work of the company—followed by a 1001 certification.

In all instances, the disclosures and certifications relate to requirements of NSF's SBIR program. If the company fails to make these disclosures or provide the required certifications, it will not receive an award or be paid. If the certifications are false, the company and its officers can more readily be prosecuted for providing material false information to the federal government because, as previously noted, the company has attested that it is aware that providing such false informa-

tion is a violation of federal law.

Mandatory Attendance at Awardee Briefings

NSF requires all companies that receive Phase I awards to attend an SBIR Phase I workshop, which includes presentations on a variety of topics to help awardees comply with NSF requirements and successfully commercialize the results of their research. All Phase I award recipients must attend these workshops, and NSF retains attendance records.

More than a decade ago, the NSF SBIR program invited my office to join in the workshop and give a presentation on the work we do. The briefing presented by my staff makes it clear to awardees that violations of SBIR program requirements constitute wrongdoing, and outlines the specific criminal, civil, and administrative consequences of such wrongdoing. Further, we describe specific cases involving SBIR recipients we have investigated and that have been prosecuted. U.S. Attorneys who have prosecuted cases of fraud against SBIR have cited these briefings as an asset in prosecutive decisions. These briefings and the documentation of awardees' attendance at them help ensure that no SBIR awardee can claim ignorance of NSF's SBIR requirements and/or the consequences of violating these requirements.

Programmatic and Investigative Challenges

In addition to identifying best practices to deter and prevent SBIR program violations, my office has also identified two challenges to investigating such violations. Following is a summary of these challenges—deficiencies in databases of SBIR awards and lack of strong certifications by some federal agencies.

Deficiencies in Databases

NSF maintains comprehensive internal databases on its SBIR program from which NSF program officers and my office can easily obtain complete information about all SBIR proposals submitted to and awards issued by NSF. However, while we have full access to NSF SBIR proposal and award information, there is currently no convenient means for obtaining detailed information about SBIR proposals submitted to and awards received by companies from the other SBIR agencies. This lack of access presents a programmatic and investigative challenge to determining whether more than one federal agency has paid for the same research.

Currently, two internet databases list SBIR awards to companies—USAspending.gov and SBA TECH-net. However, neither of these databases is complete, and neither provides sufficient detail to enable NSF's SBIR program to determine whether another agency's program had already paid for the same project. These limitations also make it more difficult for us, and other OIGs, to investigate SBIR cases, because of the significant effort required to obtain SBIR proposals and reports from other agencies. Ensuring that all SBIR agencies and their OIGs have electronic access to other agencies' SBIR proposals and awards would facilitate efforts to prevent, detect, and prosecute fraud.

Insufficient Disclosures and Certifications

As previously noted, NSF requires SBIR proposers and awardees to certify to the accuracy of required disclosures and clearly informs those entities that providing false information via those disclosures is a crime. Not all SBIR funding agencies require the number and frequency of disclosures and certifications

that NSF does, and their absence can impair the government's ability to prosecute fraud in those programs. In one case our office investigated, the final report submitted to NSF contained fifteen tables and figures, twelve of which had been submitted as accomplishments in twenty previous reports to seven other SBIR agencies. However, since none of the other agencies required certifications about overlapping or duplicative work, defense counsel was able to argue persuasively that only the NSF funding should be repaid.

Conclusion

The SBIR program at NSF is a valuable tool for providing funds to small, high-tech businesses conducting innovative research to advance NSF's mission and to possibly lead to commercialization of new technologies. NSF has supported our office's efforts to prevent and detect fraud in its SBIR program, and in conjunction with our office has instituted processes that enhance both its ability to prevent fraud and our office's ability to prosecute fraud when it occurs. My office will continue to work in partnership with NSF to prevent unscrupulous companies from fraudulently obtaining SBIR funds and to investigate allegations of duplicative funding, research misconduct, and other fraud against this important program. Additionally, we will continue to recommend practices to strengthen the integrity of the SBIR program.

This concludes my statement. I would be pleased to answer any questions you or other members may have.

Ms. Lerner's testimony emphasized the importance of certifications in preventing and prosecuting fraud against the SBIR program. Certifications establish that the applicant was aware that providing false statements to the government is a federal crime. On December 2, 2009 the Research Misconduct Working Group sponsored a meeting attended by twenty-three representatives from nine SBIR-funding agencies as well as a staffer from the Senate Committee on Commerce, Science, and Transportation, to discuss how certifications could be improved to reduce the incidence, and enhance the prosecution, of fraud against the SBIR program. The group plans to meet again and will coordinate its efforts with actions being taken by the Small Business Administration in this area.

Allison C. Lerner

Allison C. Lerner assumed the duties as Inspector General of the National Science Foundation in April 2009, reporting to the National Science Board and the Congress. As head of the Office of Inspector General she recommends policies for promoting economy, efficiency and effectiveness of NSF programs and operations. She leads efforts to prevent and detect fraud, waste, and abuse, improving the integrity of NSF programs and operations and investigating allegations of misconduct in science.

Ms. Lerner was appointed in November 2005 as counsel to the Inspector General at the Department of Commerce, a position through which she acted as the IG's principal legal advisor and managed the office's staff attorneys and legal services.

Ms. Lerner began her federal career in 1991, joining the Office of Inspector General at Commerce as Assistant Counsel, and has been a member of the Senior Executive Service since 2005.

Ms. Lerner has been honored by the President's Council on Integrity and Efficiency with three awards for excellence.

Ms. Lerner received her law degree from the University of Texas School of Law and a B.A. in liberal arts from the University of Texas. She is admitted to the bar in both Texas and the District of Columbia.

[TESTIMONY]

Hiring Practices and Other Administrative Actions

Congressional testimony before the U.S. House of Representatives, Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations (September 23, 2009)

By James J. O'Neill

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to discuss several issues that were the subject of two recent Office of Inspector General reports, Administrative Investigation – Misuse of Position, Abuse of Authority, and Prohibited Personnel Practices Office of Information & Technology, Washington, DC, and Administrative Investigation – Nepotism, Abuse of Authority, Misuse of Position, Improper Hiring, and Improperly Administered Awards, OI&T, Washington, DC. I am accompanied by Mr. Joseph G. Sullivan, Jr., Deputy Assistant Inspector General for Investigations, and Mr. Michael R. Bennett, Attorney Advisor.

While the reports deal with different VA officials, many of the same issues are contained in both reports. In keeping with the Subcommittee's instructions, we will discuss the issues related to the hiring process and other administrative actions, which include: nepotism, misuse of position, prohibited personnel practices, misuse of hiring authorities, improper funding of academic degrees, and improper administration of awards.

Nepotism

Federal law states that a public official may not appoint, employ, promote, advance, or advocate for the appointment, employment, promotion, or advancement, in or to a civilian position any person who is a relative of the public official. An individual may not be appointed, employed, promoted, or advanced in or to a civilian position in an agency if such appointment, employment, promotion, or advancement has been advocated by a public official, serving in or exercising jurisdiction or control over the agency, who is a relative. It further states that money shall not be paid from the Treasury as pay to an individual appointed, employed, promoted, or advanced in violation of this section.

The Standards of Ethical Conduct for employees of the Executive Branch prohibit an employee from using his or her public office for the private gain of relatives and prohibits the use of his or her Government position or title or any authority associated with his or her public office in a manner that is intended to coerce or induce another person, including a subordinate, to provide any benefit, financial or otherwise to himself, to friends, or to relatives.

VA policy mandates that the restrictions on the employment of relatives apply to all VA employees; that public officials may not recommend or refer a relative for consideration by a public official standing lower in the chain of command; and that "extreme care must be taken to avoid any possibility of likelihood that the nepotism law may be violated in an employment action." The policy further requires that management officials "take appropriate actions to avoid situations which have the potential for, or appearance of, being a violation of nepotism requirements" and at a minimum, document cases where relatives are employed

or being considered for employment in the same organizational element or chain of command.

One of the reports details the actions of a former VA official who was involved in the hiring of two family members through the Federal Career Intern Program. In fact, the former VA official advocated for the hiring of one family member on two separate occasions for two different positions. However, her improper actions were not limited to the hiring of the family members but also included hiring friends, involving herself in a change of work schedule for her relative, checking on the status of a cash award for the family member, and authorizing expenditures for graduate courses for family member. This former VA official also helped put a family member's application package together, and she told a subordinate that the family member was qualified for a GS-5 position and submitted arguments and documents in an effort to advocate for her assertion that the family member was, in fact, qualified. Further, she asked the selecting official to interview her family member, and instructed a subordinate, to "push" the family member's application as an FCIP candidate.

We found it problematic that the former VA official's relative, after being hired as a part-time intern trainee, was able to convert to a full-time position working a part-time schedule from a remote location over 500 miles away from the relative's managers and duty station. We found no plausible rationale supporting any aspect of this peculiar arrangement.

Misuse of Position

The Standards of Ethical Conduct for Employees of the Executive Branch state that public service is a public trust; that each employee has a responsibility to place loyalty to the Constitution, laws, and ethical principles above private gain; and that employees shall endeavor to avoid any actions creating the appearance that they are violating the law or ethical standards. The Standards also state that an employee shall not use his public office for his own private gain or for the private gain of friends or persons with whom the employee is affiliated in a nongovernmental capacity, and they prohibit an employee engaged in a financial transaction from using nonpublic information or allowing the improper use of nonpublic information to further his own private interest or that of another, whether through advice, recommendation, or by unauthorized disclosure. Also, Federal Acquisition Regulations state that Government business must be conducted in a manner above reproach and with complete impartiality and with preferential treatment for none.

We found that a VA official misused her official position for the personal gain of a friend when she told a potential VA contractor that they should consider hiring a long time friend of the VA official and provided that friend's resume to the contractor. While the contractor was never told to hire the friend, the contractor did ask the friend to help them put together their proposal and offered her full-time employment should VA award them the contract. While there may not have been an expressed quid pro quo, the VA official clearly and improperly pressured the contractor to hire the friend while the VA official was involved in setting up a VA contract.

We found that the same VA official violated Federal acquisition regulations when she shared nonpublic VA procurement information with her friend by telling her that VA planned to issue a request for proposal, that a certain contractor was a potential vendor, and suggested that her friend contact the contractor for employment, resulting in a personal gain for her friend. We found it problematic that the VA official also shared nonpublic VA information with another friend who was not employed by VA or the contractor, and allowed him to act as an emissary for a VA procurement. This gave the friend an opportunity to exploit the situation for his own personal gain and possible employment with the contractor, and it also gave the contractor a significant advantage in obtaining a VA contract.

We found that a former VA official abused her authority and engaged in prohibited personnel practices in the hiring of friends when as the appointing official she gave preference to her two friends when she selected them for positions within the Office of Information & Technology. In addition, her selection of three other individuals constituted preselection based on a previous relationship.

This same former VA official also improperly appointed her two friends at rates above the minimum salary. Person-

nel records contain no justification for their appointments at a higher pay rate, and the justification memorandum for one friend's higher salary did not comply with all the requirements outlined in VA policy. It appeared that these appointments at a higher than minimum pay rate were predicated merely on the prior existing relationships between the former VA official and these individuals, since the documentation justifying the benefit is either nonexistent or insufficient.

We found that an OI&T manager misused his position for the private gain of a family member when he helped her obtain employment within OI&T by recommending her to the hiring official. This manager was well aware that the hiring official was desperate for administrative help, and he exploited her need, perceived or otherwise, to the benefit of his family member. In addition, he knew that when he recommended his relative for the position, separate from the competitive review process, he was orchestrating a means for the relative to bypass the competitive process for the position. We also concluded that his relative's appointment did not comply with merit system principles, was made improperly, and his actions led to his relative's appointment to a position for which she was not qualified.

In addition, the same manager misused his public office for the private gain of another family member when he advocated to the Austin Human Resource staff for her appointment and a higher than minimum salary. Furthermore, a former VA official improperly appointed this family member non-competitively under the FCIP at a pay rate above the minimum salary. We found no documentation to justify the appointment at a rate above the minimum.

Prohibited Personnel Practices

Federal law states that recruitment should be from qualified individuals from appropriate sources in an endeavor to achieve a work force from all segments of society, and selection and advancement should be determined solely on the basis of relative ability, knowledge, and skills, after fair and open competition which assures that all receive equal opportunity. This is the essence of hiring based on merit. The law further provides that any employee, who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, grant any preference or advantage not authorized by law, rule, or regulation to any employee or applicant for employment for the purpose of improving or injuring the prospects of any particular person for employment, as well as knowingly take, recommend, or approve any personnel action if the taking of such action would violate a veterans' preference requirement. The Merit Systems Protection Board defines an "abuse of authority" as an arbitrary or capricious exercise of power by a Federal official or employee that adversely affects the rights of any person or that results in personal gain to preferred other persons.

We found that a VA official abused her authority and engaged in a prohibited personnel practice when she expressed to her subordinates, who were also the rating and selecting officials, that her preference was for them to hire her friend, giving the friend an advantage over other applicants, and when she failed to assure that all applicants received an equal opportunity, in particular those with veterans' preference. The VA official's efforts to hire her friend as her Executive Assistant started when the friend was a contractor employee and the VA official began integrating her into Government day-to-day business. The VA official went to the extent of requesting that a position be re-announced so that her friend had an opportunity to apply; closed out the certificate because her friend could not be hired due to a 10-point veteran blocking her; and then planned to hire her as a Supervisory Information Technology Specialist so that she could later laterally move her into an Executive Assistant position.

Additionally, the VA official expressed to the selecting official, that she "really wanted her friend to come on board," and they developed a plan to hire the friend into a GS-15 Supervisory IT Specialist position under the selecting official's area of responsibility. The selecting official selected the friend as the best qualified for the position based solely on the VA official's recommendation and desire to get the friend "on board" into Federal service; however an independent review of the applicant packages disclosed that the friend was not the best qualified. The friend even admitted to us that she did not have the technical skills necessary for the position and that it made better sense to put her skills to use as an Executive Assistant. Moreover, the VA official did not comply with VA policy when she requested that the friend be appointed at a rate above the minimum based on her qualifications and private sector salary. The VA official's limited justification did not comply with VA policy requiring her to provide a description of her recruitment efforts, a comparison of the friend's qualifications to the other applicants, or the reason for the rate instead of a recruitment incentive.

We found that another VA official abused her authority and engaged in prohibited personnel practices when she preselected three other individuals for GS-15 positions. The selecting official selected the individuals from certificates without taking the required steps to determine the best qualified candidate and with a total disregard for fair and open competition in violation of merit systems principles.

We further concluded that three other OI&T employees abused their au-

thority and engaged in prohibited personnel practices when they knowingly failed to properly process applicant packages for four GS-15 positions. Four individuals were preselected for positions, false spreadsheets were created and backdated, and the preferred candidates were listed on top.

Misuse of Hiring Authorities

Federal Career Intern Program

Executive Order 13162, dated July 6, 2000, authorized the establishment of the FCIP to assist agencies in recruiting and attracting exceptional individuals with a variety of experiences, academic disciplines, and competencies necessary for the effective analysis and execution of public programs. Federal regulations provide that appointments made under FCIP expire after 2 years; however, civil service status may be granted to career interns who successfully complete their internships and meet all qualification, suitability, and performance requirements. Regulations further state that agencies are required to provide the career interns with formal training and developmental opportunities to acquire the appropriate agency-identified competencies needed for conversion to permanent Federal employment. The U.S. Office of Personnel Management website states that the benefits to using the FCIP program are that there is no requirement to publically announce the positions; it can be used with a targeted recruitment program; it provides flexibility in training; and that after 2 years, the employee can be noncompetitively converted to a permanent appointment.

VA policy requires that any occupation for which a Career Intern Program is established must lend itself to a formal training and development component. Components of a program should include, but are not limited to, individual development plans, performance standards, position descriptions, rotational assignments, specific skills to be acquired, etc. Policy further states that HR personnel, in collaboration with the selecting official/subject matter expert, are required to identify appropriate targeted recruitment sources of candidates with the appropriate background, skills, or education; and develop a career intern formal training and development plan, provided one does not already exist elsewhere within VA for the specific career. Policy also requires HR management officers at local facilities to ensure a Career Intern Program complies with policy.

We identified three specific instances of improper appointments to Management Analyst, GS-5 positions under FCIP. We found no evidence that OI&T established a Career Intern Program for Management Analysts or that a formal plan existed for trainees to acquire the appropriate agency-identified competencies needed for conversion to permanent employment. Given the scope of recruitment activities that took place as a result of the 2006 OI&T reorganization efforts and other large scale OI&T hiring initiatives, it appears, based on personnel records reviewed, that OI&T hiring officials made additional improper Management Analyst FCIP appointments and subsequently failed to provide the required 2-year formal training program.

Improper Use of Direct-Hire Authority

Federal law provides agencies with the authority to appoint candidates directly to jobs for which OPM determines that there was a severe shortage of candidates or a critical hiring need. OPM's website states that the Direct-Hire Authority is an appointment authority that enables an agency to hire, after public notice is given, any qualified applicant without regard to rules requiring competitive rating and ranking, veterans' preference, and "rule of three" procedures.

Federal law permits an agency with delegated examining authority to use DHA for a permanent or non-permanent position or group of positions in the competitive service if OPM determines that there is either a severe shortage of candidates or a critical hiring need for such positions.

We identified four people who were appointed for IT Specialist positions at the GS-5 level under the DHA. However VA's authority for IT Specialists at the GS-5 level expired on June 14, 2004, which was prior to their appointments. We notified VA Central Office's Office of Human Resources of VA's improper use of the DHA to hire these employees. The Director of Central Office Human Resource Service told us that she conferred with the Director of Recruitment and Placement Policy Service, Office of Human Resources Management, and that she verified that VA did not have DHA for any Title 5 positions to include IT Specialists at pay grades below GS-9. We referred the improper use of DHA to the Acting Assistant Secretary for Human Resource and Administration for his immediate review and action.

Improper Funding of Academic Degrees

The *Homeland Security Act of 2002* amended the *Government Employee Training Act of 1958* by expanding an agency's authority to pay or reimburse an employee for the costs of academic degree training. VA employee development policy promulgates this authority and allows an employee to obtain an academic degree at VA expense only when such training contributes to:

1. Significantly meeting an identified agency, administration, or staff office training need that is consistent with VA's Strategic Plan;
2. Solving an identified agency staffing problem;

3. Accomplishing goals in VA's Strategic Human Capital Management Plan; and
4. A planned, systemic, and coordinated program of professional development.

VA training policy stipulates that VA officials exercising this authority must require employees selected to benefit from this provision to sign a continued service agreement prior to training. It also requires that prior to implementing academic degree training, VA officials in implementing offices are to establish a system of records and develop written plans and procedures for:

1. Accounting of funds spent for academic degree training and the number of employees and types of programs enrolled in or completed;
2. Ensuring competitive procedures for selecting employees for academic degree training are consistent with the requirements of 5 CFR § 335;
3. Ensuring educational institutions awarding an academic degree are accredited by a nationally recognized body, as recognized by the U.S. Department of Education; and
4. Certifying how such training will meet VA training needs, resolve an identified VA staffing problem, or accomplish a VA goal in the VA Strategic Human Capital Management Plan.

Finally, VA policy provides that employees may take training from non-Government sources if the following conditions are met:

1. Adequate training is not reasonably available by, in, or through a Government facility;
2. The training is the most practical and least costly to the Government; and
3. The non-Government facility does not discriminate based on race, sex, color, national origin, disability, religion, age, sexual orientation, or status as a parent.

We found six instances where OI&T managers as well as approving officials, improperly authorized the expenditure of VA funds to pay for academic degrees for OI&T employees. There was no documentation whatsoever to connect the academic training to the individuals' VA position and justify the training. Furthermore, OI&T managers were fiscally irresponsible when they not only authorized $139,330.88 in improper degree funding, but also by authorizing graduate degree funding at George Washington University, one of the nation's most expensive private universities. There is no evidence or documentation that would justify a GWU program or degree over those at other universities in Washington, DC.

OI&T did not have a program, as required by law, to allow VA to pay for academic degrees for its employees. In fact, in order to determine how much VA spent on each employee, we had to issue subpoenas to the universities in question. We found no existing OI&T system of records to account for VA funds spent for academic degree training or for the number of employees and types of programs enrolled in or completed. We found no documentation indicating that OI&T had a Masters Degree Program. We also found no records to reflect that funding was dispersed through a competitive process for selecting employees for academic degree training, ensuring that the educational institutions awarding an academic degree were accredited, or how such training would meet VA training needs, resolve an identified VA staffing problem, or accomplish a VA goal in the VA Strategic Human Capital Management Plan. Further, we found no records to indicate that employees sought their training through a Government source or from a source that was the least costly to the Government.

IMPROPER ADMINISTRATION OF AWARDS

Federal regulations require Federal employees to act impartially and to not give preferential treatment to any individual. VA policy authorizes awards to recognize individual employees who make contributions in support of the mission, organizational goals and objectives, and VA's Strategic Plan.

The September 4, 2007, OI&T Delegation of Authority Memorandum delegated award approval authority to the Principal Deputy Assistant Secretary and various Deputy Assistant Secretaries, Executive Directors, VACO Service Line Directors, and Regional Directors, as well as first and second line supervisors having the authority to approve performance and special contribution awards. Award limits were defined by management levels and further defined by individual and group amounts. The memorandum did not delegate any authority to approve incentive awards to the Director of the Executive Staff. A subsequent January 10, 2008, memoran-

dum rescinded the earlier one, and it issued new award guidance, including the position, Director of the Executive Staff, as an award approving official. Both the 2007 and 2008 memoranda identified the Principal Deputy Assistant Secretary and Deputy Assistant Secretaries as the only individuals authorized to act as both the recommending and approving officials.

OI&T senior managers recognized that there was an OI&T budgetary shortfall, but OI&T managers still spent over $24 million on awards and retention bonuses in a 2-year time period while working under a deficit. We recognize that OI&T's mass reorganization efforts were the major causes of the deficit; however, we found that not all managers were fiscally responsible when rewarding employees. One former VA official acted as if she was given a blank check book to write unlimited monetary awards. We also found that she failed to properly administer VA awards policy. Prior to the issuance of the September 2007 and January 2008 memoranda re-delegating the authority to approve awards, the former VA official was not authorized to approve awards; however, she improperly approved numerous awards worth tens of thousands of dollars. Additionally, she violated awards policy when she signed as both the recommending and approving official. Although our investigation focused on these specific allegations, we found similar violations of the awards policy by other OI&T managers.

We found four GS-15s who received about $60,000, $73,000, $58,000, and $59,000, respectively, over a 2-year period, with some personnel files containing insufficient or questionable justification. We found that various managers gave a GS-14 about $15,000 within a 9-month time period for the same body of work that was part of his primary job duties. Further, we identified two GS-5s who received 17 percent of the total amount of cash awards given to all GS-5s that year and who received awards for time periods that predated their employment. Additionally, we found a GS-13 employee who within the first 90 days of her employment received a $4,500 performance award from the former VA official who said that she did not even remember her.

A current and former DAS both told us that they were "stunned" by the total amount of appropriated funds that OI&T spent on awards/bonuses. Although we did not find that the dollar amounts given to each employee violated VA policy, we found that the money spent on many of the annual awards we examined were fiscally irresponsible, and in many cases, highly questionable.

Conclusion

In the two reports, we made over 40 recommendations to the Assistant Secretary for Information and Technology covering the issues discussed in this statement as well as others. He concurred with all of our recommendations and said that he would confer with the Office of Human Resources and Administration and the Office of General Counsel to ensure that appropriate administrative and corrective actions are taken. We will follow up in accordance with our policy to ensure that the recommendations are fully implemented.

Mr. Chairman, this concludes my statement and we would be pleased to answer any questions that you or other Members of the Subcommittee may have on these issues we have presented.

James J. O'Neill

James J. O'Neill was appointed in July 2006 as the Assistant Deputy Inspector General for Investigations. He is responsible for planning and directing investigations of alleged criminal activities related to VA programs and operations, as well as allegations of non-criminal misconduct committed by senior VA officials. Mr. O'Neill personally led the criminal and administrative investigations of the Montgomery County data loss in May 2006.

From 1999 until 2003, Mr. O'Neill served as the OIG's Chief Information Officer where he led efforts to modernize the information technology program.

Prior to joining the OIG in 1999, Mr. O'Neill completed a successful 23 year career with the U.S. Secret Service as Deputy Assistant Director for the Office of Training. In 1997, he was appointed as Special Agent in Charge in the Forensic Services Division and led the successful effort to gain the lab's first accreditation by the American Society of Crime Lab Directors. In 1971, Mr. O'Neill earned a B.A. degree in Political Science from La Salle University in Philadelphia, Pa. Prior to joining the U.S. Secret Service, he was employed as a high school teacher in Philadelphia public schools.

In 2008, Mr. O'Neill received a Presidential Rank Award for Meritorious Service.

[SPEECH]

Address to Graduates of the Combatant Command Joint Inspectors General Course

By Inspector General Gordon S. Heddell

Condensed from a speech delivered to the graduates of the Combatant Command Joint Inspectors General course on March 27, 2009, Fort Belvoir, Va.

Good morning and thank you for inviting me to address you on this occasion and to participate in your graduation from the Combatant Command and Joint IG course. I want to extend my appreciation to General Whitcomb [Army Inspector General], for hosting this beneficial course and for bringing us together today.

The opportunity to speak with you today is very special for two reasons. First, many years ago I had the honor of serving as a chief warrant officer in the Army flying helicopters.

So when I find myself in the company of members of our military or service veterans, I feel very much at home. Second, we share a common bond as inspectors general.

As a result, I really wanted to come up with something special for you today – something that would be relevant to both the military and the IG communities.

Well it just so happens that I found it – right in the middle of Gen. George S. Patton's famous speech to the Third Army.

And I'd like to read it to you now – of course with some of the general's more "colorful dialogue" deleted. He said: quote-

> "One of the bravest men that I ever saw was a soldier on top of a telegraph pole in the midst of a furious firefight in Tunisia. I stopped and asked what (the blank) he was doing up there at a time like that.
>
> He answered me saying: I'm 'Fixing the wire, Sir.'
>
> The general than asked him, 'Isn't that just a little unhealthy right about now?'
>
> The soldier looked at the general with a certain amount of caution and, He answered, 'Yes Sir, but the (darn) wire has to be fixed.'
>
> The general responded by asking- 'Don't those planes strafing the road bother you?'
>
> Without the slightest hesitation, the solider answered, 'No, Sir, but you sure as hell do!'
>
> And the general told the 3rd Army- Now, there was a real man. A real soldier."

I like this one because first and foremost, most people who have served in the military can relate to its humor.

But I also chose it because it illustrates that even though you may share some type of bond as a member of a military or civilian organization, your position may cause you to be regarded by others with some trepidation.

With General Patton, the reason was obvious. For those of us here, however – well, let me just say in my many years as an Inspector General, that there have been very few, if any occasions in which I ever heard someone say, "Oh boy, am I glad the IG is visiting us!"

That is why it is so important that we come together as we are now. We are members of a small community responsible for performing a vital but often misunderstood mission.

American industrialist Henry Ford said that "Coming together is a beginning…staying together is progress and…working together is success."

Your collaboration throughout this week and our meeting here today is an important step in our progress towards success in the Defense oversight community.

Defense Oversight

Let me start by thanking you for all you do to support our men and women both in and out of uniform. As members of the oversight community who oversee a Department as enormous as ours, I know that you have your work cut out for you. Incredible as it may seem, we are charged with protecting a force of over three million people and a budget exceeding $600 billion.

We serve two very important groups: our warfighters and the American people; therefore we must stay focused on issues that are important to the leadership and the Congress. We must attract and maintain a high quality and mission ready workforce.

We must ensure that high quality products are provided to the Department. We must:

- Avoid duplication of effort;
- Leverage each other's work when possible;
- Support each other's efforts and form partnerships; and
- Improve our ability to work together and to share lessons learned.

The Department of Defense is different than the other federal agencies in that there are internal Inspectors General, audit agencies, and investigative units that must work together to coordinate efforts. Two examples of essential collaborative efforts that I'd like to mention today are the Joint IG Activities Program and the International Contract Corruption Task Force.

Joint IG Program

First, the establishment of this course has resulted in success that we will continue to build upon by creating the Joint IG Activities Program. This program supports DoD IG's strategic priorities and the Secretary of Defense's priority of improving joint activities. This program is critical.

It has national interest and the potential for worldwide impact; it serves as a guide in oversight partnership and provides a foundation for an international concept for IG training. I'm excited about the impact that this program can have and I'm proud of all the effort that has gone into making it a success.

About the Joint IG Program

The Department of Defense Inspector General administers the DoD Joint Inspector General Program, in coordination with senior leaders of the Defense Council on Integrity and Efficiency. This program enhances the oversight of the Department by coordinating efforts and strengthening interagency relationships.

The program establishes a liaison office to interface with Joint IGs worldwide while interpreting and advising on doctrine and procedures; managing mobile training teams; producing publications and guidance; overseeing the Joint IG Qualification Course; and developing an integrated Joint Information Management network.

International Contract Corruption Task Force

One of the best stories regarding joint efforts, and certainly the best outcome for law enforcement organizations investigating and prosecuting the Global War on Terror, is the formation of the International Contract Corruption Task Force.

The mission of the task force is to deploy criminal investigative assets worldwide, to detect and investigate corruption and contract fraud, resulting primarily from the GWOT, and to successfully prosecute those cases.

The task force includes: the Defense Criminal Investigative Service; the FBI; the military services investigative units; the Special Inspectors General for Iraq and Afghanistan Reconstruction; and the Department of State and USAID Inspectors General.

The task force serves as a model for investigations where multiple federal agencies are involved in major procurements. There is no duplication of effort; information and intelligence are shared; resources are shared; and agents consult and assist each other. Numerous successful investigations have been coordinated through the task force; and the level of cooperation is unprecedented!

These types of joint work and collaborations are essential to ensuring that we are working together with a common vision and staying focused on issues that are important to accomplishing our mission.

The Warfighters

As I said earlier, we serve two groups: our warfighters and the American people. We have an awesome responsibility to ensure that the American taxpayer gets the most for their hard-earned dollars.

And we, as the DoD oversight community have a solemn duty to ensure that we do everything possible to provide our warfighters with the type of high quality, reliable equipment that will not only enable them to complete their mission, but also the ability to survive in hostile environments around the world.

There is no higher priority than the safety and security of the members

of our Armed Forces. As such, I have focused a significant amount of our resources on these areas, to include projects on Body Armor Testing, Health Care, Mine Resistant Ambush Protected Vehicles, and Electrocutions.

For example, properly tested body armor is critical to the safety of our troops. During a recent audit, we found that first article testing was not consistently conducted or scored in accordance with contract requirements. As a result, we determined that the Army did not have assurance that all inserts purchased under that contract provided the level of required protection.

We recommended that the Army identify and collect approximately 16,000 sets of ballistic inserts purchased under this contract and remove them from their inventory.

The Secretary of the Army disagreed with our finding but took action to ensure that there can be no question concerning the effectiveness of every soldier's body armor. This project is an example of dedication to ensure that every service member has the best and safest equipment possible.

Leadership

As all of you sitting here today are future IGs and leaders of the Defense oversight community; I want to close by talking about leadership and sharing an important story with you.

The story goes that sometime, close to a battlefield over 200 years ago, a man in civilian clothes rode past a small group of exhausted battle-weary soldiers digging an obviously important defensive position. The section leader, making no effort to help, was shouting orders and threatening punishment if the work was not completed within the hour.

"Why are you not helping?" asked the stranger on horseback.'

"I'm in charge here. The men do as I tell them," said the section leader, adding, "Help them yourself if you feel so strongly about it." To the section leader's surprise the stranger dismounted and helped the men until the job was finished. Before leaving, the stranger congratulated the men for their work, and approached the puzzled section leader.

"You should notify top command next time your rank prevents you from supporting your men - and I will provide a more permanent solution," said the stranger.

Up close, the section leader now recognized General Washington, and also the lesson he'd just been taught. There are two qualities that George Washington always displayed as a leader – selfless service and a commitment to taking care of people.

We have brave men and women on the battlefields. They are saying to us – we know that you will be the best leaders you can be – and you will not let us down. It is an awesome responsibility that we have. And now it is up to us to execute that responsibility properly.

Conclusion

In closing, I would like to thank so many of you who are on the front lines identifying and preventing fraud, waste, and abuse; and those of you who serve our country, sometimes in the most dangerous of places.

We in the IG community must continue to work together to ensure that we are covering all the bases, and not duplicating our efforts.

As you graduate together, let us remember that today is not the end, but only the beginning. We are all part of a much larger process – a process of learning, growing, and working together to succeed and I look forward to what the future holds for us. Thank you. Congratulations and good luck.

Gordon S. Heddell

Gordon S. Heddell was sworn in as the Inspector General for the Department of Defense on July 14, 2009, one year after being appointed as Acting Inspector General. Prior to joining the DoD IG, Mr. Heddell had served as the Inspector General at the U.S. Department of Labor for almost eight years. Mr. Heddell began his government service in 1966 as an army chief warrant officer, helicopter pilot, serving in both Korea and Taiwan during the Vietnam-era conflict.

Following his military tours of duty, Mr. Heddell served for 29 years in the U.S. Secret Service, where he held various positions involving administrative operations, protection of presidents and vice presidents, and criminal investigations. The highlights of his career with the Secret Service include serving as the deputy assistant director responsible for the overall training of the Secret Service's employees; assistant special agent in charge in Washington where he investigated all threats made against the president and vice president; and assistant special agent in charge where he supervised complex criminal investigations related to counterfeiting and financial fraud.

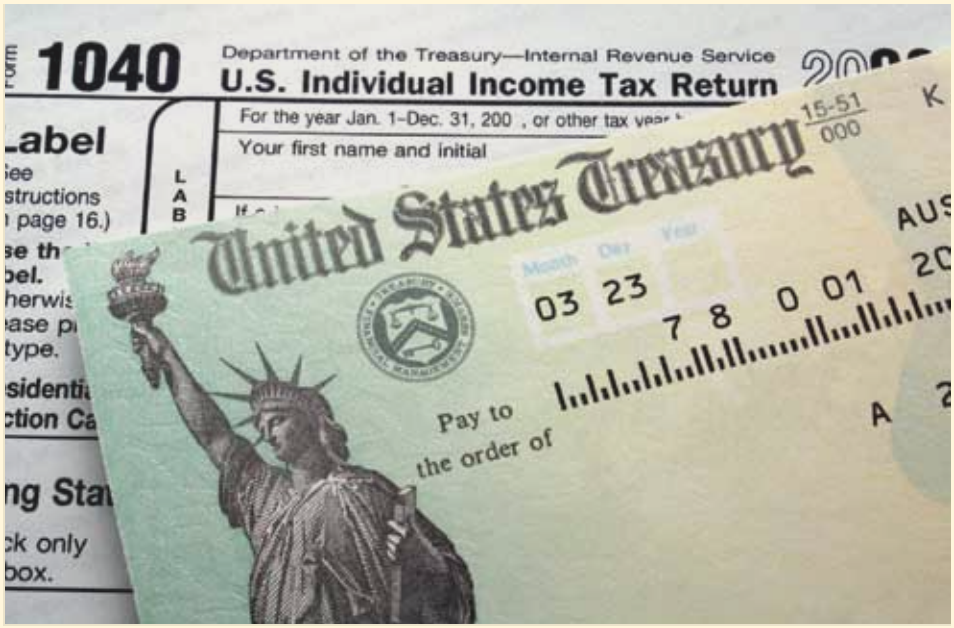
Mr. Heddell holds a B.A. in Political Science from the University of Missouri, a M.A. in Legal Studies from the University of Illinois, and was a Woodrow Wilson Public Service Fellow while at the Secret Service.

[SPEECH]

Address to the National Association of Tax Professionals 2009 Annual Conference

By Inspector General J. Russell George

Reprinted from a speech delivered to the National Association of Tax Professionals 2009 Annual Conference on July 21, 2009



Good afternoon. Thank you for that introduction, and as stated, I am Russell George, the Treasury Inspector General for Tax Administration. I appreciate the opportunity to address this important gathering.

I would like to begin by telling you a story. It's a story about Randy Nowak, a Florida businessman and owner of R.J. Nowak Enterprises.

In 2008, Mr. Nowak was being audited by the Internal Revenue Service. At the time, he had an outstanding personal income tax liability of approximately $300,000. In addition, based on his own statements, he had approximately $4,000,000 hidden offshore in a Jamaican bank account that he was concerned the IRS would discover. He also had four years of outstanding corporate tax returns for his business that he had not filed.

Many of you would agree that a taxpayer faced with a similar dilemma should probably hire an Enrolled Agent or a CPA or tax attorney to help the taxpayer negotiate a settlement in order to close the audit. Mr. Nowak . . . decided to hire a hit man . . . in order to murder the IRS agent auditing him. Nowak told an associate that the IRS agent had all of Nowak's paperwork, and if Nowak had the agent "bumped off," that would be the end of the paper trail.

In July 2008, Mr. Nowak met with a hit man in a Home Depot parking lot. Nowak handed the hit man an envelope containing ten thousand dollars in cash, which was a deposit for the twenty thousand dollars that Mr. Nowak intended to pay for the murder of the IRS agent. After identifying the IRS agent in a photograph and providing the hit man with the agent's home address, Nowak asked how much more it would cost him to have the local IRS building, "severely damaged." The two men agreed that the hit man would first take care of Nowak's original request - killing the IRS agent - and then they would talk about burning down the IRS office.

Unbeknownst to Mr. Nowak, the hit man was an undercover agent, and in March 2009, Mr. Nowak was sentenced to thirty years in federal prison for attempting to murder a government employee.

While this story has a happy ending - though not for Mr. Nowak but certainly for the IRS agent and the rest of us in general - it is just one of the many cases investigated each year by our Office of Investigations, which is an integral part of the Treasury Inspector General for Tax Administration, or TIGTA. Our Office of Investigations, along with our Office of Audit and our Office of Inspections and Evaluations, allow TIGTA to carry out its mission of safeguarding the integrity, and promoting the efficiency, of America's tax system.

Today, I will address TIGTA's role in the government's oversight of the tax preparer community - including recent audit reports and investigations that affect tax return preparers - and the critical role that tax return preparers have in ensuring the continued success of federal tax administration. I will next address the topic that I am sure is on everyone's mind. I am, of course, referring to the Commissioner of Internal Revenue Douglas

Shulman's recent announcement regarding plans to issue recommendations by the end of the year for increasing taxpayer compliance and ensuring high ethical standards of conduct for paid tax return preparers. But first, for those of you who may not be familiar with TIGTA, allow me to provide you with a brief overview.

TIGTA was created by Congress as part of the *IRS Restructuring and Reform Act of 1998* in order to provide independent oversight of the Internal Revenue Service. We are a successor organization to the IRS Inspection Service, which had been formed in 1952 in response to widespread allegations of corruption within the IRS.

TIGTA is a multifaceted organization that includes three primary operating divisions.

First, our Office of Investigations consists of federal agents who protect the IRS from external attempts to harm or corrupt IRS employees, facilities and infrastructure. TIGTA agents investigate attempts by taxpayers or others to bribe or threaten IRS employees. They investigate tax return preparers who engage in schemes to defraud their clients and the government. And they also investigate misconduct by IRS employees, including IRS employees who solicit bribes or who improperly access confidential taxpayer information.

Second, TIGTA's Office of Audit consists of auditors who conduct comprehensive reviews of IRS programs, systems and policies and provide recommendations for improving all aspects of the IRS's administration of the federal tax system. For example, they have recently issued reports addressing the increasing number of fraudulent refund claims processed by the IRS. They also have determined that the IRS has insufficient controls in place to monitor the accuracy of the direct deposit of refunds into taxpayer bank accounts. And they have called for improvements in the IRS's processing of carry back loss claims in order to ensure that taxpayers receive accurate refunds.

Their audit reports, which are available on our Web site, often result in substantial cost savings by identifying and recommending material improvements to IRS programs and procedures. As a result, our Office of Audit provides an excellent return on investment to the American taxpayer. During Fiscal Year 2008, the Office of Audit issued one hundred seventy nine audit reports identifying more than $2.4 billion in potential cost savings, thereby providing taxpayers with $67 in benefits for each dollar invested in the Office of Audit.

Lastly, our newest component is our Office of Inspections and Evaluations. Their inspections monitor the IRS's compliance with various programs and policies and assess the effectiveness and efficiency of IRS operations. Recent reports have addressed the need for legislative actions to reduce the multi-billion dollar U.S. international tax gap and examined the IRS's ability to protect personally identifiable information when such information is transported from one IRS office to another.

TIGTA's oversight responsibilities extend not only to the IRS, but, in addition, to the IRS Office of Chief Counsel and the IRS Oversight Board. As an independent office within the Department of the Treasury, I report directly to the Treasury Secretary and to Congress.

Oversight of the IRS is not an easy task. The IRS is one of the largest governmental organizations in the world, with approximately one-hundred thousand employees. Each year the IRS collects almost $3 trillion in taxes and issues approximately $430 billion in tax refunds. As IRS Commissioner Douglas Shulman has said, the IRS is the "face of government." Each year, it interacts with practically every American adult and business. Few, if any, government agencies can make the same claim.

Monitoring IRS activities is a formidable challenge, but it is one that the men and women of TIGTA are committed to carry out with the highest level of professionalism, quality and service. After all, the IRS's performance - from how efficiently and effectively it collects taxes to how well it helps taxpayers and tax return preparers comply with filing obligations - is critical to our nation's economic well-being.

As we will further discuss, we are reaching out to you, the tax preparer community, to ask for your help in carrying out our mission. We look forward to continuing to work with all of you in making sure that the integrity of the American tax system is preserved no matter what challenges our country may face in the years ahead.

Let's spend a few minutes discussing the very specific and also the very critical role that TIGTA's Office of Audit and Office of Investigations play in the government's oversight of the tax preparer community. I will begin with our Office of Audit.

This year, as well as in prior years, TIGTA's Office of Audit issued several reports identifying weaknesses in IRS programs and policies affecting tax return preparers.

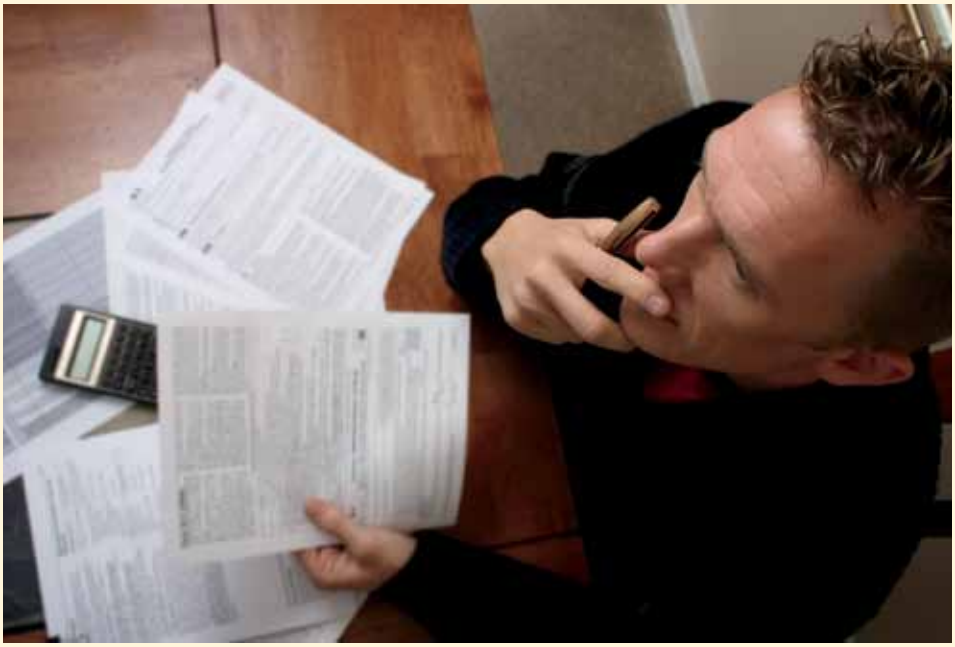
In a report issued in February, TIGTA found that the process that taxpayers must use to report complaints against tax return preparers is ineffective. The IRS processed approximately eighty three million individual federal income tax returns in calendar year 2007 that were prepared by paid tax return preparers. However, the IRS cannot determine how many complaints against tax return preparers it receives, how many complaints are investigated, and the total number of multiple complaints filed against a specific preparer or firm. As a result, the IRS is not able to evaluate

such data in order to understand the root causes of taxpayer problems, identify areas of noncompliance and address procedures that need improvement.

TIGTA recommended that the IRS should clarify the guidance that it issues to taxpayers regarding the preparer complaint process. In addition, it should develop a standard form for tax return preparer complaints that includes items necessary for the IRS to appropriately evaluate the legitimacy of such complaints. Once the form is developed, a database or tracking system should be implemented to monitor such complaints. In response to our report, the IRS agreed to update its guidance regarding tax return preparer complaints and address the other recommendations made in the report.

In another report, also issued in February of this year, TIGTA found that tax practitioners who promoted abusive tax shelters continue to be able to represent taxpayers before the IRS. The IRS Office of Professional Responsibility, or OPR, regulates the conduct of licensed tax professionals who act as power of attorneys for taxpayers that might be involved in an audit, collection proceeding or an appeal of an IRS determination. TIGTA found that OPR was unaware of a significant number of licensed tax practitioners who were assessed penalties, sentenced in a criminal proceeding or otherwise ordered by a court to stop practicing due to tax shelter violations. As a result, these tax practitioners were still eligible to represent taxpayers before the IRS.

The report noted that misconduct by such practitioners can erode public confidence in the tax system and create unfortunate consequences for taxpayers. We recommended that, among other things, the Office of Professional Responsibility determine whether additional disciplinary actions are warranted for tax practitioners who were punished



for abusive tax shelter violations. We also recommended that OPR establish written procedures for controlling and reviewing referrals of such practitioners from other IRS operating divisions. IRS management agreed with all of our recommendations.

Two additional audit reports, both issued in 2006, highlighted other weaknesses with respect to the Office of Professional Responsibility's oversight of tax practitioners. In one report, TIGTA found that the Office of Professional Responsibility does not always ensure that enrolled agents are qualified to represent taxpayers. The report found that OPR does not have consistent criteria for issuing enrolled agent licenses, verifying tax compliance and criminal backgrounds of enrolled agents, or identifying enrolled agents who are no longer eligible to represent taxpayers. As a result, taxpayers cannot be assured that enrolled agents are eligible to represent them before the IRS and have the requisite technical skills to provide such representation.

TIGTA recommended, among other things, that OPR implement processes for conducting criminal background checks on persons who apply to become enrolled agents and identify enrolled agents who are not compliant with their own federal tax obligations. IRS management agreed with our recommendations.

In the second report issued that same year, TIGTA found that the Office of Professional Responsibility needs to improve its ability to identify and take action against incompetent and disreputable tax practitioners. The study found that there are a significant number of tax practitioners whose conduct appears to warrant disciplinary action by the IRS but who have not been identified by OPR. In particular, some tax practitioners who have been convicted of tax-related crimes or whose licenses have been suspended or revoked by State authorities have not been suspended from practice before the IRS.

TIGTA recommended that, among other things, OPR should develop a process to obtain relevant information on State disciplinary actions by coordinating with State licensing authorities such as State bar associations and boards of accountancy. IRS management agreed with this recommendation.

TIGTA's Office of Investiga-

tions also has a role to play with respect to oversight of the tax preparer community. As I mentioned earlier, our Office of Investigations investigates tax return preparers who engage in schemes to defraud their clients and the government.

We routinely investigate the following three types of allegations involving tax return preparers. First, TIGTA investigates preparers who overstate their qualifications - for example, those who falsely claim to be licensed attorneys, certified public accountants or enrolled agents. Second, We investigate preparers who steal clients' tax payments or tax refunds. And third, TIGTA investigates preparers who impersonate IRS employees or misuse the IRS seal or logo. These are all activities that damage the reputation of the tax preparation industry as well as the overall integrity of tax administration.

Allow me to elaborate by providing you with examples of several actual pleas and convictions of tax return preparers that resulted from TIGTA investigations.

In January of 2009, Abdul Wahid pleaded guilty in California to mail fraud, theft of government property and aggravated identity theft and was sentenced to one hundred and thirty-two months in prison. According to court documents, Wahid owned and operated a tax return business in Los Angeles called Global Accounting and Tax Service where he would prepare personal and corporate tax returns for his clients. Those returns would show significant amounts of tax due to various taxing authorities.

Wahid would direct his clients to give him checks in the amounts of the taxes due, as reflected on the return, by falsely representing that he had already paid the tax owed to the relevant taxing authority and that the client needed to reimburse him. He would then deposit the checks into his own accounts and not pay his clients' taxes. In order to avoid detection, Wahid would prepare different returns showing little or no tax due and submit those returns to the taxing authorities.

Another example is James Richards, a tax preparer, who in July of 2008 was sentenced in a Missouri federal court for embezzling payments intended for the IRS. As the owner of Holliday and Associates, Richards was hired by his clients to prepare and file their tax returns as well as make their federal tax deposits in a timely manner.

Richards routinely asked clients to make payments toward their anticipated tax liability to him or his company but would then fail to make the clients' required tax deposits, pay over their estimated tax payments or even file the required forms with the IRS. He also falsely represented himself as a CPA in documents submitted to the IRS. Richards was sentenced to almost seven years in prison without parole and ordered to pay restitution of over $380,000 dollars.

In April of 2008, Morgan Taylor Mayfaire was indicted in U.S. District Court on 35 counts of preparing fraudulent tax returns and eight counts of falsely pretending to be an IRS employee. According to court documents, she prepared tax returns for her clients, and in return, her clients paid her fees in the amount of 10 percent of the refund claimed on their returns. Mayfaire caused approximately $475,000 to be fraudulently refunded by the IRS to her clients. She did so by willfully aiding and assisting in the preparation of Forms 1040 and 1040X with fictitious or inflated deductions that she knew the taxpayers were not entitled to claim.

In furtherance of this scheme, she also pretended to be an IRS employee by falsely representing to taxpayers that, as an IRS employee, she had ways of increasing taxpayer deductions on tax returns that no other person would know. She thereby induced taxpayers to hire her to prepare their taxes, file false tax returns, collect improper tax refunds, and to pay her fees.

In March of 2008, Angelo Principio was indicted in U.S. District Court for theft of public money. According to court documents, Principio was the principal owner and operator of Jersey Tax and Financial Services located in Middlesex, New Jersey. Jersey Tax and Financial Services provided a variety of services to its clients, including the preparation and filing of electronic federal income tax returns.

From January 2005, through December 2006, Principio and other individuals knowingly converted to their own use approximately $225,000 dollars through a tax refund scheme. As part of their scheme, Principio and others signed accurate federal tax returns for their clients and provided them with hard copies of these returns. Without the knowledge or consent of the taxpayers, Principio and others then created, substituted, and signed inaccurate tax returns which inflated the tax refund amounts. These fraudulent tax returns were filed electronically with the IRS. The fraudulently procured tax refund checks were then forwarded to Principio, who used the improperly obtained funds for his own personal benefit.

A final illustration dates to March of this year when a federal grand jury returned a 17 count indictment charging Keith Thayer Towns, of Fairfield, California, with 16 felony charges of false statements to the IRS and one misdemeanor charge for misusing the name of the IRS. The indictment alleges that from March 2004 to March 2009, Towns submitted Power of Attorney forms to the IRS in which he falsely represented that he was an Enrolled Agent certified by the IRS. The indictment further alleges that Towns advertised that he was an Enrolled Agent on his Web site.

All of us can agree that we cannot allow this type of misconduct by tax return preparers to continue. Not only are these actions illegal and unethical, but they also severely damage the credibility and reputation of the entire tax preparation community. Our investigators ask for your help in identifying such unscrupulous preparers.

TIGTA periodically receives allegations about preparers who have stolen tax payments intended for the IRS or tax refunds intended for their clients. These often come from preparers who are working with new clients. These clients may come to you because they did not get their refund in a timely manner or they received an inquiry from the IRS about a missed payment or have had a lien placed on their property.

If you suspect that a preparer has misrepresented his or her qualifications or is engaging in a scheme to defraud clients or the government, we ask you to call our hotline.

Similarly, if you suspect that your client intends to bribe or harm an IRS employee, or if you learn of an IRS employee soliciting a bribe from you or your client, we ask you to call our hotline. Our investigators routinely receive calls from tax practitioners, and they are specifically trained to deal with these types of situations.

TIGTA's Office of Audit also works with tax return preparers. Our auditors are interested in hearing about your experiences with the IRS. They are interested in hearing what you think works and what doesn't, and what is overly burdensome to you and your clients. Your feedback, based on your experience, is welcomed and appreciated. In addition, our auditors are interested in hearing from you about any areas of federal tax administration that you believe can be streamlined, made more efficient or otherwise made more user-friendly.

More than half of all taxpayers come to you as tax return preparers to have their taxes prepared and filed. You know what questions they are asking, and you know where the difficulties lie. Your first-hand knowledge and interaction with taxpayers and their concerns provides invaluable insight that is welcomed by our audit teams when it comes to reviewing and making recommendations to the IRS. As a valuable part of tax administration, your input is greatly appreciated.

Now let's turn to the topic that is probably on everyone's mind - the IRS Commissioner's recent announcement regarding recommendations that he plans to issue by the end of the year for increasing taxpayer compliance and ensuring high ethical standards of conduct for paid tax return preparers.

As all of you know, tax return preparers are an important part of the federal tax system and provide a highly valuable service to their clients. They not only ensure that their clients are able to successfully navigate an increasingly complex tax code and satisfy filing obligations, but they also play a key role in educating clients about the tax code and the importance of tax compliance.

On the other hand, unqualified or unethical tax return preparers can cause enormous damage to the federal tax system, to taxpayers and to the tax preparer community as a whole. Currently, there are no national standards that preparers are required to satisfy before selling tax preparation services to the public. In most States, anyone - regardless of training, experience, skill or knowledge - is allowed to prepare federal income tax returns for others for a fee.

Recently, IRS Commissioner Douglas Shulman announced that, by the end of the year, he will make recommendations to the Treasury Secretary and the President on how to better leverage the tax preparer community for the overall benefit of the tax system. The Commissioner will issue his recommendations after conducting numerous meetings throughout the summer with taxpayers, tax return preparers and other constituents. TIGTA, along with the National Taxpayer Advocate, support the Commissioner's efforts to address these matters.

TIGTA has been at the forefront of recommending that the IRS require the use of a single federal identification number for each paid preparer as part of its oversight of tax preparers.

We have called for the use of a single identification number since 2006. More recently, in a September 2008 audit report, TIGTA found that a majority of tax returns prepared by a sample of unenrolled preparers contained substantial errors. During the 2008 filing season, TIGTA auditors posed as clients in a large metropolitan area and paid to have tax returns prepared at twelve commercial chains and sixteen small, independently owned tax return preparation offices. The preparers in the sample were unlicensed and un-enrolled.

TIGTA found that these preparers made substantial errors when com-

pleting tax returns and correctly prepared only thirty-nine percent of the returns. Of the sixty-one percent of the returns that were prepared incorrectly, sixty-five percent contained mistakes and omissions that were considered to have been caused by human error or misinterpretation of the tax laws. The remaining thirty-five percent contained misstatements and omissions that were considered to have been caused by willful or reckless conduct.

To help alleviate these problems, we recommended that the IRS develop and require identification numbers for all paid preparers, which would enable the IRS to better identify and evaluate problems with compliance.

Just yesterday, TIGTA reiterated its call for the use of unique federal identification numbers in an audit report which found that inadequate data on paid preparers impedes effective oversight of tax return preparers by the IRS. The report found that while more than half of all tax returns filed with the IRS are prepared by tax preparers, the IRS cannot determine the population of preparers or whether the preparers are compliant with their own tax obligations, or with other tax laws and regulations.

The IRS maintains significant data on paid preparers, but it is not feasible to use such data to track or monitor preparers' activities and compliance because preparers use multiple identifying numbers when dealing with the IRS.

Under current law, preparers are not required to use a single identifying number on returns that they prepare for a fee. While the IRS requires paid preparers to sign the tax returns they prepare, preparers may identify themselves using either a Social Security Number or a Preparer Tax Identification Numbers, or PTIN. If a preparer is self-employed or a member of a firm, he or she is also asked to provide an Employer Identification Number, or EIN.

The IRS, however, does not validate preparers' identifying numbers - EINs, PTINs or Social Security Numbers - when processing returns. Furthermore, tax returns filed without identifying numbers are not rejected because processing returns is a priority for the IRS. In fact, hundreds of thousands of tax returns filed by preparers in calendar year 2008 contained no identifying numbers.

Data on preparers are decentralized among more than twenty different IRS systems that are not integrated, and there currently are no data standards among these systems to easily match preparer information.

Test results from a statistical sample of one hundred thirty-nine preparers demonstrated many of the challenges the IRS would face in attempting to identify the population of preparers. For example, multiple identifying numbers were used by sixty-three percent of the preparers in the sample - that is, preparers would use one identifying number, such as their Social Security Number, on certain returns they prepared for a fee and a different identifying number, such as their PTIN, on others returns prepared that same year.

Certain preparers were found to have used their Employer Identification Numbers instead of their Social Security Numbers or PTINs when identifying themselves on returns. And six percent of the preparers in the sample could not be identified at all because the identifying numbers they provided were invalid.

The names of the one hundred thirty-nine preparers in various IRS systems were inconsistent forty-five percent of the time. And five percent of the preparers in the sample were found not to be compliant with their own tax obligations.

A unique identifying number for each preparer along with an effective management information system are necessary in order for the IRS to facilitate tax administration and provide effective oversight of preparers. Requiring that all preparers use a unique identifying number would allow the IRS, for example, to use the PTIN application process to identify the population of preparers.

Since fiscal year 2005, the IRS's strategic plans have included an objective to ensure that accountants, attorneys and other tax practitioners adhere to professional standards and follow the law. Since fiscal year 2006, TIGTA has identified concerns that could prevent the IRS from effectively identifying all preparers or enforce the requirement for preparers to sign tax returns and/or provide identifying numbers. Requiring a PTIN for all preparers would help provide the standardization that the IRS needs to identify the preparer population and enforce the Internal Revenue Code.

Our report recommended that the IRS complete its study on requiring preparers to use a single identification number when filing returns in time for the 2011 filing season. The IRS also should develop a method to enforce Internal Revenue Code Section 6695(c) that imposes a penalty on preparers who do not provide an identification number on tax returns they prepare. TIGTA also recommended legislative changes to require paid preparers to be compliant with their own federal tax filing requirements in order to be allowed to prepare tax returns for others for a fee.

In response to our audit report, the IRS agreed in principle that preparers should use a single identification number when filing tax returns. The IRS further stated that the tax return preparer review currently underway is expected to encompass this issue as part of the IRS Commissioner's comprehensive recommendations to be issued by the end of the year.

Several other agencies and organizations have commented in the past

about proposed changes to the IRS's oversight of tax return preparers.

For example, the National Taxpayer Advocate made three specific recommendations in her recent 2009 report to Congress. First, she stated that the IRS should work with the Treasury Department to recommend enactment of legislation to regulate federal tax return preparers, including registration of unenrolled preparers, a basic examination to ensure a minimum level of competency among paid preparers and continuing professional education requirements.

Second, the Advocate called for additional IRS enforcement actions directed at return preparers who fail to perform due diligence or consciously facilitate noncompliance. Third, she recommended the mandatory use of PTINs by preparers in order to enable the IRS to identify return preparers who submit unreasonably high rates of inaccurate returns.

In 2008, the General Accountability Office, or GAO, also recommended the use of single identification numbers for paid preparers. And more recently - in fact, just last week - the Director of the IRS Office of Professional Responsibility commented on the use of preparer identification numbers. It remains to be seen, however, whether licensure, certification and continuing education requirements - as well as single identifying numbers - will be part of the Commissioner's final recommendations regarding preparer oversight.

Several bills have been introduced over the years containing proposals to regulate tax return preparers, and, in 2005, the House Committee on Ways and Means, Subcommittee on Oversight, held a hearing at which representatives of five organizations testified with respect to the regulation of return preparers. One of the groups was the National Association of Tax Professionals.

As many of you know, in 2005, the NATP issued recommendations for legislation to register paid income tax preparers. NATP's recommendations included registration or licensure of paid preparers - possibly through the existing PTIN system - in order to enable taxing authorities to determine the number of people that prepare tax returns and the quality of the work that they do. NATP also called for minimum standards testing and education requirements.

While the Commissioner's recommendations with respect to the tax preparation industry will not be presented until at least the end of the year, I encourage all of you to participate in the comment process by attending the various town hall meetings that the IRS will hold throughout the country. In fact, the IRS has already scheduled its first forum in Washington, D.C., on July 30th. I understand that the National Association of Tax Professionals is scheduled to be one of the groups represented at the forum, and I encourage you to continue to participate in the process throughout the rest of the year.

I close this session by reiterating the fact that we all must work together to ensure the integrity of the Nation's tax system. Throughout this presentation, I called for your participation and involvement in our activities, including visiting our Web site at www.tigta.gov, emailing our TIGTA Hotline Complaints Unit at Complaints@tigta.treas.gov and/or calling our TIGTA Hotline at 1-800-366-4484.

The work we do affects you and your clients, and it is in the best interest of your clients - as well as all taxpayers - that we do our best to ensure that their taxes are collected effectively and efficiently and that the integrity of our Nation's tax system is preserved.

Thank you again for the opportunity to speak with you today, and I hope you enjoy the rest of the conference.

J. Russell George

J. Russell George was confirmed by the U.S. Senate in November 2004, as the Treasury Inspector General for Tax Administration. Prior to assuming this role, Mr. George served as the Inspector General of the Corporation for National and Community Service, having been nominated to that position by President George W. Bush and confirmed by the U.S. Senate in 2002.

Mr. George received his B.A. from Howard University in Washington, DC, and his Doctorate of Jurisprudence from Harvard University's School of Law in Cambridge, Mass.

Following his work as a prosecutor, Mr. George joined the Counsel's Office in the White House Office of Management and Budget where he was assistant general counsel. He was next invited to join the White House staff as the associate director for policy in the Office of National Service. He then returned to New York and practiced law at Kramer, Levin, Naftalis, Nessen, Kamin & Frankel.

In 1995, Mr. George served as the staff director and chief counsel of the Government Management, Information and Technology Subcommittee (later renamed the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations), chaired by Representative Stephen Horn. He continued in that position until his appointment in 2002.

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 emailed to: JournalofPublicInquiry@dodig.mil

To join the mailing list, please provide your name and address by email to: JournalofPublicInquiry@dodig.mil

Journal of Public Inquiry

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

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

In order to create independent and objective units--

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

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

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