

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

The Journal of Public Inquiry



SPRING/SUMMER

2010

COUNCIL OF INSPECTORS GENERAL ON
INTEGRITY AND EFFICIENCY

Council of Inspectors General on Integrity and Efficiency

Members of the Council

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

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

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 73 Inspectors General from the following federal agencies:

Agency for International Development
Department of Agriculture
Amtrak
Appalachian Regional Commission
Architect of the Capitol
U.S. Capitol Police
Central Intelligence Agency
Department of Commerce
Commodity Futures Trading Commission
Consumer Product Safety Commission
Corporation for National and Community Service
Corporation for Public Broadcasting
Defense Intelligence Agency
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 Geospatial-Intelligence Agency
National Labor Relations Board
National Science Foundation
National Reconnaissance Office
Nuclear Regulatory Commission
National Security Agency
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

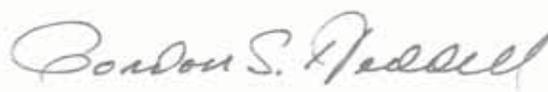
Inspectors General, like all government agencies, must continually assess the impact of contemporary events on their mission. In recent years, government oversight has been significantly influenced by events such as terrorist attacks, U.S. military engagements overseas, natural disasters, and economic recession. New trends and developments will continue to challenge Inspectors General to transform their agencies to ensure that oversight efforts are timely and relevant.

One such trend involves the extent to which Inspectors General are being called upon to identify potential cost savings within their respective departments and agencies. During periods of economic uncertainty, the duty of Inspectors General to promote efficiency becomes even more prominent. Inspectors General are expected to provide the tough oversight and spending accountability that the American taxpayers deserve.

Another trend stems from the ever-expanding role that communications and technology plays in the day-to-day affairs of Inspectors General. As the communications environment continues to change and information is exchanged in mass quantities with lightning speed, it is important that organizations take advantage of the opportunities afforded by technological developments that can be utilized to enhance audits and investigations. It is exceptionally difficult to keep pace with technological advancements, but doing so is necessary to improve the manner in which Inspectors General perform their mission.

This edition of the *Journal* includes six articles that address curbing wasteful spending, the Federal Conflict-of-Interest statute, investigating child pornography offenses by government employees, examining mortgage fraud, whistleblowing within the Intelligence Community, and familial DNA database searching. In addition, this issue contains prepared statements to Congress by two Inspectors General. The first addresses how to combat providers that abuse the health care system and the second regards the use of internal controls to safeguard United States funds for reconstruction in Afghanistan from fraud and corruption. This issue depicts the diversity of Inspectors General activities to meet challenges and realize the goals of complicated and vital missions.

It is important that we continue to collectively communicate ideas and share solutions. Thanks to your participation and input, the *Journal* remains a means of promoting oversight, accountability, and positive change. We are grateful to the editorial board and the authors for their significant contributions.



Gordon S. Heddell
Inspector General

Journal of Public Inquiry

DEPARTMENT OF DEFENSE INSPECTOR GENERAL STAFF

EDITOR-IN-CHIEF Gordon S. Heddell

PUBLISHER John R. Crane

EDITOR Jennifer M. Plozai

GRAPHIC DESIGN ASST. Jacob A. Brown

PUBLICATION SPECIALIST Katherine Y. Klegin

LEGAL EDITOR Paul W. Knoth

EDITORIAL ASST. Jamie L. Critchfield

ADMINISTRATIVE ASST. Helen M. Aaron

JOURNAL EDITORIAL BOARD

Gregory H. Friedman
Inspector General
Department of Energy

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

Mary L. Kendall
Acting Inspector General
Department of the Interior

Allison Lerner
Inspector General
National Science Foundation

Richard Moore
Inspector General
Tennessee Valley Authority

Kathleen S. Tighe
Inspector General
Department of Education



Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

- 1** **The Federal Government's Efforts to Curb Wasteful Spending: A Look at the Executive Order to Reduce Improper Payments from an IG's Perspective**
Written by Patrick P. O'Carroll, Jr.
Social Security Administration Office of Inspector General
- 6** **Issues Regarding the Federal Conflict-of-Interest Statute**
Written by Mark L. Greenblatt
Department of Justice Office of Inspector General
- 11** **Child Pornography Offenses By Government Employees**
Written by Chad Steel and Lauren Henry
Central Intelligence Agency Office of Inspector General
- 15** **HUD Watchdog Sniffing Out Mortgage Loan Fraudsters**
Written by Kimberly R. Randall
Department of Housing and Urban Development Office of Inspector General
- 20** **Intelligent Whistleblowing**
Written by Lindsay Boyd and Brian Futagaki
Department of Defense Office of Inspector General
- 24** **Familial DNA Database Searching**
Written by Fitzhugh L. Cantrell
Naval Criminal Investigative Service
- 28** **Strengthening Integrity: New Tools in the Affordable Care Act**
Testimony by Lewis Morris
Department of Health and Human Services Office of Inspector General
- 35** **Oversight of U.S. Civilian Assistance for Afghanistan**
Testimony by Donald A. Gambatesa
United States Agency for International Development Office of Inspector General

☞ Denotes the end of an article.

Disclaimer: The opinions expressed in the Journal of Public Inquiry are those of the authors. They do not represent the opinions or policies of any department or agency of the U.S. government.

THE FEDERAL GOVERNMENT'S EFFORTS TO CURB WASTEFUL SPENDING

A Look at the Executive Order to Reduce Improper Payments from an IG's Perspective

BY INSPECTOR GENERAL PATRICK O'CARROLL, JR.

Federal agencies made nearly \$110 billion in improper payments in fiscal year 2009—the highest amount to date, an amount President Obama recently called, “unacceptable.” As Office of Inspector General employees we appreciate that taxpayers deserve to know that their dollars are spent wisely and effectively; when government benefits are administered, the right people need to receive the right payment at the right time. Since the president signed Executive Order 13520 on Reducing Improper Payments in November 2009, federal agencies and their inspectors general have worked closely with the Office of Management and Budget, and the U.S. Treasury, to identify improper payments and design solutions to reduce wasteful spending.

The Office of Inspector General at the Social Security Administration has had an interesting view of the process since the executive order was signed, because the order included a number of provisions that required input from the Council of Inspectors General on Integrity and Efficiency. SSA OIG was asked to serve as a liaison for the CIGIE to work with OMB on the implementation of the order; that liaison role has included attending workgroup meetings, reviewing and commenting on work plans, and coordinating among IGs, OMB, and the U.S. Treasury.

Significant progress has been made to reduce improper payments since November 2009. The order outlined a



strategy to reduce improper payments by boosting transparency, holding agencies accountable, and creating strong incentives for compliance. In March, the president directed all federal agencies to expand their payment recapture audits, and in June, he followed up by establishing a federal “Do Not Pay List” so that there is one source for agencies to check on the eligibility status of an individual or contractor. Recently, the president signed into law the *Improper Payments Elimination and Recovery Act* to help achieve his new goal of reducing wasteful spending by \$50 billion by 2012.

Reducing improper payments is among the president's top priorities. Federal agencies are being asked to improve the reporting of improper payments and the controls they have in place to limit those payments. As an agency IG, we are focused on assisting our agency, SSA, in that process, as well as offering any guid-

ance needed from OMB in moving forward.

TRACKING IMPROPER PAYMENTS

Improper payments are payments from a federal program that should not have been made or were made in an incorrect amount; not all improper payments are overpayments, as underpayments may also be considered improper. Improper payments cover a number of financial transactions, such as incorrect payments to individuals or firms or benefit payments to ineligible program participants. These payments can be the result of documentation and administrative errors, authentication and medical errors, or verification errors. Some examples of improper payments are payments made to an ineligible recipient, duplicate payments, or payments for services not received. Additionally, when an agency's



review is unable to determine the accuracy of the payment, the payment must also be considered an error.

In fiscal year 2009, 78 government programs were deemed “susceptible,” meaning that the programs had more than \$10 million in improper payments, but seven “high-priority” programs drew the most attention because they all reported improper payments in excess of \$1 billion in the previous fiscal year. The Department of Health and Human Services, which administers the Medicare and Medicaid programs, led all of the “high-priority” programs with \$66.4 billion in improper payments. The Department of Labor, in charge of unemployment insurance, had \$12.3 billion; SSA’s retirement and disability programs had \$8 billion; the Department of Agriculture, which runs the School Lunch program and Supplemental Nutrition Assistance, had \$4.3 billion in improper payments; and the Department of Transportation, which handles Federal Highway Planning and Construction, had \$1.5 billion. The Department of Housing and Urban Development and the U.S. Treasury rounded out the seven

agencies running “high-priority” programs.

According to the White House, these improper payments included payments made in error or because of fraudulent claims by contractors and organizations, as well as benefits sent to individuals who are deceased or in jail. In fact, over the past three years, federal auditors reported that the government paid out benefits totaling more than \$180 million to approximately 20,000 Americans who were deceased; and more than \$230 million in benefits to approximately 14,000 fugitive felons or prison inmates that were not eligible for benefits.

Federal agencies are deep in the process of identifying their improper payments and the reasons for these errors. SSA, for example, identifies its improper payments through stewardship reviews of the nonmedical aspects of Retirement, Survivors’, and Disability Insurance and Supplemental Security Income on an annual basis. Between fiscal years 2004 and 2008, SSA reported about \$5.8 billion in improper payments paid to retirement and survivors’ beneficiaries about

\$8.1 billion in improper payments paid to disability insurance beneficiaries and about \$20 billion in improper payments paid to SSI recipients. Based on agency research, the majority of SSA’s improper payments occurred because of verification and local administration errors. Those errors include non-verification of earnings, income, assets, or work status; and inputting, classifying, or processing applications incorrectly.

RESOLVING THE ISSUE

Resolving the issue of improper payments for all government agencies revolves around three categories of action: boosting transparency, holding agencies accountable, and creating strong incentives for compliance.

In terms of boosting transparency, the order calls for several provisions, including:

- Creating an online dashboard of key indicators and statistics on improper payments.
- Creating and publicizing an online tool for the public to report suspected incidences of fraud, waste, or abuse.
- Requiring agencies to establish more frequent error reduction targets.
- Issuing recommendations on ways to measure program access for intended beneficiaries.

With regard to holding agencies accountable, the order’s provisions include:

- Requiring each agency to designate a current, Senate-confirmed appointee to be accountable to the president for meeting improper payment reduction targets.
- Requiring that all targets for improper payments show reduction and/or improvement and sharing the agency’s plans for meeting the reduction targets with the agency’s IG.
- Issuing recommendations on new

internal techniques agencies could use to better detect and mitigate improper payments.

Finally, in terms of creating incentives for compliance, the order requests that agencies:

- Consider administrative actions to provide state, local, and other organizations with incentives for reducing improper payments.
- Enhance contractor accountability by pursuing methods such as subjecting contractors to suspension and financial penalties for failing to disclose significant overpayments received on government contracts.



CIGIE/INSPECTOR GENERAL RESPONSIBILITIES

The effort to reduce improper payments across the broad spectrum of the federal government involves many different agencies with different operations. Therefore, collaboration and consultation are necessary and this is where CIGIE comes into play.

OMB established eight inter-agency workgroups to focus on the implementation of the order: Executive Order Guidance, Improving Measures of Access, Publishing Web sites, Improving Information Sharing, Single Audits, Incentives and Accountability, Enhancing Contractor Accountability, and Forensic Accounting and Auditing. These workgroups have made recommendations to OMB and the U.S. Treasury on actions agencies should take or controls for measuring programs and detecting improper payments; by identifying and measuring the problem, and determining the root causes of error, the government will be able to focus and prioritize its resources so that corrective actions can be developed and carried out. Throughout the process, CIGIE has consulted the workgroups on measurements, single audits, incentives, and accountability recommendations.

OMB tasked the U.S. Treasury with publishing an improper payments online dashboard and an online tool for reporting improper payments. CIGIE consulted with the U.S. Treasury during the process, making recommendations on improving information sharing with the public. The new Web site on improper payments—www.paymentaccuracy.gov—was launched in June to the public and contains high-level, historical information about improper payments, risk-susceptible programs, and actions agencies are taking to reduce wasteful spending. The

site also includes a link for the public to report fraud, waste, and abuse related to high-priority programs in agencies such as HHS, DOL, SSA, USDA, and DOT.

The order also requires that agencies operating high-priority programs provide an annual improper payment report and a quarterly high-dollar report (quarterly improper payments of more than \$5,000 to an individual or more than \$25,000 to an entity) to its OIG in May. The OIG's review of its agency's annual report is expected to be completed in September, while the review of the quarterly high-dollar report should be completed in December.

SSA RECOVERY EFFORTS

In SSA's case, the agency has a number of programs in place to protect the public's tax dollars and ensure a more efficient and effective government:

The agency is committing nearly \$760 million toward program integrity efforts for fiscal year 2010, an increase of more than \$250 million over the previous year's funding.

SSA conducts both medical and work-based continuing disability reviews to determine if a beneficiary remains eligible, as well as SSI redeterminations to re-evaluate any nonmedical factors that would affect eligibility or the benefit amount.

The agency is also participating in the Partnership Fund for Program Integrity Innovation initiative, which works to identify ways to improve service delivery, payment accuracy, and administrative efficiency of assistance programs with shared federal and state responsibilities.

Additionally, SSA has a debt collection program to recover all types of overpayments. SSA reports that it collected more than \$3 billion in Retirement, Survivors, and Disability Insur-

“We administer very complex programs for the public, paying nearly \$60 billion in benefits each month to our beneficiaries. While such complexities can lead to improper payments, each of us has a duty to protect taxpayer dollars by minimizing these improper payments.”

-Commissioner Astrue

ance and SSI benefit payments in fiscal year 2009. To recover overpayments, the agency uses internal debt collection techniques, such as payment withholding and follow-up billing, as well as external debt collections authorized by the *Debt Collection Improvement Act of 1996* and the *Foster Care Independence Act of 1999*.

Social Security Commissioner Michael J. Astrue is serving as the agency's accountable official. In a message to SSA employees in August, Commissioner Astrue said that agency employees must work diligently to strengthen the integrity of its programs to curb improper payments. “One of our most basic responsibilities is to ensure that we are paying eligible beneficiaries the right amount at the right time,” Commissioner Astrue said. “We administer very complex programs for the public, paying nearly \$60 billion in benefits each month to our beneficiaries. While such complexities can lead to improper pay-

ments, each of us has a duty to protect taxpayer dollars by minimizing these improper payments.”

IMPROPER PAYMENTS ELIMINATION AND RECOVERY ACT

When President Obama signed the *Improper Payments Elimination and Recovery Act* in July, he stated that the legislation would “help ensure that our government serves as a responsible steward for the tax dollars of the American people, and builds on the efforts we’re taking to cut wasteful spending.”

According to the White House, the IPERA will complement and help implement the administration's campaign against improper payments. Specifically, the legislation will improve agency efforts to reduce and recover improper payments in several ways, including:

- *Identification and Estimation of Improper Payments:* The IPERA requires agencies to conduct annual risk assessments, and if a program is found to be susceptible to significant improper payments, then agencies must measure improper payments in that program. Further, over time, the IPERA lowers the threshold for determining whether a program is susceptible to improper payments.
- *Payment Recapture Audits:* The IPERA expands the types of programs that are required to conduct payment recovery audits (from contracts to all types of programs and activities, including grants, benefits, loans, and contract payments), and lowers the threshold for programs and activities that must conduct these reviews if cost-effective (from \$500 million to \$1 million in annual outlays).

- *Use of Recovered Improper Payments:* The IPERA also authorizes agency heads to use recovered funds for additional uses to those currently allowed, including: to improve their financial management, to support the agency's OIG, and for the original intent of the funding.
- *Compliance and Non-Compliance Requirements:* Currently, if an agency does not reduce improper payments or implement the existing law, there are no repercussions. Under the IPERA, there is a list of actions that an agency must take to be in compliance with the law, and the agency IG is responsible for determining whether the agency is in compliance. If the agency is found not to be in compliance, then the IPERA contains a series of actions that the agency must take to improve its error reduction efforts.

For CIGIE, the new law includes a provision that requires the Federal Chief Financial Officer's Council to consult with CIGIE, as well as recovery audit experts, on a study of the implementation of the law's recovery audit provision. The study will include the costs and benefits of agency recovery audit activities, and will evaluate the effectiveness of using private contractors, agency employees, employees from other agencies, or some combination of these groups to do recovery auditing. The report will go to the Senate Committee on Homeland Security and Governmental Affairs, the House of Representatives Committee on Oversight and Government Reform, and the



Comptroller General—it must be completed within two years of enactment of the act (July 22, 2012).

For each OIG, there are several provisions in the new law that will have an effect on OIG operations. First, the new law allows up to five percent of the amounts collected from recovery auditing by an agency to be used by the IG of that agency. The money is to be used to carry out this new law or for any other activities of the IG relating to investigating improper payments or auditing internal controls associated with payments. This provision would apply only to recoveries of overpayments from discretionary appropriations made after enactment, or July 22, 2010. Also, agencies can retain up to 25 percent to be used to address improper payments.

The new law also requires each agency's IG to report each fiscal year on its agency's compliance with this act. The IG's report is to be provided to the head of the agency, the Senate Committee on Homeland Security and Governmental Affairs, the House of Representatives Committee on Oversight and Governmental Reform, and the Comptroller General.

If an agency is determined by the IG to be non-compliant for two consecutive years for the same program

or activity, then the agency may have to put more money and resources into addressing improper payments. Specifically, if there are two consecutive years of non-compliance with this new law and the director of OMB determines that additional funding would help the agency come into compliance, the head of the agency shall obligate additional funding in an amount determined by OMB, to increase compliance efforts.

An additional provision in the new law will affect OIGs down the road. Specifically, there is a requirement that OMB must develop criteria as to when an agency should be required to obtain an opinion on internal controls over improper payments. OMB is to develop this criteria within a year of enactment of the law—July 22, 2011.

CONCLUSION

The president has outlined an aggressive plan of action to reduce wasteful spending throughout the federal government, announcing a public goal of cutting improper payments by \$50 billion in the next two years. Thus far, agencies have complied with requests to report their improper payments and identify the causes of those monetary errors. This important collaboration among federal agencies, OMB, the U.S. Treasury, and the CIGIE will continue in an effort to reduce improper payments and improve administrative efficiency and service delivery.

For more information on improper payments, visit www.paymentsaccuracy.gov. For more information on SSA's efforts to reduce improper payments, visit www.ssa.gov/improperpayments. ❧



Patrick P. O'Carroll, Jr.

Patrick P. O'Carroll, Jr. currently serves as the inspector general for the Social Security Administration, having been appointed to that position on November 24, 2004.

Prior to his appointment as Inspector General, Mr. O'Carroll held a number of increasingly responsible positions in the SSA OIG organization, including assistant inspector general for investigations and assistant inspector general for external affairs. Mr. O'Carroll also brought to the OIG the benefits of his 26 years of experience with the U.S. Secret Service.

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



ISSUES REGARDING THE FEDERAL CONFLICT-OF-INTEREST STATUTE

BY MARK GREENBLATT

In general terms, federal law prohibits federal employees from participating in official government matters when those matters would impact their financial interest.¹

While this prohibition may seem clear on its face, the application of the statute, 18 U.S.C. § 208, can raise thorny issues. This article examines the legal landscape surrounding two critical elements of the § 208 analysis—whether an employee’s actions amount to “participation,” and whether the government activity at issue constitutes a “particular matter” within the scope of the prohibition.

BACKGROUND

Before Section 208 was enacted, Section 434 was the governing conflict-of-interest prohibition. That provision, which had been in place for more than 100 years, was quite narrow. Section 434 penalized only government officials that engaged in the “transaction of business” with an entity in which they had a financial interest. The “transaction of business” language was largely interpreted to include only the actual execution of a government contract.

1) 18 U.S.C. 208(a) provides: “Except as permitted by subsection (b) hereof, whoever, being an officer or employee of the executive branch of the United States government, or of any independent agency of the United States, a Federal Reserve bank director, officer, or employee, or an officer or employee of the District of Columbia, including a special government employee, participates personally and substantially as a government officer or employee, through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise, in a judicial or other proceeding, application, request for a ruling or other determination, contract, claim, controversy, charge, accusation, arrest, or other particular matter in which, to his knowledge, he, his spouse, minor child, general partner, organization in which he is serving as officer, director, trustee, general partner or employee, or any person or organization with whom he is negotiating or has any arrangement concerning prospective employment, has a financial interest...[s]hall be subject to the penalties set forth in Section 216 of this title.”



In the early 1960s, Congress, in the words of the Fifth Circuit, recognized that Section 434 was “fundamentally defective in that it allowed public officials to engage in a large number of activities which are wholly incompatible with the duties of public office.”² Congress therefore enacted Section 208 in 1962, broadening the scope of conflict-of-interest prohibitions far beyond that of Section 434.

In drafting language for the new conflict-of-interest prohibition, Congress relied largely on a proposal formulated by the New York City Bar Association. The New York City Bar Association convened a special committee that examined the deficiencies of the then-governing conflict-of-interest laws for two years, prepared an extensive analysis of the legal landscape, and drafted model federal conflicts-of-interest legislation. That proposal, which recommended

2) *United States v. Nevers*, 7 F.3d 59 (5th Cir. 1993).

sweeping changes, was the foundation for the 1962 statute. Harvard professor Roswell B. Perkins led the NYC Bar Association Committee and following the enactment of the 1962 conflict-of-interest provisions, published a lengthy analysis on the new prohibitions in the *Harvard Law Review*. Perkins’s article provided important commentary on the relevant statutory language and numerous courts, including three federal circuits have relied on his seminal article to interpret Section 208. Professor Perkins’s analysis is incorporated in this article to provide his insight on the meaning of the two elements of Section 208 examined here.

WHETHER AN EMPLOYEE’S ACTIONS AMOUNT TO “PARTICIPATION”

The first significant element of the Section 208 analysis is that the government

official must “participate” in a government matter, both “personally” and “substantially.” These terms have been interpreted quite broadly, encompassing almost every type of action an official can take. As discussed below, only a small subset of official conduct is excluded from the scope of personal and substantial participation.

“Personal” participation, according to the interpretive federal regulations, means “to participate directly.”³ The regulations also state that personal participation “includes the direct and active supervision of the participation of a subordinate in the matter.”⁴ The Office of Government Ethics appears to have adopted an even broader scope of personal participation, construing the term to include not just an official’s direct participation or supervision of the matter, but also actions that are arguably one step removed, such as the official’s decision on which employees will work on the matter.⁵ Because the scope of personal participation is so broad, the question of whether an official’s participation was sufficiently “personal” does not appear to have engendered significant case-law.

In contrast, there has been more extensive development of the “substantial” participation element. Consistent with congressional intent to broaden the scope of the conflict-of-interest prohibition, the statute includes an expansive list of prohibited participation, providing that employees may not participate in certain matters through “decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise.”⁶ This language came virtually verbatim from the NYC Bar Association proposal, and professor Perkins observed

that this language was “more illustrative than substantive” and that it was “designed to give practical significance to the more abstract but sweeping concept of participation.”⁷

The interpretative regulations add further texture to the statutory language, defining the term “substantial” to mean that the employee’s involvement is “of significance to the matter.”⁸ The regulations state that:

Participation may be substantial even though it is not determinative of the outcome of a particular matter. . . . A finding of substantiality should be based not only on the effort devoted to a matter, but also on the importance of the effort. While a series of peripheral involvements may be insubstantial, the single act of approving or participating in a critical step may be substantial. Personal and substantial participation may occur when, for example, an employee participates through decision, approval, disapproval, recommendation, investigation, or the rendering of advice in a particular matter.⁹

Taken together, the language in the statute and regulations cast a wide net. Several cases have involved employee conduct that falls squarely within the concept of substantial participation, such as an employee’s activities in “various aspects of the letting, administration, and performance” of the contracts at issue;¹⁰ an employee’s approval of a budget that contained a payment to the contractor at issue;¹¹ and an official’s involvement in her agency’s internal deliberations about a possible procurement activity.¹² Similarly, the OGE issued an advisory letter in which it concluded that an employee’s

responsibilities, which included providing reviews of acquisition proposals that would largely determine whether procurement requests would be approved, would constitute participation within the scope of § 208.¹³

When an employee’s actions do not fall squarely in the governing language, courts and other legal authorities have construed substantial participation broadly. The Seventh Circuit adopted such an expansive construction of substantial participation in United States v. Irons.¹⁴ In that case, the defendant argued that Section 208 covered only “pre-contractual activities” and that the acts of “causing delivery to be made of the [purchased] equipment” and “receiving payment of monies for such equipment” were not substantial participation under the statute. In making that argument, Irons asserted that the phrase “or otherwise” in the list of prohibited actions should be interpreted narrowly, pursuant to the rule of ejusdem generis.¹⁵

The court rejected that narrow reading because it concluded that the statute’s legislative history “demonstrates an intention to proscribe rather broadly employee participation in business transactions involving conflicts of interest and to reach activities at various stages of these transactions.”¹⁶ With that intent in mind, the Irons court elected to “construe the statutory phrase ‘or otherwise’ in a realistic and relatively inclusive fashion.”¹⁷

More specifically, the court concluded that Section 208 covered an employee’s participation in pre-contractual or preliminary activities such as recommendations or investigations, as well as

3) 5 C.F.R. § 2635.402(b)(4).

4) Id.

5) See OGE Informal Advisory Memorandum 04 X 5, 2004 WL 3323967 (stating “Participating in a decision concerning who should work on a matter, how a matter should be handled, or whether a matter should be acted upon, is a form of participation in the matter”).

6) 18 U.S.C. § 208(a).

7) 76 Harv. L. Rev. at 1128.

8) 5 C.F.R. § 2635.402(b)(4).

9) Id.

10) See K&R Engineering Co. vs. United States, 616 F.2d 469 (Ct. Cl. 1980).

11) See United States v. Bouchev, 860 F.Supp. 890 (D.D.C. 1994).

12) See United States v. Selby, 557 F.3d 968 (9th Cir. 2009).

13) OGE Informal Advisory Letter to DAE0, 92 x 12 1992 WL 518818 (O.G.E.).

14) 640 F.2d 872 (7th Cir. 1981).

15) The Irons court described ejusdem generis as a principle of statutory construction in which “the scope of a general term in a statute is limited by the nature of the preceding class or thing (in this case matters generally preliminary to the formation of a contract) unless a contrary intent is clearly shown.” Id. at 875-876.

16) Id. at 876.

17) Id.

acts associated with the execution of a contract.¹⁸

While the scope of substantial participation is expansive, it is not limitless. Professor Perkins noted that this provision was not intended to prohibit an employee's involvement in "purely ministerial or procedural acts."¹⁹ Accordingly, the regulations interpreting the meaning of substantiality expressly exclude such minor activities: "[A finding of substantial participation] requires more than official responsibility, knowledge, perfunctory involvement, or involvement on an administrative or peripheral issue."²⁰ The regulations provide an example in which an employee's participation in a matter too tangential to qualify as "substantial":

An agency's Office of Enforcement is investigating the allegedly fraudulent marketing practices of a major corporation. One of the agency's personnel specialists is asked to provide information to the Office of Enforcement about the agency's personnel ceiling so that the office can determine whether new employees can be hired to work on the investigation. The employee personnel specialist owns \$20,000 worth of stock in the corporation that is the target of the investigation. She does not have a disqualifying financial interest in the matter (the investigation and possible subsequent enforcement proceedings) because her involvement is on a peripheral personnel issue and her participation cannot be considered "substantial" as defined in the statute.

United States v. Ponnappula, a Sixth Circuit case, provides a good illustration of how purely administrative or perfunctory actions are not considered substan-

tial participation for § 208 purposes.²¹ In that case, the government retained an attorney to act as a trustee in a foreclosure sale. The attorney's participation in the matter was limited to publishing legal notices of the sale and performing administrative tasks at the closing, such as filling out the government-supplied, standard memorandum of sale. The sale later resulted in civil litigation in which the purchaser sought to void the contract, in part because the government attorney allegedly suffered from a conflict of interest. The Sixth Circuit affirmed the district court's ruling that the government attorney's participation in the sale was not substantial within the scope of Section 208. The court's conclusion hinged on the fact that the attorney's duties were administrative in nature and that she "had no input regarding the terms of the sale nor the content of the pre-printed terms of the memorandum."²² Citing professor Perkins's article, the Ponnappula court found that "[a] statute aimed at preserving the integrity of the decision-making process does not need to extend to employees who have no discretion to affect that process."²³

Another noteworthy issue related to the "participation" element is the focal point of this analysis. As described in professor Perkins' analysis, the predecessor to Section 208 focused on "the nature of the action taken by the government official in relation to the private party involved."²⁴ Section 208, in contrast, "shifts the focus to the role the government official plays in bringing about the action taken by the government."²⁵ The House of Representatives report discussing the prohibition touched on this issue, stating: "Section 208(a)...would bar any significant participation in gov-

ernment action in the consequences of which to his knowledge the employee has a financial interest."²⁶

While cases involving Section 208 generally appear to focus on the employee's participation in the government action, one case appears to examine the employee's participation with the private party. In that case, United States v. Alfonzo-Reyes, the government charged that Alfonzo, the defendant government official, had participated in a third party's application for a \$500,000 loan from his agency.²⁷ Alfonzo moved for dismissal on the basis that he had not participated in the government's processing of the third party's loan request.

The court rejected the motion. Importantly, the Alfonzo-Reyes court did not rely on evidence that the official had participated in the government's loan approval process; in contrast, the court found that Alfonzo had participated by: (i) assisting the third party in the application process; (ii) advising the third party that, while waiting for the government loan to be disbursed, he should take a letter of approval from the agency and obtain a \$150,000 loan from a private bank; and (iii) advising the third party to obtain a larger loan amount from the bank and writing a letter to the bank stating that the government had approved the \$500,000 loan to the third party. As noted above, however, Alfonzo-Reyes seems to be unique in this regard, in that most cases appear to focus the Section 208 analysis on the employee's participation in the government's actions.

18) Id. at 876-879.

19) 76 Harv. L. Rev. 1113, 1128. Perkins also cautioned, however, that such exclusions do not "create a loophole for the lazy executive in the chain of command who may have not bothered to dig into the substance of the case."

20) 5 C.F.R. § 2635.402(b)(4).

21) See 246 F.3d 576 (6th Cir. 2001).

22) Id. at 583.

23) Id.

24) 76 Harv. L. Rev. at 1130.

25) Id.

26) See H.R.Rep.No. 748, 87th Cong., 1st Sess. 24 (1961) (quoted in Irons, 640 F.2d at 878) (emphasis added).

27) See 384 F.Supp.2d 523 (D. Puerto Rico 2005).

WHETHER THE GOVERNMENT ACTIVITY AT ISSUE CONSTITUTES A “PARTICULAR MATTER”

One of the most critical questions in the Section 208 analysis is whether the government action in which the employee is participating is a “particular matter.” The statute provides a detailed list of covered actions—namely, “a judicial or other proceeding, application, request for a ruling or other determination, contract, claim, controversy, charge, accusation, arrest”—as well as an expansive catch-all: “or other particular matter.” Professor Perkins believed that the importance of this language (and the equivalent provisions in sister conflicts provisions) is that “it is all-encompassing in so far as the scope of government proceedings is concerned.”²⁸ Perkins also noted that the current provision expanded the narrow scope of its predecessor, which focused solely on a relatively limited class of “claims.”

While the concept of a “particular matter” is expansive, legal authorities have not interpreted the phrase to be quite as “all-encompassing” as Perkins asserted. OGE has emphasized that the term “is not so broad as to include every matter involving government action.”²⁹ In particular, the governing regulations expressly exclude “the consideration or adoption of broad policy options that are directed to the interests of a large and diverse group of persons.”³⁰ Examples of proceedings that are too generalized to constitute a particular matter include the IRS’s amendment of its regulations to change the manner in which depreciation is calculated,³¹ the Social Security Administration’s consideration of changes to its appeal procedures for disability

claimants,³² health and safety regulations applicable to all employers,³³ the allocation of additional resources to the investigation and prosecution of white-collar crime by the Justice Department,³⁴ comprehensive legislative proposal for health care reform,³⁵ deliberations on the general merits of an omnibus bill, and a report of a panel on tax reform addressing a broad range of tax policy issues.³⁶

There is a point of inflection, however, at which the government’s action or proceeding is directed to a sufficiently “discrete and identifiable” class of persons that the action constitutes a particular matter within the scope of Section 208.³⁷ The regulations provide two examples that illustrate this inflection point. Example 9 states:

The formulation and implementation of the response of the United States to the military invasion of a U.S. ally is not a particular matter. General deliberations, decisions and actions concerning a response are based on a consideration of the political, military, diplomatic and economic interests of every sector of society and are too diffuse to be focused on the interests of specific individuals or entities. However, at the time consideration is given to actions focused on specific individuals or entities, or a discrete and identifiable class of individuals or entities, the matters under consideration would be particular matters. These would include, for example, discussions whether to close a particular oil pumping station or pipeline in the area where hostilities are taking place, or a decision to seize a particular oil field or oil tanker.

Similarly, example 10 states:

A legislative proposal for broad health care reform is not a particular matter because it is not focused on the interests of specific persons, or a discrete and identifiable class of persons. It is intended to affect every person in the United States. However, consideration and implementation, through regulations, of a Section of the health care bill limiting the amount that can be charged for prescription drugs is sufficiently focused on the interests of pharmaceutical companies that it would be a particular matter.

The DC Circuit summarized the “limiting principle” of the particular matter analysis, stating that the term applies “only to matters in which the governmental decision at stake is focused on conferring a benefit, imposing a sanction, or otherwise having a discernable effect on the financial or similarly concrete interest of discrete and identifiable persons or entities.”³⁸ Examples of government actions or proceedings that fall squarely within the scope of a particular matter include a regulation applicable only to meat packing companies,³⁹ a regulation prescribing safety standards for trucks on interstate highways,⁴⁰ recommendations concerning specific limits on commercial use of a particular facility,⁴¹ determinations or legislation focused on the compensation and work conditions of the class of Assistant United States Attorneys,⁴² and the decision to pursue an administrative enforcement action against a specific company or group of companies.⁴³

32) See id.

33) See id. (Example 4).

34) See id. (Example 5).

35) See id. (Example 8).

36) See OGE Informal Advisory Memorandum 06 X 9, at 8, (citing OGE Informal Advisory Letter 05 X 1).

37) OGE has described this inflection point, stating: “Usually, a particular matter arises when the deliberations turn to specific actions that focus on a certain person or a discrete and identifiable class of persons.”

38) Van Ee v. EPA, 202 F.3d 296 (D.C. Cir. 2000). Although Van Ee involved 18 U.S.C. § 205, the federal provision prohibiting a federal employee from acting as an agent or attorney before the government in connection with any covered matter in which the United States is a party or has an interest, the court noted that the term had been “similarly construed” in § 208. See id.

39) See 5 C.F.R. § 2640.103(a)(1)(Example 3).

40) See 5 C.F.R. § 2635.402(b)(3)(Example 2).

41) See OGE Informal Advisory Letter 00 x 4.

42) See 18 Op. O.L.C. 212, 219-220 (1994).

43) See id. at 217-218 (quoting Memorandum for C. Boyden Gray, Counsel to the President, from J. Michael Luttig, Acting Assistant At-

28) 76 Harv. L. Rev. at 1127.

29) OGE Informal Advisory Memorandum 06 X 9, at 4, 2006 WL 5380985 (O.G.E.).

30) 5 C.F.R. § 2635.402(b)(3).

31) 5 C.F.R. § 2640.103(a)(1)(Example 1).

“A legislative proposal for broad health care reform is not a particular matter because it is not focused on the interests of specific persons, or a discrete and identifiable class of persons. It is intended to affect every person in the United States.”

Three noteworthy opinions provide further texture on the particular matter analysis. First, for circumstances in which the government’s action does not fit neatly into the statute’s list of covered actions, the Justice Department Office of Legal Counsel articulated a test to determine whether the action in question constitutes a particular matter within the purview of § 208. Employing the principle of *eiusdem generis*, the OLC concluded that “whether or not the object of deliberation, decision, or action constitutes a ‘particular matter’ will depend upon how closely analogous the object of deliberation, decision, or action is to the object of a typical ‘judicial proceeding,’ ‘claim,’ ‘application,’ or other matter enumerated in Section 208.”⁴⁴

Second, the Ninth Circuit ruled in *United States v. Jewell* that, if an employee takes several impermissible actions related to a single transaction, those

separate actions constitute one violation of Section 208, not a separate violation for each individual act.⁴⁵ In *Jewell*, the indictment alleged that each routine invoice the defendant signed under a single contract constituted a different particular matter. The Ninth Circuit ruled that each particular matter must be a discrete transaction, not acts that are part of a larger transaction, and that they cannot be continuous or overlapping with another matter.

The third notable case is *United States v. Lund*, in which the Fourth Circuit concluded that Section 208 was not limited to matters involving non-governmental third parties.⁴⁶

Lund was indicted on three counts of violating § 208 for his alleged participation in three intra-agency personnel matters in which his wife had a financial interest. Before trial, *Lund* moved to dismiss the indictment, arguing that the statute did not apply to intra-agency personnel matters. The district court granted the defense motion because it considered the provision ambiguous and found evidence that Congress intended § 208 to apply only to conflicts involving “outside suppliers of goods and services to the government.” The Fourth Circuit reversed, ruling that the terms “contract” and “application” should be interpreted according to their plain meaning: “nothing on the face of the statute suggests a congressional intent to limit those terms to less than their normal reach.” Noting that Section 208 expanded the scope of the activities covered by federal conflict-of-interest laws to include a wide range of government activities, the *Lund* court concluded that Section 208 was not limited to matters involving non-governmental third-parties and that it also covered intra-agency personnel matters. ☞

45) See 827 F.2d 586 (9th Cir. 1987).

46) See 853 F.2d 242 (4th Cir. 1988).



Mark L. Greenblatt

Mark L. Greenblatt is an investigative counsel in the Oversight & Review Division of the U.S. Justice Department Inspector General’s Office. Mr. Greenblatt has led criminal and administrative investigations into allegations of misconduct by senior-level Justice Department officials.

Prior to joining the Justice Department OIG, Mr. Greenblatt served as the chief counsel and staff director to the minority of the U.S. Senate Permanent Subcommittee on Investigations, which is the investigative arm of the U.S. Senate. During his PSI tenure, Mr. Greenblatt led numerous bipartisan investigations, focusing on government waste, homeland security, and consumer protection matters.

Before joining PSI, Mr. Greenblatt was a litigation associate at two large international law firms and a law clerk for a Federal District Judge.

He received his undergraduate degree from Duke University and a J.D. from Columbia University School of Law.

torney General, Office of Legal Counsel, Re: Applicability of 18 U.S.C. § 208 to General Policy Deliberations, Decisions and Actions (Aug. 8, 1990) (the “Gray Memorandum”).

44) *Id.* at 220 (quoting Gray Memorandum). It is noteworthy that the application of *eiusdem generis* in this way appears to conflict with professor Perkins’s understanding of congressional intent regarding the particular matter phrasing. In his article, Perkins asserted that, by spelling out the wide array of individual covered matters, “the same effect has been achieved” as using a single comprehensive term. See 76 Harv. L. Rev. at 1127. Therefore, Perkins might argue that Congress did not intend to limit the scope of the statute to those government actions that are closely analogous to the listed matters.

CHILD PORNOGRAPHY OFFENSES BY GOVERNMENT EMPLOYEES

**BY CHAD STEEL AND
LAUREN HENRY**

A growing problem facing the inspector general community is the proliferation of child pornography found on U.S. government systems and traversing government networks. The FBI's Innocent Images initiative handles over 2,500 cases annually and has seen an exponential growth in child pornography coincident with the growth in popularity of the Internet.¹ As a cross-section of society as a whole, a commensurate percentage of growth in abuse by U.S. government employees is a reasonable conclusion. The possession or viewing of images depicting minors engaged in sexual activity is a violation of 18 U.S.C. § 2252(A) and potentially 18 U.S.C. § 1466(A). The IG community face a number of challenges in preventing, detecting, and responding to this problem.

CHILD PORNOGRAPHY ON GOVERNMENT SYSTEMS

For most employees, misusing a government computer or network to obtain, distribute, or produce child pornography is inconceivable. At most government agencies, the acceptable (and unacceptable) use of the Internet for official duties has become a subject of regular employee training. Employees are given clear instructions as to what is and what is not acceptable usage of government computers. The majority of government information systems clearly display a warning banner advising the user to avoid improper or unauthorized use, and

1) Federal Bureau of Investigation. Innocent Images National Initiative. [Online] [Cited: September 2, 2010.] <http://www.fbi.gov/publications/innocent.htm>.



inform the user that their activities may be monitored.

Since searching for child pornography is clearly unlawful and a gross violation of acceptable use, we must explore what leads employees to disregard policy, ignore their training, and pay no heed to warning banners and engage in this behavior. Due to this incongruity, there is a general sense of disbelief when child pornography is found on a government system, and those outside of the OIG are typically unaware of the extent to which it occurs. As a result of our investigations and through our experience with child pornographers, we have identified several reasons for this type of behavior and activity.

One common starting point for some employees is simple curiosity—they want to test the limits of what they are able to access. In their minds, they

are not doing anything wrong because they are not necessarily looking to actually view the porn, but looking to see if they can gain access to it or not. The access may start with “traditional” adult pornography and move into the area of child pornography over time.

Another contributing factor is the perceived anonymity in large groups. Many individuals believe that their agency is large and bureaucratic, and unable to effectively monitor all activities on all the systems. Successful forays into unauthorized use in which they do not get caught reinforces this message. If they are able to view inappropriate material on one occasion without any repercussions, they will become more brazen and continue to view/download more with less fear of being caught.

For some individuals, there is an added excitement that comes from

viewing the images at work where there is a possibility of getting caught. These individuals may claim to be getting their arousal from the taboo nature of the act, rather than from the images themselves. Additionally, a number of individuals viewing child pornography are acknowledged pedophiles, and as such, they do not believe that viewing child pornographic images is even wrong. These individuals will rationalize to themselves that what they are doing is perfectly normal and acceptable; hence, they do not exhibit concern or fear for the consequences of viewing these images at work.

Whatever reason that gets them started in viewing these images, for many, it becomes an addiction. Although these individuals know that they might be terminated from employment or arrested, the need to view the images and the level of arousal attained by doing such outweighs any and all possible consequences.

Finally, we also found that some individuals who have access to pornographic images of children in the course of their official duties will sometimes continue to view them outside of their professional responsibilities. Close monitoring by investigative teams, including agents, forensic examiners, and managers should be performed and contraband materials should be tightly controlled and audited.

It is important to understand the different reasons as to why individuals engage in this type of behavior in order to prepare and conduct effective and successful interviews. Whether their motives are genuine or just simple rationalizations, they provide effective material to use as themes in the subject interview. Having a subject admit they were “just curious” or were “testing the system” as an initial step requires significantly less cognitive dissonance than an admission that they are a pedophile, and can lead to

additional disclosures. Further, a better understanding of possible motivations enhances the effectiveness of investigations, as well as assists in identifying methods of prevention and earlier detection.

THE INVESTIGATIVE TEAM

Conducting investigations involving child pornography is difficult, even for seasoned and experienced investigators due to disturbing images viewed during the course of the investigation. It is critical for those involved to identify their capabilities and vulnerabilities for reviewing these types of images. In order to staff a team of investigators for this work, a number of interests should be considered.

First, although the number of investigators available for a case often dictates assignment, working on these cases should be voluntary. Those who decide to be a part of the team should be aware of what is involved, specifically the viewing of disturbing images. Furthermore, it is valuable for investigators to submit to an assessment prior to participating in these investigations. Some agencies now have established screening and/or assessment processes for those involved. The assessments range from formal psychological instruments and tests to informal discussions; regardless of the type of assessment, any assessment is beneficial.

Second, it is advantageous when investigators on the team have a background and familiarity with crimes involving illegal or coerced sexual activity. Training is available from Internet Crimes Against Children Task Force, from the National Child Advocacy Center, and from other training such as the Internet Investigations Training Program at FLETC. These skills will also complement any risk assessments for supple-

mentary contact offenses.²

Once on a team, resources and guidance should be readily available as individuals can be impacted personally or professionally by the viewing of these images. Likewise, team members should be aware of each other's status as well as their own and be able to recognize if they are no longer capable of continuing on the team.

Although investigators deal with all types of heinous crimes throughout their careers, child pornography investigations have issues of secondary victimization not present in other crimes. Therefore, agencies should employ prudence and attention when staffing for these investigations.

PREVENTION

Preventing child pornography from entering government systems starts at the policy level. At a minimum, policy on what is an appropriate and what is an inappropriate use of government computers should be in effect. The policy should be easy to understand and readily accessible to all employees. Ideally, employees should also have annual training and sign an appropriate agreement. Additionally, employees should be notified that their activities will be monitored and violations investigated.

Non-IT policy decisions have an impact on child pornography proliferation internally as well. Having an environment where computers are visible to others, being mindful of “off-hours” work, and effective background screening can significantly reduce the likelihood of child pornography offenses occurring. Finally, the internal publication of successful prosecutions by IG investigators in cases involving child pornography is effective as a reminder of the con-

2) The 'Butner Study' Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders. Bourke, Michael and Hernandez, Andres. 2008, Journal of Family Violence, Vol. 24, No. 3, pp. 181-191.

sequences of violations.

Blocking of inappropriate materials can occur through filtering on the organization's Internet connections. A proxy server which logs Web requests and blocks sites based on a "black list" can be effective as a deterrent to "casual" access of inappropriate materials, and can prevent accidental stumbling across inappropriate Web sites. Blocking ports which are not used can likewise limit the use of programs such as peer-to-peer software which avoid the proxy servers, and has an additional benefit of reducing the attack surface for malware.

DETECTION

Detection of child pornography within a government agency can take place two ways – with data in transit and with data at rest. Data in transit-based methods identify individuals as they attempt to obtain or view child pornography over the agency network. Data at rest-based approaches look for child pornography indicators present on digital resources stored within the agency.

Detecting child pornography at the perimeter can be effective for activity conducted while individuals are connected to the organization's network. There are three primary mechanisms for detecting child pornography that traverse the company network—traffic analysis, block list violations, and keyword analysis.

Traffic analysis attempts to identify unusual network traffic patterns. Individual machines using bandwidth inconsistent with the office's work schedule (e.g. late at night, weekends), connecting on unusual TCP ports, or consuming high amounts of bandwidth are likely targets. Though there will be many false positives, the analysis will help with general IT capacity planning and will identify other activity of interest to the IG

community such as copyright violations (large movie downloads) and adult pornography.

Block list violation analysis assumes the presence of some degree of filtering based on URLs or specific Internet ports. While these filters are never comprehensive, by monitoring the logfiles for large numbers of "denied" connections, you can identify likely targets trying to get around the security system.

Keyword analysis identifies words in traffic that match keywords used by those seeking child pornography. Depending on the network, all traffic can be searched or searches can be limited to just logged data like URL query strings (which can show the terms used on a search engine). When using keyword lists, it is more effective to use words and phrases exclusively associated with child pornography. Words such as "teen" will appear frequently as part of news stories whereas words such as "R@ygold" are exclusively associated with child pornography. A list of keywords and phrases can be provided by the authors upon request.

With the move toward portability and work-at-home flexible work agreements, government computers are being exposed to environments outside the fence line. As such, traditional perimeter controls like proxy servers and firewalls present on the agency's Internet connections have become less effective. Additionally, the proliferation of USB-based media has increased the risk for loading data from non-networked sources. Because of this, scanning of local disks for child pornography centric activity is a needed defensive layer.

For local drives, software packages such as EnCase Enterprise provide a capability to analyze the file systems for child pornography through the use of local agents. Less expensive is the use of open source tools such as hashdeep and md5deep, developed by Jesse Korn-

blum while working as a special agent for the Air Force Office of Special Investigations, to examine hard drives for the presence of previously identified child pornography using known-bad hash values. Agencies should consider performing a file system audit to detect both child pornography and other known-bad content (such as hacking tools) as part of the IT support function when a laptop is turned in for maintenance, or scheduling scans on desktops and servers for low-traffic periods.

RESPONSE

IG special agents have access to resources to assist in child pornography investigations of employees that are not readily available in external investigations. First, if routine monitoring is done and employees are warned using a combination of click-through banners and training, the reasonable expectation of privacy can be fairly readily mitigated on government-owned machines. This potentially allows workplace searches and digital examinations of equipment without the need for a search warrant.

Second, IGs generally have access to a wealth of information on offenders in two categories – activity-based information and employee-provided information. This information can be used as the basis for subpoenas and as additions to affidavits for email and physical search warrants. Activity-based information is information on usage (primarily Internet usage) collected from e-mail systems, proxy servers, and other internal resources. E-mail accounts, social networking profiles, auction activity, and confederate information can all be gleaned from electronic records. Additionally, the wealth of information provided by employees as part of the normal course of business can be effective in tracking user activity. Personnel

“...IGs generally have access to a wealth of information on offenders in two categories – activity-based information and employee-provided information. This information can be used as the basis for subpoenas and as additions to affidavits for e-mail and physical search warrants.”

files, financial disclosure forms and direct deposit forms can contain location and account information ranging from home e-mail addresses to bank account numbers. Additionally, information on outside employment, properties owned, and family makeup can be used in risk assessment planning.

The National ICAC Task Force maintains a very useful database of child pornography trafficking over peer-to-peer networks,³ and FBI’s Innocent Images program collects identifiers that

3) 42 U.S.C. Chapter 154, § 17601-17612.

come up during other investigations nationwide. These sources can be utilized to vet identifiers ranging from IP addresses to e-mail addresses to Facebook identities that may have arisen in other investigations. Additionally, the National Center for Missing and Exploited Children maintains a database of known victims of child exploitation which can be used to identify the individuals present in suspect images.⁴

CONCLUSION

While child pornography crimes on U.S. government networks are not the most frequent investigations encountered in the inspector general community, they do occur. Their particularly heinous nature and the associated abuse of trust makes it well worth the time and effort for the inspector general community to ensure that they are aggressively investigated and prosecuted. Inspectors general who take a proactive approach in preventing and detecting child pornography and have a well-trained and planned out response mechanism will be in a better position to minimize the impact of this serious problem on their respective institutions. ❧

4) National Center for Missing and Exploited Children. Child Victim Identification Program, Office of Justice Programs, U.S. Department of Justice. 2010.

Lauren Henry received a bachelor’s degree in Administration of Justice from Rutgers University in 1997 and a master’s degree in Forensic Psychology from Argosy University in 2009. Ms. Henry has a strong background in law enforcement and criminal investigations. She started as an inspector with the U.S. Immigration and Naturalization Service shortly after graduation. After two years with INS, Ms. Henry accepted a position as a special agent for the U.S. Department of State, Diplomatic Security Service. Ms. Henry worked for DSS for approximately two years before joining the U.S. Air Force Office of Special Investigations. Her career with OSI began at Osan Air Base, Republic of Korea, and continued with a position at the Criminal Investigation Task Force at Ft. Belvoir. Additionally, Ms. Henry was a polygraph examiner for OSI responsible for counterintelligence scope and criminal issue examinations. She currently works as a special agent for the Central Intelligence Agency OIG.

Chad Steel holds a Bachelor of Science and Master of Science in Computer Engineering from Villanova University. He is currently performing research on the automated identification of child pornography in pursuit of a doctorate in computer forensics at Virginia Polytechnic Institute and State University. Mr. Steel formerly served as the head of IT investigations for a Global 20 company, worked as the chief security officer for a government contractor, and has performed forensic examinations for both government and private clients. Mr. Steel wrote a popular book on Windows Forensics, and taught Digital Forensics at Penn State’s graduate program and the Federal Law Enforcement Training Center.



HUD WATCHDOG SNIFFING OUT MORTGAGE LOAN FRAUDSTERS

BY KIMBERLY RANDALL

Mortgage fraud hurts all of us. It ruins lives, destroys neighborhoods, and costs taxpayers billions. One inspector general watchdog is on the hunt and looking to make bad players in the mortgage business pay – literally.

Lenders originated \$14 billion in fraudulent loans in 2009, according to industry experts.¹ While the focus in recent years has been on the subprime² mortgage implosion, the federal sector was not spared. The Federal Housing Administration, commonly known as “FHA,” felt the sting as well.

FHA provides mortgage insurance to lenders that will essentially make the lender whole when a borrower defaults on the mortgage. FHA’s estimated share of the \$14 billion national mortgage fraud estimate was more than half of the nationwide estimate - a staggering \$7.5 billion.³ The U.S. Department of Housing and Urban Development Office of Inspector General is the agency tasked with rooting out waste, fraud, and abuse in HUD programs like FHA, and has recently taken bold steps, like “zero tolerance,” to focus on fraudsters from a civil fraud standpoint, making them pay.



HOW DOES CRIMINAL FRAUD DIFFER FROM CIVIL FRAUD?

Many of the elements of criminal fraud are similar to those for civil fraud, but there are notable differences – the most notable being the burden of proof. Criminal prosecution requires proving the defendant committed the fraud beyond a reasonable doubt. Civil action remedies require proving only the preponderance of the evidence. The issue of intent is different between a civil and criminal case, and it is much easier to prove in a civil case than in a criminal case.

Another distinction is that criminal cases typically result in jail time for and restitution from the guilty party, while civil cases seek monetary compensation from the defendant of double or triple damages incurred by the

federal government, plus penalties. In essentially all criminal mortgage fraud cases, the potential for civil fraud exists and the two are not mutually exclusive. Cases can be processed in parallel under both the criminal and civil statutes. HUD OIG is making a concerted effort to pursue civil cases against fraudsters through its newly established Civil Fraud Division.

WHAT IS MORTGAGE FRAUD?

The Federal Bureau of Investigation defines mortgage fraud as a material misstatement, misrepresentation, or omission that an underwriter or lender relies on to fund, purchase, or insure a loan.⁴ Mortgage loan fraud is divided into two categories: fraud for property and fraud for profit. Fraud for property

1) Federal Bureau of Investigation, 2009 Mortgage Fraud Report – Year in Review: http://www.fbi.gov/publications/fraud/mortgage_fraud09.htm.

2) Subprime mortgages are home loans granted to individuals with poor credit histories who, as a result of their poor credit ratings (usually below 600), would not qualify for conventional mortgages. Lenders view subprime borrowers as having a higher-than-average risk of defaulting on the loan, which typically results in unfavorable loan conditions such as high interest rates.

3) Ibid.

4) Ibid.

entails misrepresentations by the applicant for the purpose of purchasing a property for a primary residence. This scheme usually involves a single loan and usually involves a borrower engaging in the fraud. Although applicants may embellish income and conceal debt, their intent is usually to repay the loan. Fraud for profit, however, often involves multiple loans and elaborate schemes perpetrated to gain illicit proceeds from property sales.⁵ Fraud for profit may be perpetrated by lenders, realtors, loan officers, and underwriters without any knowledge on the part of the borrower. Gross misrepresentations concerning appraisals and loan documents are common in fraud-for-profit schemes, and participants are frequently paid for their participation.⁶

HOW BIG A PLAYER IS FHA IN THE MORTGAGE INDUSTRY?

FHA held a very small part of the mortgage market when the subprime meltdown began. In fiscal year 2007, FHA held approximately four percent of the market, by loan count.⁷ Since then, FHA has quickly become the largest government insurer of mortgages in the world.⁸ As private mortgage insurers tightened their lending practices, FHA mortgages became a primary form of loans originated throughout the country.⁹

The size of FHA's single-family portfolio has increased by nearly 50 percent from \$466 billion in fiscal year 2008 to more than \$697 billion in fiscal year 2009.¹⁰ FHA currently has more

than six million single-family mortgages and 13,000 multifamily mortgages in its portfolio.¹¹ As of January 2010, FHA's share of the overall mortgage market had increased to more than 30 percent of all new loans.¹² With FHA's growth, the Government National Mortgage Association (Ginnie Mae)¹³ has also significantly increased its securitization of FHA and other federal agency loans into mortgage-backed securities. Ginnie Mae's market share has risen sharply from 5.1 percent in calendar year 2007 to 29.6 percent as of June 2010, in part because of the major decline in privately insured mortgage-backed securities issued while federal agency issuance of mortgage loans in fiscal year 2010 remained stable.¹⁴ Therefore, FHA's increased loan activity has made it a huge player in the mortgage industry, but being a huge player has made FHA an even bigger target for fraudsters.

Since its inception in 1934, FHA has been self-sustaining, meaning that insurance premiums paid by borrowers into the fund have been able to cover the losses from fluctuating defaults and foreclosures.¹⁵ However, higher claims and lower recoveries from the sale of foreclosed properties taken over by HUD have negatively affected the insurance fund in recent years. FHA is currently recovering only about 40



cents on the dollar of each insurance claim it has paid.¹⁶

FHA's November 2009 actuarial review concluded that the insurance fund's capital ratio¹⁷ is falling below the federally mandated two percent reserve. This means that should economic conditions and insured loan performance prove worse than projected in the study, the FHA insurance fund would not be able to sustain the needed level of funds to pay lenders for the high rate of losses incurred.¹⁸ With losses of this magnitude and a less than two percent reserve, mortgage fraud has a significant effect on the FHA insurance fund, emphasizing the need for civil actions to recover monies to make the federal government whole from losses resulting from fraudulent loans.

16) Ibid.

17) The 1990 Cranston-Gonzalez National Affordable Housing Act (42 U.S.C. §12701) defines the capital ratio as the ratio of the FHA insurance fund's economic value to its unamortized insurance-in-force.

18) Federal Housing Administration Annual Management Report, fiscal year 2009. <http://www.hud.gov/offices/hsg/fhfy09annualmanagementreport.pdf>.

5) Ibid.

6) Ibid.

7) Actuarial Review of the Federal Housing Administration Mutual Mortgage Insurance Fund (Excluding Home Equity Conversion Mortgages) for Fiscal Year 2009, issued November 6, 2009 http://hud.gov/offices/hsg/comp/rpts/actr/2009actr_exhecm.pdf.

8) Federal Housing Administration: http://portal.hud.gov/portal/page/portal/HUD/federal_housing_administration (July 29, 2010).

9) Ibid.

10) Kenneth M. Donohue, Inspector General, U.S. Department of Housing and Urban Development, written statement of Mr. Donohue before the Committee on Appropriations, Subcommittee on Transportation, Housing and Urban Development, and related agencies, United States Senate, March 25, 2010.

11) Ibid.

12) David H. Stevens, Assistant Secretary for Housing and FHA Commissioner, U.S. Department of Housing and Urban Development, prepared remarks for Exchequer Club, Washington, D.C., January 20, 2010 http://portal.hud.gov/portal/page/portal/HUD/press/speeches_remarks_statements/2010/Speech_01202010.

13) Ginnie Mae is a wholly-owned government corporation within HUD. The Ginnie Mae guaranty allows mortgage lenders to obtain a better price for their mortgage loans in the secondary market. The lenders can then use the proceeds to make new funds available for mortgage loans. Ginnie Mae guarantees investors the on-time payment of principal and interest on Mortgage-Backed Securities (MBS) that are backed by federally insured or guaranteed loans - mainly loans insured by FHA or guaranteed by the Department of Veterans Affairs. Ginnie Mae MBS are created when eligible mortgage loans are pooled by approved issuers and used as collateral for the issuance of securities in the secondary market. MBS are commonly referred to as "pass-through" certificates because the principal and interest of the underlying loans is "passed through" to investors. Regardless of whether the mortgage payment is made, investors in Ginnie Mae MBS receive full and on-time payment of principal and interest.

14) Inside Mortgage Finance Publications, Inside MBS & ABS: <http://www.imfpubs.com> (July 29, 2010).

15) Ibid.



HOW IS HUD'S WATCHDOG MAKING FHA FRAUDSTERS PAY?

HUD Inspector General Kenneth Donohue created a new Civil Fraud Division made up of 17 forensic auditors and a civil fraud attorney dedicated to assisting the new division. Their primary focus is mortgage fraud and finding ways to make the fraudsters pay back ill-gotten gains to the FHA insurance fund.

HUD OIG is pursuing prosecution of not only FHA lenders, but also the principals and individuals involved in fraud-related schemes. As industry participants migrate from subprime to FHA-insured loans, HUD OIG is concerned that those individuals that were involved in fraudulent subprime lending activities will bring their former fraudulent practices into FHA's loan portfolio. In 2007, HUD OIG successfully persuaded Congress to expand the Financial Institution

Reform, Recovery, and Enforcement Act of 1989, a banking statute, to include fraud against FHA. FIRREA penalties can reach 30 years imprisonment and \$1 million per violation or up to \$5 million for a continuing violation. By pursuing civil fraud cases against such individuals, HUD OIG hopes to keep them from furthering their schemes through FHA loans.

Coordination among federal entities is the key to making an impact on fraudulent loan activities. HUD OIG strongly believes in joint efforts to further its work and as such, is a principal member of a national Mortgage Fraud Working Group that arose out of the President's Financial Fraud Enforcement Task Force. The Mortgage Fraud Working Group also includes the Department of Justice, the Federal Bureau of Investigation, and the National Association of Attorneys General. This group looks to combine its criminal and civil resources to fight mortgage fraud.

In furtherance of HUD OIG's commitment to this endeavor, it initiated Operation Watchdog in January 2010, a focused review of poor performing FHA lenders. HUD OIG also contributed to Operation Stolen Dreams, a nationwide Department of Justice mortgage fraud sweep.

Operation Watchdog is an ongoing HUD OIG initiative focusing on mortgage companies with significant claim rates against the FHA mortgage insurance program. This initiative was prompted, in part, by the FHA commissioner who was alarmed by the incidence of excessive default rates by a number of poor performing FHA lenders. HUD OIG served subpoenas to the corporate offices of 15 mortgage companies in 11 states across the country, demanding documents

and data related to failed loans¹⁹ with original mortgage amounts of nearly \$41 million. HUD OIG identified these direct endorsement companies from an analysis of loan data focusing on companies with a significant number of claims, a certain loan underwriting volume, a high ratio of defaults and claims compared to the national average, and claims that occurred earlier in the life of the mortgage. These are key indicators of problems at the origination or underwriting stages of a mortgage loan.²⁰

While the lenders were not selected based upon known wrongdoing, HUD OIG is aggressively pursuing indicators of fraud if identified during the analysis. It is important to discern, for the long-term viability of the FHA program, whether these high claims and default rates were the result of a weak economy or if companies were ignoring, or even purposefully violating, FHA regulations. HUD OIG wants to send a very distinct message to the industry that, as the mortgage landscape has shifted, HUD OIG and the Department are watching very carefully and are poised to take action against bad performers, including pursuing civil fraud cases.²¹

Operation Stolen Dreams was the federal government's largest mortgage fraud takedown in United States history. Unlike previous mortgage fraud sweeps, Operation Stolen Dreams focused not only on federal criminal cases, but also on civil enforcement and restitution for victims.²² During the investigation, the government took action against more than 1,500 defendants who were

19) Ibid.

20) Ibid.

21) Ibid.

22) Federal Bureau of Investigation, Headline Archives, Operation Stolen Dreams, Hundreds Arrested in Mortgage Fraud Sweep, June 17, 2010 http://www.fbi.gov/page2/june10/mortgage_061710.html.

responsible for more than \$3 billion in losses due to bad loans and fraudulent practices. The government took civil action against nearly 400 defendants that led to recoveries of nearly \$200 million. When civil and criminal remedies were not feasible, the government used HUD administrative actions to deny bad lenders participation in the FHA mortgage insurance program.²³

WHAT TOOLS ARE IN THE OIG TOOLBOX TO PURSUE CIVIL REMEDIES?

HUD OIG, in concert with HUD, can employ several civil statutes or administrative remedies in addressing fraudulent activity in connection with HUD programs. These statutes and administrative remedies can result in a variety of remedies to HUD, including civil judgments, the imposition of monetary penalties and other sanctions, suspension, or debarment. The most used statute is 31 U.S.C. §3729, the False Claims Act which makes any person liable who knowingly submits, or causes to be submitted, a false or fraudulent claim for payment to the federal government or to an entity funded with federal monies. The federal government may recover three times the damages it sustains, plus a penalty of between \$5,500 and \$11,000 per violation. The statute of limitations is six years after the fraudulent act(s), or three years after discovery of the fraud if more than six but know more than 10 years have passed. For FHA loans, the False Claims Act liability is established when the defendant submits a false claim or HUD pays a fraudulent claim of the balance of a mortgage loan upon default. FHA insured the loan based on false statements made by the defendant,

making the defendant liable.

Another very useful civil action tool that is new to HUD is 12 U.S.C. §1833a, FIRREA. As described earlier, FIRREA is a banking statute that was changed as of July 31, 2008, to include FHA-insured loans. Under FIRREA, the federal government may recover civil penalties against persons who violate or conspire to violate specific provisions of criminal statutes involving financial fraud. Although liability depends on a violation of a criminal statute, the burden of proof is the preponderance of the evidence. The statute of limitations is 10 years. The United States may recover up to \$1 million per violation or up to \$5 million for a continuing violation. The civil penalty may be greater than these amounts if the defendants derived pecuniary (monetary) gain from the violation, or if the violation resulted in pecuniary loss to any person, in an amount greater than the \$1 million to \$5 million penalties, but cannot exceed the amount of such gain or loss. Another feature of FIRREA is that the Department of Justice can use subpoenas to compel testimony from the target before filing the complaint, and to produce documentary evidence.

As demonstrated by the chart on the following page, filing a FIRREA case versus using a criminal statute for submitting a false loan application to obtain a loan from a financial institution has monetary and evidentiary advantages.

If the fraud is ongoing or is about to be committed, the federal government can file an injunction pursuant to 18 U.S.C. §1345, the Anti-Fraud Injunction Act. This Act provides a civil remedy to stop a person who is violating, or is about to violate, a statutory offense such as bank, mail, or wire fraud; or who is committing, or is about to commit, a banking law violation. The government can use this

statute to freeze the perpetrator's assets.

The Department of Justice in the Central District of California recently filed three FIRREA cases²⁴ developed by HUD OIG.²⁵ These were the first FIRREA cases ever filed in relation to FHA loans. In each case, real estate professionals created false documents to obtain or help others obtain an FHA-insured loan. FHA has paid claims on many of these loans and other loans are in default.

HUD has administrative remedies that it can impose on those that defraud its programs. HUD can use 31 U.S.C. §3801 et seq., the *Program Fraud Civil Remedies Act*. Congress was concerned that small false claims were not being pursued so it gave agencies like HUD the ability to bring actions on false claims that are less than \$150,000. PFCRA cases are similar to False Claims Act cases but PFCRA cases are handled by the defrauded agency rather than through the judicial system. PFCRA imposes liability for false claims as well as false certification statements made to the federal government. PFCRA penalties cannot exceed \$7,500 per violation and damages imposed cannot exceed twice the amount of the false claim. The statute of limitations is six years with no option to extend. HUD's Office of Program Enforcement litigates PFCRA cases and levels the sanctions against bad players. PFCRA is an effective tool to more quickly and easily send a message to 'smaller-dollar' fraudsters than the more involved process of filing fraud cases in district court.

The HUD Reform Act of 1989 (12 U.S.C. §1708) established HUD's Mortgagee Review Board and 24 CFR (Code of Federal Regulations) Part 25 outlines its duties and procedures, which

23) Kenneth M. Donohue, Inspector General, U.S. Department of Housing and Urban Development, prepared remarks for the annual Association of Government Accountants, Professional Development Conference, Orlando, Florida, July 14, 2010.

24) United States of America vs. Beachwood Realty, et al., CV 10-4401; United States of America vs. Lowie Joey Enerio, CV 10-4402; and United States of America vs. Edward Woo Chen, CV 10-4403.

25) *Ibid*.

include withdrawing a lender's authority to write loans to be insured by FHA. In addition, HUD can impose civil monetary penalties on bad players under HUD-specific regulations in 24 CFR Part 30.35, which identifies 15 types of violations by mortgage lenders. Through its Mortgage Review Board, HUD can impose penalties of up to \$7,500 per violation, not to exceed \$1.375 million. Similarly, 24 CFR Part 30.36 allows HUD to impose penalties on anyone who submits false information in connection with an FHA-insured loan, up to \$6,050 for each violation, not to exceed \$1.21 million.

Further, HUD can debar and suspend individuals under 2 CFR Part 180 and 2 CFR Part 2424. Debarments and suspensions reach across all federal agencies. In addition, it can issue limited denials of participation but these are specific to HUD, limited to the program area defrauded, and are limited in the geographic area that the fraudster is denied participation.

WHAT MESSAGE DOES HUD OIG HAVE FOR FRAUDSTERS?

HUD's watchdog is on alert and sending a clear message - commit fraud against FHA and you will pay. HUD OIG is aggressively pursuing civil cases against bad players, and availing itself of HUD administrative sanctions to recover monies for FHA and to get bad players out of FHA programs. The agency expects that leveling large monetary damages and penalties against mortgage fraudsters will make civil proceedings an effective deterrent. Mortgage fraud can take months or even years to reveal itself, which means that HUD OIG has its work cut out for it in the coming years. But the agency is encouraged by its early successes and will continue to sniff out mortgage loan fraudsters and bring them to justice. If your organization is interested in setting up a civil fraud group or otherwise increasing your pursuits of civil fraud, contact Deputy Assistant Inspector General for Audit Ms. Joan Hobbs at (213) 534-2470. ☞



Kimberly R. Randall

Kimberly R. Randall is the director of HUD OIG's Civil Fraud Division. Ms. Randall has worked in the OIG community for 23 years, working for the U.S. Department of Agriculture, Resolution Trust Corporation, and HUD.

She earned her Bachelor of Science in Business Administration (Accounting) from the University of Central Missouri.

Ms. Randall is a certified public accountant and a certified fraud examiner. Her recent OIG honors and awards include being named HUD OIG's 2008 Audit Manager of the Year and receiving a 2005 PCIE Award for Excellence.

Within HUD OIG, Ms. Randall serves as an ombudsperson and supervisory training instructor, and served as a mentor for its leadership development program.

False Loan Application

12 U.S.C. § 1833a

18 U.S.C. § 1014

- | | |
|---|--|
| <ul style="list-style-type: none"> • \$ Penalty: \$1M, or up to \$5M for continuing violations or the gain or loss amount - whichever is greater • No imprisonment • Preponderance of the evidence • Pre-filing discovery • Compelled target statement | <ul style="list-style-type: none"> • \$ Penalty: \$1M & restitution • Imprisonment • Beyond a reasonable doubt • Pre-filing discovery • No compelled target statement |
|---|--|

INTELLIGENT WHISTLEBLOWING

BY LINDSAY BOYD AND
BRIAN FUTAGAKI

The tension between Congress' and the American people's need for information, and the executive branch's interest in discretion and confidentiality is structural to the republic. Nowhere are competing interests more compelling than in the case of intelligence community whistleblowing. The Department of Defense Office of Inspector General plays a critical role in balancing these interests by providing an authorized place for DoD whistleblowers to make classified disclosures as well as an authority to investigate allegations of reprisal against whistleblowing complainants in DoD intelligence agencies. DoD is home to a majority of the nation's intelligence agencies.¹ Therefore, DoD IG provides protection to a substantial number of the nation's civilian intelligence personnel. This article will give a history of the intelligence community whistleblowing and outline the procedures employed by DoD IG to protect DoD intelligence community whistleblowers from reprisal.²

THE INTELLIGENCE COMMUNITY AND THE WPA

The Civil Service Reform Act of 1978 came about due to a growing public concern over the efficiency, integrity, and



accountability of the federal workforce.³ These concerns led to the establishment of the merit system principles, a set of governing principles for the federal workforce.⁴ Included in these principles is the notion that employees should be protected from reprisal for whistleblowing.⁵ The CSRA provided the first substantive protections for agency whistleblowers, creating the Office of Personnel Management, the Office of Special Counsel, and the Merit Systems Protection Board.⁶ The Whistleblower Protection Act of 1989 enhanced whistleblower protections of the CSRA by recognizing that federal employees who make protected disclosures “serve the public interest by

assisting in the elimination of fraud, waste, abuse, and unnecessary government expenditures.”⁷ Specifically, the WPA gave whistleblowers an independent right to pursue an appeal to MSPB.⁸

However, both the CSRA and the WPA contained an exemption for employees of the intelligence community.⁹ Substantive protections for intelligence community whistleblowers arise from two specific sources: the Intelligence Community Whistleblower Protection Act of 1998, and the Inspector General Act of 1978. In 1998, Congress passed the ICWPA.¹⁰ Despite its name, the ICWPA does not contain general protections against reprisal. Perhaps a more appropriate name for the ICWPA would be the Intelligence Community

1) The Department of Defense intelligence agencies include the Defense Intelligence Agency, National Security Agency, National Reconnaissance Office, and National Geospatial-Intelligence Agency as well as all military service and combatant command intelligence components.

2) This article discusses policies and procedures pertaining to DoD intelligence agencies. DoD does not receive disclosures or investigate reprisal involving intelligence personnel outside of DoD such as persons employed by the Central Intelligence Agency or Federal Bureau of Investigation. Also, any changes enacted by recent legislation creating an Inspector General for the intelligence community is not addressed in this article.

3) H. Manley Case, Project on the Merit Systems Protection Board: The Civil Service Reform Act of 1978: Article: Federal Employee Job Rights: The Pendleton Act of 1883 to the Civil Service Reform Act of 1978, 29 How. L.J. 283 (1986).

4) 5 U.S.C. § 2301.

5) 5 U.S.C. § 2301(b)(9).

6) Civil Service Reform Act of 1978, P.L. 95-454; 92 Stat. 1111 (codified at 5 U.S.C. §§ 1101, 1201, 1211).

7) Whistleblower Protection Act of 1989, P.L. 101-12; 103 Stat. 16.

8) 5 U.S.C. § 1221.

9) 5 USC § 2302 (a)(2)(c).

10) Intelligence Community Whistleblower Protection Act of 1998, P.L. 105-272; 112 Stat. 2396 (codified at 5 U.S.C. App. § 8h).

Disclosure Act since the act addresses a very specific dilemma, namely, how does one report wrongdoing when the wrongdoing involves classified information? The ICWPA provides some answers.

The ICWPA allows for employees of the four DoD intelligence agencies (Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, and National Reconnaissance Office) to bring matters of “urgent concern” to congressional attention through the Office of Inspector General.¹¹ The statute defines “urgent concern” to mean “a serious or flagrant problem, abuse, violation of law or executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinion concerning public policy matters.”¹² Once an employee has made a disclosure to an IG under the ICWPA, the law proscribes a very specific sequence of events which must take place. The Inspector General must determine whether the complaint is credible within 14 calendar days of receiving the complaint.¹³ Upon making such a determination, the inspector general shall transmit to the head of the establishment (and in the case of DoD, the secretary of defense) a notice of that determination, together with the complaint or information.¹⁴ The head of the establishment must then forward the transmittal to the intelligence committees within seven calendar days of receipt of the information.¹⁵

It is important to emphasize what the ICWPA does not do. The ICWPA does not provide statutory protection from reprisal.¹⁶ It also does not apply to personnel detailed or assigned

to the military services, combatant commands, or the Office of the Secretary of Defense, unless they are employees of the four DoD intelligence agencies.¹⁷ The ICWPA does not cover all complaints of DoD intelligence agency employees.¹⁸ Rather, it provides an authorized channel for employees of the four DoD intelligence agencies to communicate classified information of “urgent concern” to Congress.

Congress passed the Inspector General Act in 1978, the same year as the CSRA. The IG Act authorizes the inspectors general to receive and investigate complaints or information received from agency employees concerning a violation of law, rules, or regulations; or mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to the public health and safety.¹⁹ Like the CSRA, the IG Act also contains substantive protections against whistleblower reprisal providing:

Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to an inspector general, unless the complaint was made or the information disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.²⁰

Unlike the CSRA, the IG Act contains no exemption for intelligence community employees.²¹ Within DoD IG, the Civilian Reprisal Investigations direc-

“Since the nature of work in a DoD intelligence agency uncompromisingly requires access to sensitive and classified material, revoking a security clearance is tantamount to termination for any of its employees.”

torate investigates allegations of reprisal from civilian appropriated fund employees.²² DoD IG exercises primary jurisdiction over complainants from DoD intelligence agencies that do not have access to OSC.²³ While the reforms of 1978 intended to apply the merit system principles to all federal agencies, these laws exempted intelligence personnel from any enforcement mechanisms. CRI provides an avenue for intelligence personnel to have their cases investigated by a neutral and objective party.

PROTECTING THE INTELLIGENCE COMMUNITY

The CRI directorate was established under the investigations division of DoD IG in 2003. The directorate investigates cases of whistleblower reprisal by determining whether a complainant was subject to a negative action as a result of disclosing instances of fraud, waste, and abuse; or violations of law, rule, and regulation. In conducting its investigations, CRI operates under laws and definitions outlined under Title 5 of the United States Code (5 U.S.C.), which pertains

11) 5 U.S.C. App. § 8H.
12) 5 U.S.C. App. § 8H (h).
13) 5 U.S.C. App. § 8H (b).
14) Id.
15) 5 U.S.C. App. § 8H (c).
16) 5 U.S.C. App. § 8H.

17) Id.
18) 5 U.S.C. App. § 8H (a)(1)(A).
19) 5 U.S.C. App. § 7.
20) 5 U.S.C. App. § 7 (c).
21) The IG Act does provide that the Secretary of Defense may restrict IG action in certain intelligence and national security matters. 5 USCS Appx § 8 (b)(1).

22) DoDD 5106.1 ¶ 5.19.1.
23) Inspector General Instruction 7050.71(2)(h)(1) and 7050.11 (e) (f).

to professional standards of civilian government employees. Under section 2302 of 5 U.S.C., a negative action that a whistleblower may experience, such as demotion or termination, is defined as a personnel action.²⁴ If a CRI investigation reveals causality between a disclosure of wrongdoing and a personnel action taken against the civilian source of that disclosure, the related case is substantiated. However, should an involved agency produce clear and convincing evidence that a personnel action would have been taken against a civilian employee absent their disclosure of alleged wrongdoing, the inspector general will not substantiate the case.

There are various avenues by which whistleblower reprisal complaints are referred to CRI. In many cases, complainants file their cases with the DoD Hotline. Any DoD employee who believes that they have been retaliated against for reporting a violation of law, rule, or regulation, can contact the hotline to file a report. Once the preliminary report is written up and assigned a case number, it may be forwarded to CRI for review. In addition, complainants from the intelligence community may contact a member of Congress to report the whistleblower retaliation. Should the representative's office deem the account viable, it may in turn be forwarded to CRI. Similarly, inspectors general of the intelligence agencies themselves may receive reprisal complaints and refer them to CRI.

Once an investigation is concluded, the inspector general issues a report to the proponent command of the involved agency. Reports of unsubstantiated claims typically result in a permanent closure of the case with no corrective action. Reports of substantiated whistleblower reprisal accompany recommendations that the case's complainant be made whole through remedies such as

formal apology or back pay, while corrective action be taken against management officials responsible for the reprisal action.

CRI offers especially broad protection to DoD intelligence community whistleblowers because it is the only entity that recognizes a negative change in a civilian DoD employee's security clearance as grounds for an investigation. While 5 U.S.C. offers significant security for civilian whistleblowers, it is not without limitation in protecting employees of DoD intelligence agencies. Section 2302 of Title 5 lists 12 separate prohibited personnel practices that, when following a disclosure of wrongdoing, may constitute a whistleblower reprisal.²⁵ Especially egregious actions such as termination, reassignment, or demotion are included among these; however, action against a security clearance is not. Since the nature of work in a DoD intelligence agency uncompromisingly requires access to sensitive and classified material, revoking a security clearance is tantamount to termination for any of its employees.

For this reason, CRI investigates allegations of reprisal by security determination through the authority of the IG Act of 1978. Under the IG Act, there are no exemptions for intelligence community whistleblowers and a revocation of security clearance may be investigated as a potential abuse of authority. In its reports outlining cases of reprisal through security clearance decisions, CRI classifies a negative action taken by a responsible management official as a "unfavorable personnel security determination." The DoD Personnel Security Program defines an "unfavorable personnel security determination" as:

A denial or revocation of clearance for access to classified information; denial or revocation of access to classified infor-

*mation; denial or revocation of a Special Access authorization (including access to Special Compartmented Information; nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring trustworthiness determination under this regulation; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.*²⁶

In addition to the actions included in this definition, CRI also investigates suspension of security clearances as well as recommendations to an agency's central adjudication facility to revoke, deny, or suspend security clearances as possible unfavorable personnel security determinations. While not actionable by themselves, suspensions and recommendations to a CAF are examined by CRI because they may constitute contributing pretexts to reprisal through security determination.²⁷ By identifying these measures as actionable unfavorable personnel security determinations, CRI is able to provide broad protection to whistleblowers within the DoD intelligence community.

Notable examples of CRI's work within the last three years include:

- A case of whistleblower protection at the National Security Agency. The complainant alleged reprisal for disclosing that a managing official created a hostile work environment through intimidating and inappropriate workplace conduct. NSA substantiated the complainant's allegation of reprisal by significant change in work duties, responsibilities, and

24) 5 U.S.C. § 2302.

25) 5 U.S.C. § 2302 (b).

26) DoD 5200.2-R, Department of Defense Personnel Security Program, Subsection DL1.1.30.

27) Johnson v. Department of Justice, 2007 M.S.P.B. 42; 104 M.S.P.R. 624, ¶7 (2007).

- hours. DoD IG concurred;
- A case of alleged whistleblower reprisal within the Defense Intelligence Agency. The complainant in this case alleged reprisal for disclosing misuse of a congressionally-authorized countertrafficking and counternarcotics billet. DIA did not substantiate the allegation, concluding that clear and convincing evidence existed and that the negative action would have been taken absent the complainant's disclosure. DoD IG concurred;
- A case of whistleblower protection at the now-dissolved Counterintelligence Field Activity. The complainant alleged reprisal for disclosing an agency supervisor's relationship with and preferential treatment of a retained defense contractor. DoD IG substantiated the complainant's allegation of reprisal by removal of duties, reassignment, and eventual termination.

As partners of DoD IG, NSA and DIA are at the forefront of whistleblower protection within the intelligence and counterintelligence community. By fostering these partnerships, as well as utilizing the IG Act of 1978, DoD IG aims to investigate claims of whistleblower reprisal from the defense intelligence community in order to protect all of its employees from reprisal.

With solid and thorough whistleblower protection mechanisms in place, workers from all corners of the DoD may help to ensure that this nation's largest and most well-funded professional entity may truly serve as a model of integrity and efficiency. ☞



Brian Futagaki

Brian Futagaki is an investigator on the Procurement Fraud Reprisal Team in the Civilian Reprisal Investigations Directorate of DoD IG.

Mr. Futagaki began his career with Wells Fargo Bank in San Jose, Calif. Later, he accepted a position in Chiba-ken, Japan as a language instructor and event planner. While in Asia, Mr. Futagaki worked as a volunteer organizer for the non-governmental organization PEPY Ride, which provides educational relief to rural Cambodian communities.

Mr. Futagaki has a bachelor's degree in Economics and Quantitative Studies from the University of California at Santa Cruz and a master's degree in Public Diplomacy from Syracuse University.

Mr. Futagaki also spent the summer of 2008 in Geneva, Switzerland, where he interned with the World Health Organization. In addition, he interned at the Support to Public Diplomacy office of the Department of Defense, where he assisted in drafting strategic communication plans pertaining to Bangladesh, Japan, and Afghanistan.



Lindsay Boyd

Lindsay Boyd is an investigator on the National Security Reprisal Team in the Civilian Reprisal Investigations Directorate of DoD IG.

Ms. Boyd began her association with the Office of Inspector General while at The George Washington University Law School, serving as an investigative law clerk.

Prior to law school, Ms. Boyd served as a community representative to the Honorable Bob Filner (CA-51), managing congressional inquiries regarding the Departments of Defense, Veterans Affairs and the National Guard.

Prior to joining the Department of Defense, Ms. Boyd also clerked with the Office of the Public Defender for Arlington County and the City of Falls Church. Ms. Boyd also clerked for the Humane Society of the United States, assisting attorneys in researching and preparing animal protection lawsuits in state and federal courts. Ms. Boyd graduated with honors from the George Washington University Law School in 2009 and is a member of the State Bar of California.

FAMILIAL DNA DATABASE SEARCHING

BY FITZHUGH CANTRELL

Recent advances in DNA technology are evolving so rapidly that some have surpassed current state and national criminal laboratory policies. None of these advances in DNA technology is more controversial than familial DNA database searching. The traditional DNA database search involves identifying an exact match between a crime scene DNA profile and a criminal database suspect profile. Familial DNA database searches occur following a failed exact match search and involve changing the parameters of the search to include partial or close DNA matches between the crime scene profile and the criminal databases. Once a close match is identified, a criminal investigation focuses on the relatives of the near DNA match, attempting to determine if they are responsible for the crime. This investigative practice has been embraced by police services in Great Britain and enthusiastically supported by a handful of prosecutors in the U.S. However, the practice has been criticized by many in the legal and academic communities due to privacy rights issues. To further complicate this practice, there still remains an issue as to what exactly constitutes familial DNA database searching.

There is an important distinction between familial DNA database searching and partial DNA matches. A partial DNA match is an *unintended* match during a normal initial criminal database search. A familial DNA database search involves a *deliberate* follow-up search for similar matches usually following an initial search that failed to



identify an exact match from the criminal database. This distinction between the two searches is particularly important when the suspect profile is deteriorated and contains less than the full identifying DNA markers. Assessing a partial match practice can be particularly difficult when the case involves a deteriorated DNA sample, one with less than the normal 26 alleles, something that is not uncommon in crime scene DNA, particularly cold cases.¹ In comparing familial searching and partial match practices, one finds that legal professionals are equally divided on the practice, both stating that if you allow one practice, it is hard to disallow the other. From a legal standpoint, it is hard to separate the two practices.

An important aspect of the problem involving familial DNA searches is the lack of a national standard involving its practice in the U.S. State policies vary on allowing its practice within their state criminal database systems. At the nation-

al level, the FBI's Combined DNA Index System prohibits these types of searches. The FBI CODIS has recently made some concessions in their policy to allow states to share this type of information if they choose. The FBI's policy leaves it up to the individual states to decide whether to allow familial DNA database searching, and has critics on both sides of the issue. Many consider this policy a failure to take a position on the practice, which has resulted in various state policies on the practice.²

FAMILIAL SEARCHING POLICY INCOHERENCE

Initially, familial searching was limited to individual state practices as well as the CODIS inter-state regulations. This rule prohibited the release of any identifying information about an offender in one state's database to officials in another state unless the offender's DNA was an exact match. In 2006, however, Denver

1) Harmon, Rockne. Forensic/Cold Case Consultant. Former district attorney. Personal interview. March 12, 2010.

2) Ram, Natalie. Greenwall Fellow in Bioethics and Health Policy at John Hopkins and Georgetown Universities. Personal interview. January 20, 2010.

District Attorney Mitch Morrissey identified a local case where a close match was found between evidence taken from the scene of a rape in Denver and with convicted felons in California, Oregon, and Arizona. This match indicated that the actual perpetrator was potentially a relative of one of the unidentified convicted felons. DA Morrissey approached the FBI and convinced them to modify their stance regarding familial DNA searching. Follow-up testing by the states revealed that none of the profiles in the state databases were related to the Colorado rapist. Regardless of the lack of success, the new FBI interim policy left it up to each state to decide whether it would report to intra-state investigators any partial matches that might turn up in the course of ordinary database searches.³

Since the FBI released its interim policy, states have taken a number of approaches to the issue. California was the first to set up a comprehensive familial searching policy. Maryland is the only state with state legislation on familial searching, and it bans the practice. This variance is further complicated when you examine different state DNA database collection and use standards. Kentucky collects DNA samples from persons found guilty of misdemeanors while at the same time restricting DNA appeal testing for inmates serving life sentences. Other states collect DNA samples from only convicted felons. Despite the broad spectrum of state policies on DNA, many states have not taken an “official stance” on familial DNA database searching. Nonetheless, there are trends of state familial DNA database searching policy and statute expansion. Of the 32 states with some policy or practice already in place, at least 16 permit the reporting of a partial DNA match to criminal investigators for the purpose of familial

investigation.⁴ The practice is still very premature in states like California which has had the policy since 2008. Initial reports were that California has attempted familial searching six times and have yet to identify a partial match until a recent break came in July 2010.⁵ In the break, the LAPD arrested the “Grim Sleeper” serial killer, Lonnie David Franklin, who the police have charged with 10 counts of murder. This arrest was California’s first successful attempt in familial DNA searching.⁶

POLICY ALTERNATIVES

The three main policy alternatives for the FBI CODIS laboratory regarding familial DNA searching are: (1) the FBI should discourage familial searching within states by denying national funding to those states that allow its practice; (2) the FBI should encourage familial searching both within states and nationally by requiring states to perform familial searches or risk being denied federal funds; or (3) the FBI should maintain the interim policy which allows states to set their own policy regarding familial searching and does not conduct national

familial searches using CODIS. The criteria used to properly evaluate these alternatives are: the legal and privacy rights issues surrounding familial DNA searching, the effectiveness of familial searching, and the impact familial searching will have on public safety.

PRIVACY RIGHTS AND FAMILIAL SEARCHING

Privacy advocates argue that “developing technology, rather than constitutional analysis and informed public decision making, is driving the expansion of DNA databanks.”⁷ The Supreme Court has repeatedly held that authorities may not conduct searches for general law enforcement purposes without probable cause. Maryland is one of the few states that has outlawed familial DNA searching. Critics are also disturbed by the demographics of DNA databases. Some consider the existing criminal databases as already racially skewed and further developing familial DNA leads from these databases would exacerbate the problem.⁸

Despite the vocal concern by privacy and defense advocates, legal scholars recognize that making a Fourth Amendment claim about familial DNA searching is difficult. DA Morrissey argues that since individuals in the database have already been arrested or convicted of a crime, they have a reduced expectation of privacy. Additionally, DA Morrissey argues that the alleged suspect who



4) Ram, Natalie. “DNA Confidential.” *Science Progress*. November 2, 2009.

5) *Supra* note 1.

6) Simon, Mallory. “Arrest made in Los Angeles Grim Sleeper serial killer case.” *CNN.com*; <http://www.cnn.com/2010/CRIME/07/07/grim-sleeper.arrest/index.html?iref=S1>. July 7, 2010.

7) Simoncelli, Tania, and Sheldon Krinsky. “A New Era of DNA Collection: At What Cost to Civil Liberties?” *American Constitution Society for Law and Policy*. 2007.

8) Nakashima, Ellen. “From DNA of Family, a Tool to Make Arrests.” *Washington Post*. April 21, 2008.

3) Rosen, Jeffrey. “Genetic Surveillance for All.” *Slate Magazine*. March 17, 2009.

Alternatives	Costs*	Legal Feasibility	Safety Impact	Political Feasibility	Total
Encourage State Familial Searches	3	2	2.5	2	9.5
States Decide Independently	2.5	4	1.5	3	11
Discourage State Familial Searches	4	1.5	0	1.5	7

Chart: Scale 0-4 (0 - none, 1 - little, 2 - moderate, 3 - significant, 4 - high)

*Costs meaning affordability.

left his DNA at the crime scene gave up his expectation to privacy when he left his DNA sample there. The last legal argument favoring familial searching simply states a suspect identified from a familial search cannot claim legal standing to challenge the DNA profile search of his sibling, parent, or offspring. This standing issue is a fundamental issue to overcome, even before a challenge can be seriously pursued. The conventional legal wisdom is that familial DNA searching is a close call that legally depends on the specifics involved, but may be a harder challenge for the defense because of the legal standing issue.⁹

THE EFFECTIVENESS OF FAMILIAL DNA SEARCHING

On page 1315 of Frederick Bieber, et al, Science magazine article "Finding Criminals Through DNA of Their Relatives," writes about the effectiveness of familial DNA searching. Bieber states, "consider a hypothetical state in which the "cold-hit" chance of finding a match between a crime scene and someone in the offender database is 10 percent. For example, if among criminals who are not in the database themselves, five percent of them have a close relative (parent/child or sibling) who is. Based on these

projections, the estimates indicate that up to 80 percent of those five percent could be indirectly identified. It follows that kinship analyses could increase a 10 percent cold-hit rate to 14 percent which is an overall increase of 40 percent." Last year there were approximately 20,000 cold hits and it is estimated that familial searching has the potential for thousands more once the practice becomes a standard investigative step.¹⁰ They argue this based on the ineffectiveness of DNA database operations in a study conducted by the University of Nebraska at Omaha by Samuel Walker and Michael Harrington, where only one of eighteen database searches led to the violator responsible. Some law enforcement officials have expressed concern that funding for these DNA database searches and analysis would reduce existing funding from more established law enforcement measures such as following up on traditional investigative leads or placing uniform officers on patrol.¹¹

THE PUBLIC SAFETY IMPACT OF FAMILIAL DNA SEARCHING

It is difficult to state the public safety impact of familial DNA searching since the practice has just started in the United States. Despite the potential impact to public safety, the fundamental question remains: is familial DNA searching

worth the risk to privacy at the national level? Many believe that it isn't, citing studies that state the overwhelming majority (87 percent) of traditional-offender hits occur within the state in which the crime occurred. The costs involved in encouraging all states to perform familial DNA searching are moderately low. Initial start-up costs in implementing a modified version of the existing computer software for the state databases could be significantly reduced if they used or modified the current software that either California or Colorado utilizes.¹² Other costs involve additional comprehensive DNA testing on the seized sample. The real issues underlying familial DNA searching concern the legal and political feasibility of the practice. Legal scholars on both sides of the issue agree that both fortuitous partial DNA matches and familial searching are difficult to distinguish legally, and both practices should be found either unconstitutional or constitutional.¹³ The Policy Alternative Chart attempts to rate the likelihood of potential outcomes with a higher number given to that which is most reasonable.

POLICY ALTERNATIVE CHART AND ANALYSIS OF THE ALTERNATIVES

The Policy Alternative Chart analysis favors keeping the current policy of the FBI CODIS, which allows states to decide whether to conduct familial DNA searches. The fundamental belief is that familial DNA searching is likely premature for making final decisions on the practice at the national level. Also, many believe that states can have different practices on aspects of public safety and privacy rights like familial searching. The practice could be just another potential capability of a state database, something

9) Supra note 1.

10) Supra note 7.

11) Bieber, Frederick, Charles Brenner, and David Lazer. "Finding Criminals Through DNA of their Relatives." Science Magazine, Vol. 312. June 2, 2006.

12) Supra note 1.

13) Supra note 2.

that doesn't necessarily need a national standard given the difficulty involved. Overall, it would be difficult for the FBI CODIS to advocate the practice at the national level citing an expected significant improvement to public safety without additional successes like the "Grim Sleeper" case as well current U.S. state statistics on the practice.

The potential political landmines involving familial DNA searching come from all sides: privacy right groups, groups critical of "big brother" government expansion, African-American political leaders concerned with law enforcement racial profiling, and law and order groups critical of perceived "pro-criminal" legislation if the practice is prohibited. Political ideology of the state appears to be a factor in the practice, but this is not always the case. Despite a greater percentage of traditional "red states" having policy in favor of the familial searching, there are several significant exceptions. California, a traditional blue state, was the first state to formally approve familial searching. Connecticut, New York, Washington, and Oregon also permit partial match searches to be reported. However familial searching is not allowed in historically political "swing states" like Ohio and Michigan.¹⁴

THE FUTURE OF FAMILIAL SEARCHING

California Attorney General Jerry Brown decided to resolve the issue of familial searching in California by establishing a state policy on the practice instead of pushing the legislation, which is something many believe is the future of familial searching. California's familial searching policy placed significant safeguards in place, establishing strict criteria which must be presented to the Familial Searching Committee. The FSC is made up of a panel of state certified

subject matter experts in both the legal and scientific fields. Some of the criteria require that cases being presented to the FSC must have all logical investigative leads completed and a full DNA profile identified from a single source profile in a crime scene. A single source profile in a crime scene is usually common in sexual crimes or violent crimes involving only one attacker. The CA familial searching policy states that it can only be used in major violent crimes where there is a serious risk to public safety. Furthermore, the CA policy requires additional comprehensive DNA testing on all suspect samples before the search is conducted. When a familial search identifies a match, the FSC (not the investigator) initiates a background investigation on the candidate to determine whether that candidate can be eliminated by historical facts and relationships or circumstances surrounding being a potential relative of the true perpetrator.¹⁵

The CA familial searching policy is one of the most advanced pro-familial searching policies and the FBI CODIS should gather a working group of subject matter experts surrounding various legal, scientific, and human rights fields to closely monitor their results. Familial DNA database searching is no doubt an important scientific advancement, but its use by law enforcement should be taken with caution. An incremental state-by-state approach to the practice, despite its many drawbacks, could be an effective test case for determining its national impact on public security as well as privacy rights. ☛

This article is a condensed version of a capstone paper submitted to Georgetown University as a requirement of the Inspector General Master of Policy Management program.



Fitzhugh L. Cantrell

Fitzhugh L. Cantrell is a supervisory special agent with the Naval Criminal Investigative Service currently assigned to the Office of Special Projects. He began his law enforcement career as a state trooper with the Maryland State Police. Mr. Cantrell previously served as the supervisor of the NCIS Cold Case Homicide Division and special agent afloat onboard the U.S. Naval aircraft carrier USS Truman (CVN 75) in support of Operation Iraqi Freedom. He earned his Bachelor of Arts from Hampden-Sydney College, has a master's degree in Public Administration from Old Dominion University, and another master's degree in policy management from Georgetown University.

¹⁴) Supra note 2.

¹⁵) Supra note 1.

STRENGTHENING INTEGRITY: NEW TOOLS IN THE AFFORDABLE CARE ACT

Congressional testimony before the U.S. House of Representatives, Committee on Ways and Means, Subcommittees on Health and Oversight

BY LEWIS MORRIS

June 15, 2010 - Good morning Chairmen Stark and Lewis, Ranking Members Herger and Boustany, and other distinguished members of the subcommittees. I am Lewis Morris, Chief Counsel to the Inspector General for the U.S. Department of Health & Human Services. I thank you for the opportunity to appear before you today to discuss new tools in the recently enacted Patient Protection and Affordable Care Act that will help to combat fraud, waste, and abuse in the health care system.

Fraud, waste, and abuse cost taxpayers billions of dollars each year and put beneficiaries' health and welfare at risk. The impact of these losses and risks is exacerbated by the growing number of people served by these programs and the increased strain on federal and state budgets. With new and expanded programs under the Affordable Care Act, it is critical that we strengthen oversight of these essential health care programs.

My testimony will describe OIG's strategy for strengthening the integrity of the health care system and how the Affordable Care Act significantly bolsters that effort. It will also describe how OIG is using data, technology, and cutting edge techniques to advance the fight against health care fraud.



HEALTH CARE FRAUD, WASTE, AND ABUSE ARE SERIOUS PROBLEMS

Although there is no precise measure of health care fraud, we know that it is a serious problem that demands an aggressive response. While the majority of health care providers are honest and well-intentioned, a minority of providers who are intent on abusing the system can cost taxpayers billions of dollars.

Health care fraud schemes commonly include billing for services that were not provided or were not medically necessary, purposely billing for a higher level of service than what was provided, misreporting costs or other data to increase payments, paying kickbacks, and/or stealing providers' or beneficiaries' identities. The perpetrators of these schemes range from street criminals who believe it is safer and more profitable to steal from Medicare than trafficking in

illegal drugs, to Fortune 500 companies that pay kickbacks to physicians in return for referrals.

Many OIG investigations target fraud committed by criminals who masquerade as Medicare providers and suppliers, but who do not provide legitimate services or products. The rampant fraud among durable medical equipment suppliers in South Florida is a prime example. In these cases, our investigations have found that criminals set up sham DME storefronts to appear to be legitimate providers, fraudulently bill Medicare for millions of dollars, and then close up shop and reopen in a new location under a new name and repeat the fraud. The criminals often pay kickbacks to physicians, nurses and even patients to recruit them as participants in the fraud scheme.

The Medicare program is increasingly infiltrated by violent crimi-

nals, and our investigations are also finding an increase in sophisticated and organized criminal networks. For example, in Los Angeles in 2008, six men were charged with running an organized crime ring that stole nearly \$2 million from federal and private insurers. These criminals stole money from Medicare and other insurers by stealing the identities of legitimate providers and then funneled these funds into other criminal enterprises, including illegal drug rings. During the arrests in these cases, investigators encountered and seized weapons and ammunition, including assault rifles, submachine guns, and handguns, as well as bullet-proof vests.

Some fraud schemes are viral, i.e., schemes are replicated rapidly within geographic and ethnic communities. Health care fraud also migrates—as law enforcement cracks down on a particular scheme, the criminals may shift the scheme (e.g., suppliers fraudulently billing for DME have shifted to fraudulent billing for home health services) or relocate to a new geographic area. To combat this fraud, the government’s response must also be swift, agile, and organized.

Health care fraud is not limited to blatant fraud by career criminals and sham providers. Major corporations such as pharmaceutical and medical device manufacturers and institutions such as hospitals and nursing facilities have also committed fraud, sometimes on a grand scale. OIG has a strong record of investigating these corporate and institutional frauds, which often involve complex billing frauds, kickbacks, accounting schemes, illegal marketing, and physician self-referral arrangements. In addition, we are seeing an increase in quality of care cases involving allegations of substandard care.

Waste of funds and abuse of the health care programs also cost taxpayers billions of dollars. In fiscal year 2009, the Centers for Medicare & Medicaid Ser-

vices estimated that overall, 7.8 percent of the Medicare fee-for-service claims it paid (\$24.1 billion) did not meet program requirements. Although these improper payments do not necessarily involve fraud, the claims should not have been paid. For our part, OIG reviews claims for specific services, based on our assessments of risk, to identify improper payments. For example, an OIG audit uncovered \$275.3 million in improper Medicaid payments (federal share) from 2004 to 2006 for personal care services in New York City. As another example, an OIG evaluation of payments for facet joint injections (a pain management treatment) found that 63 percent of these services allowed by Medicare in 2006 did not meet program requirements, resulting in \$96 million in improper payments.

OIG’s work has also demonstrated that Medicare and Medicaid pay too much for certain services and products, and that aligning payments with market costs could produce substantial savings. For example, in 2007, OIG reported that Medicare reimbursed suppliers for pumps used to treat pressure ulcers and wounds based on a purchase price of more than \$17,000, but that suppliers paid, on average, approximately \$3,600 for new models of these pumps. Likewise, in 2006, Medicare allowed approximately \$7,200 in rental payments over 36 months for an oxygen concentrator that cost approximately \$600 to purchase. Beneficiary coinsurance alone for renting an oxygen concentrator for 36 months exceeded \$1,400 (more than double the purchase price).

OIG’S FIVE-PRINCIPLE STRATEGY

Combating health care fraud requires a comprehensive strategy of prevention, detection, and enforcement. OIG has been engaged in the fight against health

care fraud, waste, and abuse for more than 30 years. Based on this experience and our extensive body of work, we have identified five principles of an effective health care integrity strategy.

1. Enrollment: Scrutinize individuals and entities that want to participate as providers and suppliers prior to their enrollment or reenrollment in the health care programs.
2. Payment: Establish payment methodologies that are reasonable and responsive to changes in the marketplace and medical practice.
3. Compliance: Assist health care providers and suppliers in adopting practices that promote compliance with program requirements.
4. Oversight: Vigilantly monitor the 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.

OIG uses these five principles in our strategic work planning to assist in focusing our audit, evaluation, investigative, enforcement, and compliance efforts most effectively. These broad principles also underlie the specific recommendations that OIG makes to HHS and Congress. The Affordable Care Act includes provisions that reflect these program integrity principles and that we believe will promote the prevention and detection of fraud, waste, and abuse in the health care system.

AFFORDABLE CARE ACT

The breadth and scope of health care reform alter the oversight landscape in many critical respects, and as a result, OIG will assume a range of expanded oversight responsibilities. The ACA provides us with expanded law enforcement authorities, opportunities

for greater coordination among federal agencies, and enhanced funding for the Health Care Fraud and Abuse Control program. In addition, new authorities for the secretary and new requirements for health care providers, suppliers, and other entities will also promote the integrity of the Medicare, Medicaid, and other federal health care programs. The following are a few examples of how the ACA will strengthen our oversight and enforcement efforts.

EFFECTIVE USE OF DATA AND INTEGRITY OF INFORMATION

Provisions in Section 6402 of the Affordable Care Act will enhance OIG's effectiveness in detecting fraud, waste, and abuse by expanding OIG's access to and uses of data for conducting oversight and law enforcement activities. For example, Section 6402 exempts OIG from the prohibitions against matching data across programs in the Computer Matching and Privacy Protection Act and authorizes OIG to enter into data sharing agreements with the Social Security Administration.

The law also requires the department to expand CMS's integrated data repository to include claims and payment data from Medicaid, Veterans Administration, Department of Defense, Social Security Administration and Indian Health Service, and fosters data matching agreements among federal agencies. These agreements will make it easier for the federal government to help identify fraud, waste, and abuse.

Further, the ACA recognizes the importance of law enforcement access to data. Access to "real-time" claims data—that is, as soon as the claim is submitted to Medicare—is especially critical to identifying fraud as it is being committed. Timely data is also essential

to our ability to respond with agility as criminals shift their schemes and locations to avoid detection. We have made important strides in obtaining data more quickly and efficiently, and the Affordable Care Act will further those efforts.

In addition to claims data, access to records and other information is of critical importance to our mission. Pursuant to Section 6402 of the ACA, OIG may, for purposes of protecting Medicare and Medicaid integrity, obtain information from additional entities—such as providers, contractors, subcontractors, grant recipients, and suppliers—directly or indirectly involved in the provision of medical items or services payable by any federal program. This expanded authority will enable OIG to enhance our oversight of the Medicare and Medicaid programs. For example, OIG audits of part D payments can now follow the documentation supporting claims all the way back to the prescribing physicians.

Ensuring the integrity of information is also crucial, and the Affordable Care Act provides new accountability measures toward this end. For example, Section 6402 provides OIG with the authority to exclude from the federal health care programs entities that provide false information on any application to enroll or participate in a federal health care program. The ACA also provides new civil monetary penalties for making false statements on enrollment applications, knowingly failing to repay an overpayment, and failing to grant timely access to OIG for investigations, audits, or evaluations.

OIG'S HEALTH CARE INTEGRITY STRATEGY AND RECOMMENDATIONS

In addition to promoting data access and integrity, health care reform includes numerous program integrity provisions that

support an effective health care integrity strategy. Consistent with the OIG's five-principle strategy, these include authorities and requirements to strengthen provider enrollment standards; promote compliance with program requirements; enhance program oversight, including requiring greater reporting and transparency; and strengthen the government's response to health care fraud and abuse.

Section 6401 of ACA requires the secretary to establish procedures for screening providers and suppliers participating in Medicare, Medicaid, and the Children's Health Insurance Program. The secretary is to determine the level of screening according to the risk of fraud, waste, and abuse with respect to each category of provider or supplier. At a minimum, providers and suppliers will be subject to licensure checks. The ACA also authorizes the secretary to impose additional screening measures based on risk, including fingerprinting, criminal background checks, multi-state database inquiries, and random or unannounced site visits. These provisions address significant vulnerabilities that OIG has identified in Medicare's enrollment standards and screening of providers, and are consistent with recommendations that we have made to prevent unscrupulous providers and suppliers from participating in Medicare.

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 prevent, detect, and respond to health care fraud, waste, and abuse. OIG dedicates significant resources to promoting the adoption of compliance programs and encouraging health care providers to incorporate integrity safeguards into their organizations as an essential component of a comprehensive antifraud strategy. For example, starting

later this year, OIG will conduct compliance training programs for providers, compliance professionals, and attorneys across the country. This compliance training will bring together representatives from federal and state agencies to address local provider, legal, and compliance communities. The training will focus on methods to identify fraud risk areas and compliance best practices so that providers can strengthen their own compliance efforts and more effectively identify and avoid illegal schemes that may be targeting their communities.

The Affordable Care Act authorizes the secretary to require providers and suppliers to adopt, as a condition of enrollment, compliance programs that meet a core set of requirements, to be developed in consultation with OIG. In addition, the ACA requires skilled nursing facilities and nursing facilities to implement compliance and ethics programs, also in consultation with OIG. These new requirements are consistent with OIG's longstanding view that well-designed compliance programs can be an effective tool for promoting compliance and preventing fraud and abuse. These provisions are also consistent with recent developments in states that have made compliance programs mandatory for Medicaid providers.

Consistent with OIG recommendations, the ACA also facilitates and strengthens program oversight by increasing transparency and reporting requirements. The new transparency requirements will shine light on financial relationships and potential conflicts of interest between health care companies and the physicians who prescribe their products and services. Specifically, Section 6002 requires all U.S. manufacturers of drug, device, biologics, and medical supplies covered under Medicare, Medicaid, or CHIP to report informa-

tion related to payments and other transfers of value to physicians and teaching hospitals. This information will be made available on a public website. The types of payments subject to disclosure have been the source of conflicts of interest and, in some cases, part of illegal kickback schemes in many of OIG's enforcement cases. OIG already includes similar disclosure requirements in our corporate integrity agreements with pharmaceutical manufacturers as part of the settlement of these cases. The requirement of public disclosure of these payments will help the government, as well as the health care industry and the public, to monitor relationships and should have a sentinel effect to deter kickbacks and other inappropriate payment relationships.

The quality of care in nursing homes also may improve with the increased transparency required by the Affordable Care Act. Section 6101 requires nursing facilities and skilled nursing facilities to report ownership and control relationships. Disclosure of these relationships is critical to facilitating better oversight of and responding to quality of care and other issues. Historically, law enforcement has struggled to determine responsibility within an organization's management structure. We have had to resort to resource intensive and time consuming investigative and auditing techniques to determine the roles and responsibilities of various management companies that are affiliated with a single nursing facility. Establishing accountability is challenging in part because corporations sometimes intentionally construct byzantine structures that obscure responsible parties from view. OIG has seen a variety of methods used to conceal true ownership, including establishing shell corporations, creating limited liability companies to manage operations of individual homes, creating

LLCs for real estate holdings, and creating affiliated corporations to lease and sublease among the various inter-owned corporations. The new requirements for disclosure of ownership and control interests will help ensure that corporate owners and investment companies that own nursing homes will no longer be able to provide substandard care, deny responsibility, and leave underfunded shell companies to take the blame.

Additional transparency provisions in the ACA will shine light on the administration of the Medicare and Medicaid programs. Section 6402 will require Medicare and Medicaid program integrity contractors to provide performance statistics, including the number and amount of overpayments recovered, number of fraud referrals, and the return on investment of such activities, to the inspector general and the secretary. This latter requirement is consistent with OIG's call for greater accountability in the performance and oversight of CMS' program integrity contractors.

In addition to strengthening the government's ability to detect fraud and abuse, the Affordable Care Act strengthens the government's ability to respond rapidly to health care fraud and hold perpetrators accountable. For example, it expressly authorizes the secretary, in consultation with OIG, to suspend payments to providers based on credible evidence of fraud. Significantly, the ACA also increases criminal penalties under the Federal Sentencing Guidelines for federal health care offenses and expands the types of conduct constituting federal health care fraud offenses under title 18 of the United States Code. Put simply, criminals who commit health care fraud are going to be cut off from the Medicare trust funds faster, serve longer prison terms, and face larger criminal fines.

Each of these integrity provi-

sions advances the fight against fraud, waste, and abuse. Further, we expect that the combined impacts of these new program integrity measures will be greater than the sum of the parts. Preventing unscrupulous providers and suppliers from gaining access to the health care programs and beneficiaries is the first step in an integrated integrity strategy. Requiring compliance programs and providing guidance helps to ensure that those permitted to participate in the programs do not run afoul of the law or program requirements. Expanded oversight and reporting requirements will help the government, industry, and the public monitor the programs and identify potential fraud, waste, and abuse more quickly and effectively. In combination, the ACA's new enforcement authorities and tools will help change the calculus undertaken by criminals when deciding whether to target Medicare and Medicaid by increasing the risk of prompt detection and the certainty of punishment.

FUNDING OF THE HEALTH CARE FRAUD AND ABUSE CONTROL PROGRAM

In addition to providing new authorities and enforcement tools, the Affordable Care Act provides critical new funding that will enable OIG to expand and strengthen current enforcement and oversight efforts to combat fraud, waste, and abuse.

The HCFAC program is a comprehensive effort, under the joint direction of the attorney general and the secretary of HHS, acting through OIG, designed to coordinate federal, state and local law enforcement activities with respect to health care fraud and abuse. The HCFAC program provides OIG's primary funding stream to finance anti-fraud activities such as:

- Support of Criminal and Civil False

Claims Act investigations and enforcement;

- Support of administrative enforcement activities;
- Evaluations of Medicare contractor operations;
- Medicare and Medicaid reimbursement for prescription drugs, and other issues;
- Audits of payments to hospitals, home health agencies, Medicare advantage plans, and Medicare part D plans;
- Expansion of our use of technology and innovative data analysis to enhance our oversight and enforcement activities;
- Monitoring of providers under corporate integrity agreements;
- Issuance of advisory opinions and other guidance to the health care industry; and
- Establishment of Medicare Fraud Strike Force teams.¹

From its inception in 1997 through 2009, HCFAC program activities have returned more than \$15.6 billion to the federal government through audit and investigative recoveries, with a return on investment of more than \$4 for every \$1 invested in OIG, DOJ, and FBI investigations, enforcement, and audits.² HCFAC-funded activities have a further sentinel effect, which is not captured in this ROI calculation. HCFAC-funded activities are a sound investment, and HHS and DOJ are receiving vital new HCFAC funding—\$10 million per year for 10 years in fiscal years 2011–2020 in ACA, and an additional \$250 million is spread across FY 2011–2016 in the Health Care and Education Reconciliation Act of 2010. With our share of this

critical new funding, OIG will expand our Medicare and Medicaid investigations, audits, evaluations, enforcement, and compliance activities to support our health care program integrity efforts.

NEW HEALTH CARE DELIVERY MODELS

Experience has taught us that how health care programs pay for services dictates how the programs are defrauded. For example, when Medicare pays on a fee-for-service basis, the incentive is to bill for excessive, unnecessary services. When the program pays on a capitated basis, the incentives are reversed; unethical providers stint on needed care. Health care reform legislation contains numerous provisions that encourage the evolution of delivery and payment models to improve quality and enhance efficiencies through greater integration, collaboration, and coordination among providers. These models include, for example, accountable care organizations, medical homes, gainsharing, and bundled payment systems. These new payment and delivery models will require a fresh examination of fraud and abuse risks.

As these new models develop in the health care market, the existing fraud and abuse laws will remain important fraud-fighting tools. However, some new arrangements may require new approaches to combating fraud, waste, and abuse. Moreover, depending on their design and operation, some new arrangements may pose different risks that will need to be addressed. These risks could include, for example, stinting on care, discrimination against sicker patients, misreporting quality and performance data, and gaming of payment windows to “double bill” for otherwise bundled services. Further, industry stakeholders have raised concerns that existing fraud and abuse laws designed to restrain the

1) Medicare Fraud Strike Forces are a joint OIG-DOJ initiative used to fight concentrations of Medicare fraud in specific geographic “hot spots.” Strike Force teams include special agents from OIG and FBI, DOJ prosecutors, and oftentimes state and local law enforcement officials.

2) The \$4 to \$1 return on investment is a 3-year rolling average from 2006–2008, which is used to help account for the natural fluctuation in returns from investigative, enforcement, and audit activities.

influence of money on medical decision-making may complicate or impede certain reforms, because the fraud and abuse laws generally restrict economic ties between parties in a position to generate federal health care program business for each other.

INNOVATIVE USE OF DATA

Health care fraud schemes have become more sophisticated and better able to morph quickly in response to anti-fraud initiatives. Innovative uses of information technology have dramatically enhanced OIG's ability to respond to this challenge. For example, OIG is capitalizing on technology to process and review voluminous electronic evidence obtained during our health care fraud investigations. Using Web-based investigative software, OIG analyzes large quantities of email or other electronic documents more efficiently and identifies associations among emails contained in multiple accounts based on content and metadata. This technology is enabling investigators to complete in a matter of days analysis that used to take months with traditional investigative tools. Recently, OIG expanded the impact of this cutting-edge technology by making it available to our law enforcement partners for use in joint investigations.

Efficient and effective analysis of claims data to detect fraud indicators also is shaping how we deploy our law enforcement resources. OIG is using data to take a more proactive approach to identifying suspected fraud. In 2009, OIG organized the multi-disciplined, multi-agency Advanced Data Intelligence and Analytics Team (data team) to support the work of the Health Care Fraud Enforcement and Prevention Action Team. The data team, composed of experienced OIG special agents, statisticians, programmers, and auditors and DOJ analysts, combines sophisticated

data analysis with criminal intelligence gathered from special agents in the field to more quickly identify health care fraud schemes, trends, and geographic "hot spots." For example, the data team has identified locations where billing for certain services is more than 10 times the national average. The data team's analyses inform the deployment of Strike Force resources and selection of new locations to focus and leverage government resources in the areas with concentrations of health care fraud. Medicare Fraud Strike Forces have been established in seven fraud hot spots—Miami, Los Angeles, Detroit, Houston, Brooklyn, Tampa, and Baton Rouge.

As of May 31, 2010, our strike force efforts nationwide have charged over 550 defendants, obtained over 300 convictions, resulted in the sentencing of over 250 defendants, and secured over \$260 million in court-ordered restitutions, fines, and penalties. We believe that our strike forces also have had a marked sentinel effect. Though deterrence is difficult to quantify, we have empirical evidence that our data-driven strike force model for investigating and prosecuting health care fraud has resulted in reductions in improper claims to Medicare. Claims data showed 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, a particularly hot spot for DME fraud, decreased by 63 percent to just over \$1 billion from nearly \$2.76 billion during the preceding 12 months.

OIG uses advanced data analytics and information technology in our evaluation and audit work as well as our investigative efforts. OIG program evaluators use empirical analyses to identify patterns of potential fraud and abuse and alert CMS to these findings so that it can take appropriate fraud prevention and oversight measures. For example,

we recently analyzed all Medicare home health claims that were submitted and fully paid in 2008 to identify geographic areas that exhibited aberrant Medicare home health outlier payment patterns. Our analysis found that Miami-Dade County accounted for more home health outlier payments in 2008 than the rest of the Nation combined. We also found that 23 counties nationwide exhibited aberrant home health outlier payment patterns similar to that of Miami-Dade County, but to a lesser extent. These findings demonstrate that home health services in Miami-Dade County, as well as other counties, warrant additional review as part of ongoing antifraud activities such as HEAT.³

OIG is currently conducting an analysis of national billing patterns of pharmacies, prescribers, and beneficiaries for part D drugs in 2009. Using claims data, we will identify questionable patterns that may suggest drug diversion, billing for drugs not provided, and other types of fraud. We are conducting similar analyses for other services as well: ongoing work on outpatient therapy services and independent diagnostic testing facilities will identify high-utilization counties and providers and identify claims with unusual characteristics suggestive of fraud.

OIG is also using advanced data analysis techniques to monitor whether and how criminals are adapting their fraud schemes in response to the government's program integrity efforts. For example, in the coming months, we will issue a report analyzing how utilization of two specific inhalation drugs may have changed in the wake of Medicare program integrity efforts targeting one, but not the other, of the two drugs. We are also using a combination of claims

3) *Aberrant Medicare Home Health Outlier Payment Patterns in Miami-Dade County and Other Geographic Areas in 2008* (issued December 2009), available at <http://oig.hhs.gov/oei/reports/oei-04-08-00570.pdf>.

and sales data to determine whether the amount of the drug in question billed by South Florida suppliers and paid for by Medicare exceeded the total amount of the drug distributed for sale in the area. By using innovative data analysis to detect unusual patterns, OIG is able to target high-risk services and geographic regions and make recommendations to address systemic vulnerabilities.

To perform timely and independent audits and evaluations of the Medicare and Medicaid programs, OIG has established a data warehouse. By bringing data from CMS into OIG's servers, the data warehouse improves expediency by providing OIG staff with direct access to program data (rather than having to request data from CMS on a case-by-case basis), integrates claims data by type of service (e.g. inpatient, physician/supplier, prescription drugs) for cross-service data analysis, and facilitates OIG's use of sophisticated data analysis tools. In addition to claims data, we also obtain reference data (e.g., provider demographics, cost reports, beneficiary/recipient eligibility data, Drug Enforcement Administration active and retired registrants, SSA Master Death file, and other health care-related resources). Having more robust data and information enhances our ability to detect fraud and abuse.

Despite having these essential tools in OIG's anti-fraud arsenal, we are acutely aware of the increasing sophistication of the criminals who are intent on exploiting the health care system. We are committed to enhancing existing data analysis and mining capabilities and employing advanced techniques, such as predictive analytics and social network analysis, to counter new and existing fraud schemes. As part of that commitment, we are developing a consolidated data access center, which will integrate

business intelligence tools and data analytics into our fraud detection efforts. It will also provide the opportunity to access, analyze, and share data—consistent with applicable privacy, security, and disclosure requirements—with our law enforcement partners. Such a centralized data access center will enhance the efficiency and coordination of our collective efforts by giving law enforcement agents an opportunity to put the pieces together and see the totality of the fraud scheme.

Through this data enhanced collaboration, law enforcement will be able to increase the numbers of credible investigative leads, recoveries, and avoidances of improper Medicare and Medicaid payments and detect emerging fraud and abuse schemes and trends. In addition, these tools will support our effective targeting of audits and evaluations to identify program vulnerabilities and recommend systemic solutions.

CONCLUSION

Health care fraud, waste, and abuse cost taxpayers billions of dollars every year and require focused attention and commitment to solutions. The Affordable Care Act provides additional authorities and resources that will significantly enhance our effectiveness in fighting health care waste, fraud, and abuse. Through the dedicated efforts of OIG professionals and our collaboration with HHS and DOJ partners, we have achieved substantial results in the form of recoveries of stolen and misspent funds, enforcement actions taken against fraud perpetrators, improved methods of detecting fraud and abuse, and recommendations to remedy program vulnerabilities. Thank you for your support of this mission. I would be happy to answer any questions that the committee may have. ☞



Lewis Morris

Lewis Morris is the chief counsel in the Office of Inspector General, U.S. Department of Health and Human Services. As part of the OIG's effort to promote compliance with program requirements, Mr. Morris oversees the issuance of the compliance program guidances, advisory opinions, and other assistance to the health care industry.

Prior to serving as the chief counsel and during a 25-year career in the OIG, Mr. Morris has been the assistant inspector general for Legal Affairs, the inspector general's special prosecutor, the deputy general counsel, and a trial attorney. He also has served as a special assistant U.S. attorney for the Middle District of Florida, the Eastern District of Pennsylvania, and the District of Columbia. Mr. Morris is the recipient of the Thomas D. Morris Leadership Award, the Hubert H. Humphrey Award for Service to America, and the Attorney General's Award for Distinguished Service in recognition of his contributions to the fight against health care fraud. He is on the board of directors of the American Health Lawyers Association.

OVERSIGHT OF U.S. CIVILIAN ASSISTANCE FOR AFGHANISTAN

Congressional testimony before the U.S. House of Representatives, Committee on Appropriations Subcommittee on State, Foreign Operations, and Related Programs

BY INSPECTOR GENERAL DONALD GAMBATESA

July 15, 2010 - Madam Chairwoman Lowey, Ranking Member Granger, and distinguished members of the subcommittee, thank you for inviting me here today to testify on fraud and corruption in Afghanistan. I know you are concerned about recent media reports describing allegations of corruption among Afghan officials, funds being diverted to the Taliban, and large amounts of currency being exported from Afghanistan. The subcommittee understandably wants assurances that U.S. foreign assistance funding is being protected from fraud, waste, and abuse. I would be happy to share our views with the subcommittee on these important issues.

INTRODUCTION

Afghanistan's reputation for corruption and fraud is well known. A January 2010 report from the United Nations states that it is almost impossible to obtain a public service in Afghanistan without paying a bribe. The country's ranking in Transparency International's Corruption Perceptions Index has continued to drop dramatically since 2005. The latest report for 2009 ranks Afghanistan at 179 out of 180 countries—the second worst in the world. Furthermore, the environment is extraordinarily dangerous. Since 2002, approximately 400 people, mostly



Afghan nationals working on USAID projects, have been killed and approximately 500 injured and disabled in attacks.

The U.S. Agency for International Development currently has over 260 U.S. civilian personnel and more than 150 foreign service nationals working in Afghanistan. These employees oversee approximately 100 ongoing grants and contracts worth over \$7 billion. Since 2002, the agency has invested more than \$9 billion in foreign assistance programs in Afghanistan.

The Office of Inspector General has provided oversight of USAID programs in Afghanistan since fiscal year 2003. Because of the unusually high risks and large commitment of foreign assistance funds in Afghanistan, we have

devoted substantial oversight to programs in that country. Since 2003, we have conducted 34 performance audits and made 128 recommendations to correct deficiencies and make program improvements. We have issued 33 financial audits, which have resulted in nearly \$100 million in sustained questioned costs. I should mention that USAID has been extremely responsive in implementing our performance audit recommendations: 80 percent have been addressed, and the agency is taking corrective actions in response to those that remain open.

We have initiated more than 70 investigations, which have resulted in recoveries and savings of approximately \$150 million; and nine administrative actions such as employee and contractor

terminations, and suspensions and debarments. In the past 2 years alone, we have referred 10 individuals to the Department of Justice for prosecution and 4 individuals to local Afghan prosecutors. During the same time period, five have been convicted on criminal charges such as bribery, major fraud, and conspiracy.

Before I discuss the specifics of some of our work and the internal controls that are in place to safeguard program funds, I should tell you that we have no evidence linking USAID assistance programs to the large quantities of U.S. dollars that are reportedly being shipped from Afghanistan. Although Afghanistan is largely a cash economy, USAID seeks to provide funds to contractors and grantees through electronic transfers and local currency.

FRAUD INVESTIGATIONS

Our criminal investigators understand USAID programs and have a great deal of experience conducting fraud investigations in Afghanistan. To leverage our resources, we work collaboratively with the Special Inspector General for Afghanistan Reconstruction, the Federal Bureau of Investigation, the International Contract Corruption Task Force, and other law enforcement agencies. We also work with local Afghan police officials and prosecutors. Our investigations focus on allegations of fraud and serious mismanagement by individuals and organizations. When the allegations involve host country nationals, we assist Afghan police and prosecutors in conducting certain investigative activities, such as surveillance of suspects, executing search warrants, and effecting arrests. These efforts have resulted in successful prosecution in Afghan courts.

For example, an ongoing investigation of a USAID contractor has resulted in the termination of 10 em-

ployees. The contractor was responsible for implementing a \$349 million local governance project intended to address causes of instability and support for the insurgency and to encourage local communities to take action in promoting their own stability and development. Employees of the contractor had approached owners of various companies bidding for subcontracts, offering to help the companies win awards in exchange for a percentage of the contracts' value. Our office has referred the case to an Afghan prosecutor, and we will recommend that the terminated employees be barred from future U.S. government awards.

“The country’s ranking in Transparency International’s Corruption Perceptions Index has continued to drop dramatically since 2005. The latest report for 2009 ranks Afghanistan at 179 out of 180 countries—the second worst in the world.”

Another recent investigation resulted in the arrest and prosecution under Afghan law of an employee working on a USAID community development project. The individual was accused of embezzling nearly \$193,000 while working as a finance coordinator on a \$229 million local governance program. He was responsible for depositing the contractor’s monthly tax payments to the Af-

ghan Ministry of Finance, but the ministry reported that it had not received the payments. Local Afghan law enforcement officials, with our investigators’ assistance, discovered that the bank deposit slips the subject had submitted to the contractor as proof of payment were not legitimate. The individual has now been charged with forgery violations under Afghan law and is in jail in Kabul awaiting trial.

Although the Afghan government has not interfered with any of our investigations, we sometimes have difficulty pursuing investigations because of concerns for the security of informants and witnesses. Individuals who provide us with information are often reluctant to continue to participate in investigations out of fear for their safety. When we cannot pursue investigations for this reason, we share relevant information with the appropriate U.S. government agencies within the Kabul Embassy.

In addition to our investigative efforts, our auditors also identify suspected fraud. A recent audit of an agricultural program in Afghanistan found widespread irregularities in the records showing distribution of seed and fertilizer, as well as in timesheets for employees in cash-for-work programs. In both cases, recipients were required to mark beneficiary rolls with their fingerprints as evidence that they had received commodities or cash under the program, but the auditors found numerous instances in which fingerprints appeared to be identical. A program subcontractor told the audit team about other cases in which program commodities had not been received by the targeted farmers and the names of allegedly nonexistent people had appeared in beneficiary rolls. Our investigators are looking into these irregularities. We will continue to conduct performance audits

of USAID programs so that we can identify other possible fraud and mismanagement. Our oversight in Afghanistan for the remainder of 2010 will include audits and reviews of programs related to economic development, roads, health and education, availability of technology, electoral support processes, and alternative development. We will also complete an ongoing review of security contracts to determine whether bribes were paid to the Taliban or other groups in exchange for protection.

CONTROL SYSTEMS

USAID has several systems in place to prevent fraud and abuse. For example, USAID conducts preaward surveys of contractors and grantees to ensure that they have the necessary accounting systems and experienced personnel to manage USAID funds responsibly.

In addition, accounting and audit provisions are in place that require annual financial audits of contracts and grants, and mandate that contractors and grantees maintain records showing how USAID funds were used. These provisions must also be included in any sub-awards.

USAID has also imposed financial reporting requirements for contractors who receive advance payments. Specialists examine the contractors' vouchers to determine acceptability of the charges before forwarding them to a certifying officer for payment.

Assistance projects are overseen by USAID employees or by third parties, who conduct site visits and review program progress reports. However, our audits have noted that the oversight is not as robust as it should be and that USAID does not have a sufficient number of qualified personnel on the ground to effectively monitor projects. In response, USAID is developing a more effective monitoring and evaluation process, to



include increasing staffing and training. Our office supplements USAID's oversight by performing financial audits, and we provide policy direction and quality control for financial audits of contractors and grantees performed by public accounting firms that we have found to be eligible to audit USAID funds. The audits focus on determining whether USAID funds have been used for agreed-upon purposes, and the auditors also provide reports on cost-sharing contributions, internal controls, and compliance with contract and grant terms and applicable laws and regulations. Auditors pay particular attention to controls over cash, since cash payments are considered to be more vulnerable to fraud and misuse.

We conduct concurrent audits of the highest-risk program areas, such as infrastructure projects, to provide early detection of potential problems. As I mentioned earlier, we also conduct performance audits that focus on whether USAID programs are achieving their intended goals.

Finally, we conduct fraud education activities to inform USAID staff, contractors, and grantees (including subcontractors and subgrantees) about

fraud indicators and to encourage them to contact OIG if they encounter any indications of fraud or misconduct. In the past 90 days alone, we have provided these briefings to more than 500 people.

OVERSIGHT CHALLENGES

Oversight in Afghanistan is complicated by a multitude of factors: security concerns, language limitations, cultural differences, and lack of jurisdiction over certain funds.

As part of the U.S. government's commitment to the Paris Declaration principles, USAID is channeling increasing levels of development funding directly to the government of Afghanistan. By leading the resulting development projects, the Afghanistan government can shape more development activities, promote project sustainability, and build public confidence in the government's ability to deliver programs that improve the welfare of the people. However, Afghanistan is still developing the capacity to manage projects and monitor and account for associated resources. This places federal dollars at greater risk of waste, fraud, and abuse. USAID must develop an approach to building Afghan-

istan's capacity that balances the imperative for local engagement in the development process with effective stewardship of taxpayer dollars.

The effective stewardship of taxpayer dollars is also critical for budget support provided to the Afghan government through trust funds or other instruments managed by international organizations. USAID/OIG does not have audit rights to these funds. Therefore, oversight of these funds becomes the responsibility of the implementing entity.

MOVING FORWARD

Considering the reported problems of corruption and the lack of capacity in Afghan institutions for safeguarding resources, we believe that USAID funding is at significant risk of waste, fraud, and abuse. Several steps could be considered to minimize these risks:

- Require that direct assistance to the government of Afghanistan be committed through specific projects, so that USAID funds can be traced to end uses, as opposed to being commingled with other sources of funding.

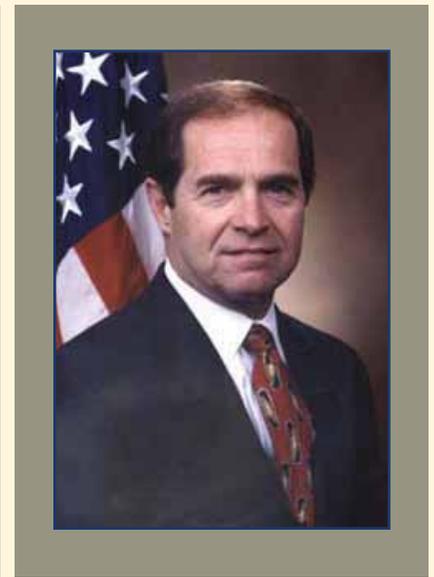


- Require concurrent audits—conducted or supervised by USAID/OIG—of USAID's direct assistance to the government of Afghanistan.
- Adopt specific contracting practices for Afghanistan and other conflict settings that limit the tiers of subcontractors and subgrantees.

In addition to the options I have mentioned, OIG can take the following actions, as resources permit, to further mitigate risk:

- Review USAID's preaward survey and certification process to determine whether further strengthening is required of the criteria for approving organizations for awards.
- Conduct a review of cash disbursement practices employed by USAID contractors and grantees.
- Increase participation with other federal agencies that are following the trail of expenditures in Afghanistan.

We appreciate the subcommittee's interest in our work. To help OIG meet its oversight challenges, we ask for favorable consideration of proposals to expand our personnel authorities that are provided in versions of H.R. 4899. These authorities would allow us to increase our oversight presence in Afghanistan by supplementing existing staff with other highly qualified and experienced personnel. We would also use these authorities to retain personnel with the language skills and cultural understanding that would enhance our audit and investigative activities. We share the subcommittee's concerns about ensuring that funding appropriated to foreign assistance programs in Afghanistan is not wasted or channeled to those who wish to do us harm, and we are making every effort to respond to associated reports and allegations. I would be happy to answer any questions you may have at this time. ☺



Donald A. Gambatesa

Donald A. Gambatesa began his tenure as inspector general at USAID on January 17, 2006, after more than 30 years of service in federal law enforcement. Mr. Gambatesa serves concurrently as the inspector general for the Millennium Challenge Corporation, the United States African Development Foundation, and the Inter-American Foundation. From 2001 to 2005, Mr. Gambatesa served as the deputy director of the United States Marshals Service, where he was responsible for judicial security and all administrative and investigative operations of that agency. Previously, he served as the special agent in charge of the Special Investigations Division in the Office of Inspector General at the USAID, and over 24 years as a special agent of the United States Secret Service.

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

Invitation to Contribute Articles to the Journal of Public Inquiry

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

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

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

By email:
JournalofPublicInquiry@dodig.mil

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

Journal
of Public Inquiry

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

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

In order to create independent and objective units--

- (1) to conduct and supervise audits and investigations relating to the programs and operations of the establishments listed in section 11(2);
- (2) to provide leadership and coordination and recommend policies for activities designed (A) to promote economy, efficiency, and effectiveness in the administration of, and (B) to prevent and detect fraud and abuse in, such programs and operations; and
- (3) to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action;