

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

The Journal of Public Inquiry



SPRING / SUMMER

2006

PRESIDENTS COUNCIL ON
INTEGRITY AND EFFICIENCY

EXECUTIVE COUNCIL ON
INTEGRITY AND EFFICIENCY

Editorial Board

Christine C. Boesz, Inspector General, National Science Foundation

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

Johnnie E. Frazier, Inspector General, Department of Commerce

Gregory H. Friedman, Inspector General, Department of Energy

J. Russell George, Treasury Inspector General for Tax Administration

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

Patrick O'Carroll, Inspector General, Social Security Administration

Barry R. Snyder, Inspector General, Federal Reserve Board

Staff

Editor-in-Chief

Thomas F. Gimble, Acting Inspector General, Department of Defense

Publisher

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

Editorial Services

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

Printing

Department of Defense Office of the Inspector General

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

Note:

The opinions expressed in *The Journal of Public Inquiry* are the author's alone. They do not represent the opinions or policies of the United States or any Department or Agency of the United States Government.

TABLE OF CONTENTS

<i>Articles</i>	Pages
<i>Defense Investigators and the War on Terrorism</i> by Louis Beyer, Inspector General, Naval Criminal Investigative Service	3-10
<i>Access to Information by Office of the Inspector General and Other Accountability Offices</i> by Glenn A. Fine, Inspector General, U.S. Department of Justice and Anne Sheppard, Evaluation Director, Office of the Inspector General, U.S. Department of Justice	11-16
<i>Convincing Contractors to Report Their Own Procurement Fraud to the Inspector General</i> by Alan S. Larsen, Esq., Counsel to the Inspector General and Eric R. Feldman, Inspector General, National Reconnaissance Office	17-22
 <i>Capstone Papers</i>	
<i>Addressing Whistleblower Protection for Employees of Department of Defense Intelligence Agencies</i> by Julie C. Kienitz, Auditor, Department of Defense Office of the Inspector General	23-26
 <i>Speeches</i>	
<i>From Internal Controls to Audit Readiness</i> by Mary L. Ugone, Deputy Inspector General for Auditing, Department of Defense Office of the Inspector General and Judy Padgett, Program Director for Quality Assurance, Department of Defense Office of the Inspector General	27-34

-Denotes the end of an article.

In This Issue . . .

Welcome to the Spring/Summer 2006 issue of *The Journal of Public Inquiry*. We are fortunate to present several noteworthy articles this season that are related to Inspector General (IG) activities. These articles cover a wide range of topics of interest to the IG community.

The lead article in this issue is *Defense Investigators and the War on Terrorism*, which was written by Louis Beyer, Inspector General, Naval Criminal Investigative Service (NCIS). Mr. Beyer makes use of his experiences in Iraq to illustrate how Defense Criminal Investigative Organizations support the Global War on Terrorism.

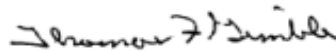
Glenn A. Fine, Inspector General, U.S. Department of Justice, and Anne Sheppard, Evaluation Director, Office of the Inspector General, U.S. Department of Justice, provide a revealing article on *Access to Information by Offices of the Inspector General and Other Accountability Organizations*.

The third article in this issue is *Convincing Contractors to Report Their Own Procurement Fraud to the Inspector General* written by Alan S. Larsen, Counsel to the Inspector General and Eric R. Feldman, Inspector General National Reconnaissance Office.

Addressing Whistleblower Protection for Employees of the Department of Defense Intelligence Agencies is a Georgetown University Executive Masters of Policy Management capstone paper written by Julie C. Kienitz, Auditor, Department of Defense, Office of the Inspector General.

Finally we present a speech titled *From Internal Controls to Audit Readiness* delivered by Mary L. Ugone, Deputy Inspector General for Auditing and Judy Padgett, Program Director for Quality Assurance and Policy both with the Department of Defense Office of the Inspector General.

We want to offer our sincere thanks to all those who contributed their expertise in writing these articles for *The Journal of Public Inquiry*.



Thomas F. Gimble
Acting Inspector General

Defense Investigators and the War on Terrorism

Louis Beyer

Inspector General, Naval Criminal Investigative Service

The Defense Criminal Investigative Organizations (DCIOs) have a long history of providing criminal investigative and counterintelligence support to the Department of Defense and our nation. Criminal investigators, who are skilled in gathering information, collecting evidence, and interviewing people, are currently in great demand in the Global War on Terrorism. This article discusses the missions being supported and some of the challenges faced. While each of the DCIOs supports the war on terrorism, this article focuses on the contributions of the Naval Criminal Investigative Service, for which the author works. In publishing this article, it is hoped that readers will gain a greater appreciation for the contributions of the DCIOs, and that the sharing of lessons learned will strengthen that support in the future.

Background

The Naval Criminal Investigative Service (NCIS) is responsible for conducting felony criminal investigations and counterintelligence activities in support of the Department of the Navy. The NCIS mission is to prevent terrorism, protect secrets, and reduce crime impacting the Navy and Marine Corps. The agency, headquartered in Washington, DC, and with over 150 offices worldwide, has just over 2,400 personnel; some 1,200 of whom are civilians credentialed as special agents. NCIS special agents are trained at the Federal Law Enforcement Center in Glynco, Georgia, as criminal

investigators. The skills possessed by these investigators - including interviewing and interrogating, processing crime scenes, developing informants, conducting protective security details, administering polygraphs and presenting cases for prosecution - have placed them in high demand as the nation responds to events in the wake of September 11, 2001. On any given day, NCIS personnel are deployed to Iraq, Afghanistan, Kuwait, Djibouti, Guantanamo Bay, Cuba, and elsewhere in support of the Global War on Terrorism.

“NCIS was assigned the task of protecting the governors in Basra and Hillah.”

NCIS personnel conduct criminal investigative, counterintelligence and counterterrorism activities around the globe on a daily basis, in close cooperation with the Navy and Marine Corps forces the agency supports. NCIS special agents deploy aboard all Navy aircraft carriers and with amphibious task forces. In overseas locations, NCIS agents work with local police and security services to identify and reduce threats to naval personnel, facilities and ships. NCIS agents routinely conduct advances before U.S. ships visit foreign ports to identify and mitigate security threats. NCIS is the primary organization within the Navy responsible for conducting personal protection operations for naval officials and visiting dignitaries. Thus, it was inevitable that NCIS and the other DCIOs would have a role in supporting military operations in Iraq.

Protective Service Operations

As the first phase of military operations in Iraq ended in June 2003 and the U.S. began stability operations, the Department of Defense turned to NCIS and its Army and Air Force counterparts to protect the provincial governors of the Coalition Provisional Authority. NCIS was assigned the task of protecting the governors in Basra and Hillah. While this mission might normally go to the Department of State's Diplomatic Security Service, the State Department presence in Iraq was limited and stabilization activities, led by the Coalition Provisional Authority, were a DoD mission. This assignment provided unique challenges for the organization. Although NCIS has a long history of conducting protective service operations, including in Italy during the height of the Red Brigade's activity and in the Philippines in the late 1980s, the environment in Iraq required changes in tactics, training and equipment. Traditional protective service operations are designed to challenge a lone or small group of attackers and to cover and extract the protectee from the area of the threat. s

Routine operations use heavily armored vehicles that are not very maneuverable or designed for use on unimproved roads. Agents are traditionally armed with easily concealable pistols and submachine guns. Movements are intended to be low key, so as not to draw undue attention.

In Iraq, NCIS details were equipped with M-4 and MP-5 submachine guns to provide greater firepower and engage adversaries at a greater distance. Initially, NCIS had no Level IV body armor in its inventory. In addition, the supply of commercially available body armor was very limited, and NCIS was competing with the military services for what was available.

The agency chose to use light armored vehicles as they provide greater maneuverability than their heavier counterparts. In addition, despite its wartime support mission, NCIS is not equipped for these contingency missions and had to redirect the few existing lightly armored vehicles it possessed or procure them rapidly.

Use of tactical military vehicles was shunned as nonmilitary vehicles allowed the details some protection since the insurgents were at the time focused on primarily attacking military convoys.



Then Secretary of the Navy Gordon England and his NCIS protective detail meeting Major General James Amos, USMC, in Al Asad, Iraq.

Prior to the Global War on Terrorism, NCIS relied primarily on existent commercial and law enforcement communication infrastructures. But the limitations of this dependency became readily apparent with the missions to Iraq. The first teams deployed to the area found the communications infrastructure broken and of limited utility.

Tactical communications consisted of vehicle-to-vehicle radios, Iridium satellite telephones, and a handwritten listing of emergency contact numbers. Complicating the situation further was the limited interoperability between military radios, and the commercially available equipment.



Meeting the initial challenges required the installation of dedicated radio repeaters in Baghdad and Hillah. These systems greatly increased the range of operational communications, and bridged the gap until more permanent solutions could be introduced.

As the missions have expanded throughout Iraq and ultimately the globe, the agency has acquired a wide array of communications devices to meet a variety of exigencies. Tactical radios, encrypted satellite telephones, multi-band radios and portable satellite terminals have significantly improved the ability to operate in deployed environments.

The new weapons, vehicles, equipment and the fact that NCIS training for protective service operations had been limited for years due to budget constraints, necessitated refresher training for teams being deployed to Iraq. NCIS teamed with the Federal Law Enforcement Training Center (FLETC) to conduct the training at the latter's center in Artesia, New Mexico. The desert environment and range facilities there proved ideal in training for operations in Iraq. This training has since been provided to Marine Corps personnel deploying to the Horn of Africa, Iraq, and Afghanistan.

The provincial governors' jobs required regular interaction with local officials, and NCIS teams traveled frequently in their assigned sectors. Two teams of 8-12 agents were deployed originally for 45 days, but this was extended as the numbers required for this and other missions multiplied.

In the end, the protective deployments were capped at 90 days because of the fatigue associated with conducting these highly stressful operations. With the transition of the Coalition Provisional Authority governance to an elected Iraqi government, the NCIS protective service mission in Iraq has largely ended.



NCIS personnel conducting high risk training operations.

Additional Missions

In addition to the personnel protection mission, NCIS personnel conducted other missions in Iraq. Special agents trained in computer crime were enlisted as part of the Iraqi Survey Group that searched the countryside for evidence of weapons of mass destruction.

NCIS cyber agents are specifically trained to seize, access and examine evidence contained on computers. They participated in raids on military bases and government facilities, allowing real-time exploitation of seized computer media. NCIS polygraphers have also been playing a significant role in the current war. Polygraphs were used prior to the war to vet Iraqi nationals willing to support U.S. military operations. Since the outbreak of hostilities, NCIS polygraphers have deployed to Iraq and Afghanistan to aid in the interrogation of detainees.

The polygraph has proven to be an effective tool in eliciting information. Faced with a shortage of personnel trained as polygraphers, and the fact that the initial polygraph training cycle lasts 1 year, NCIS has used special authorities to rehire retired polygraphers to meet its deployment requirements.



NCIS special agent collecting evidence at an insurgent bomb-making site in Baghdad.

Moreover, NCIS personnel have deployed to Iraq as part of the Strategic Counterintelligence Directorate (SCID).

The SCID incorporates NCIS, Air Force Office of Special Investigations, Army Intelligence and Security Command, and DoD Counterintelligence Field Activity personnel and operates in Baghdad, Irbil, Hillah, and Basra to counter foreign intelligence and terrorist activities. SCID personnel recruit informants, investigate terrorist attacks, process evidence from raids, and interrogate detainees.

SCID activities have resulted in the prevention of terrorist attacks, seizure of weapons caches, and the identification and arrest of insurgents. NCIS and other SCID personnel frequently operate with the Iraqi court system to support the prosecution of insurgents.

NCIS personnel are also in Iraq to provide felony criminal investigative support to the Marine Corps, which has a major presence in western Iraq. NCIS agents address the gamut of investigative requirements, from deaths due to improvised explosive devices, larceny of weapons and equipment, crimes against persons, and economic crime. NCIS investigations support the commander in maintaining good order and discipline among U.S. personnel and conserving the resources necessary for the war.

As was true in the case of personnel involved in protective service operations, NCIS recognized the need to better train its other deploying personnel to operate in a combat zone. While NCIS special agents accompanied naval forces during the Vietnam war, it is unusual for NCIS personnel to be deployed in support of a long-term land campaign without a clearly defined secure rear area.

In Iraq and Afghanistan it is not uncommon for agents to deploy via helicopter or convoy to the most remote areas to examine crime scenes, exhume bodies and collect evidence. NCIS once again teamed with FLETC to conduct a four week High Risk Operations Training Course. The course includes achieving proficiency in the firing of the M-4 and MP-5, small unit tactics to defend against insurgent attacks, counter-ambush driving, and combat first aid. Instruction is also provided in the Laws of War, including the proper handling of detainees, terrorist tactics and improvised explosive devices, and conducting investigations and collection activities in a combat environment. Students are required to conduct daily physical exercises and pass a physically challenging attack scenario in order to graduate and deploy.

The High Risk Operations Training Course has been well received by NCIS students and those from other agencies. FLETC, which is building a counterterrorism training facility on its Glynco facility, has used the course and the



lessons learned from NCIS deployments to develop new training scenarios and improve its facilities to better simulate the challenges of these missions.

Managing the logistic tail to these deployments also required innovation. The NCIS Middle East Field Office, located at Naval Support Activity Bahrain, developed a deployable office in an air-conditioned CONEX box to support temporary NCIS offices positioned forward in Kuwait and Iraq. The office in Kuwait became the entry and exit points for NCIS personnel deploying to Iraq. Here NCIS deployers were equipped with vehicles, firearms and body armor. Villas were rented to house personnel on temporary duty as a cheaper and more secure alternative to staying in hotels. Tachyon satellite communication systems were used for the first time to provide unclassified and classified computer connectivity back to the supporting field office in Bahrain.

Most recently, Ms. Dawn Sorenson, the NCIS Forensic Sciences Division Chief, deployed to Iraq to improve the ability of U.S. Marine forces to gather forensic evidence for more rapid exploitation. Ms. Sorenson and NCIS agents instructed the Marines on collecting fingerprints and other biometric data. She established a forward-positioned tactical forensic latent print laboratory to reduce the time required to analyze the collected material from weeks to hours. Military teams are finding that having the forensic results available during tactical interrogations provides them an additional tool that helps them corroborate other intelligence and often to elicit truthful responses from detainees.

Over 400 NCIS personnel have been trained for deployment to Iraq, Afghanistan, Kuwait, and the Horn of Africa in the last 3 years. Some personnel have deployed more than once; in some cases as many as three occasions. DoD regulations require that only emergency essential civilian employees deploy to combat areas and that those personnel should be volunteers if at all possible. NCIS recognized early on that sustaining the deployments would be a challenge as time went on. As a result, deployments have been lengthened from 60 to 120 days, with some managerial assignments lasting 180 days. NCIS developed a deployment avail-

ability roster (DAR) process, whereby all employees are requested to indicate their preference for missions planned for the next 4 to 6 months.

The DAR process allows employees to plan ahead several months and has

been able to fill all missions with volunteers. Augmenting the NCIS special agents have been naval reservists with law enforcement and intelligence backgrounds. Civilian personnel deploying to Iraq receive hazardous duty, post differential, and overtime pay. In addition to predeployment training, all NCIS personnel are debriefed upon mission completion by program managers and trainers to identify and rapidly implement lessons learned.

Returning personnel are also debriefed by NCIS staff psychologists to identify health issues and are granted administrative leave to complete the decompression and reacclimation processes. The NCIS Director or his senior staff officiates at periodic awards ceremonies where employees are recognized with a newly created NCIS deployment medal. These award

“Over 400 NCIS personnel have been trained for deployment to Iraq, Afghanistan, Kuwait, and the Horn of Africa in the last 3 years.”

ceremonies are frequently attended by Navy and Marine Corps flag or general officers and receive local media coverage.

Recognizing the long-term outlook for the GWOT and the impact of these deployments on NCIS operations, NCIS created a Contingency Response Field Office (CRFO) at Glynco, Georgia. The CRFO's mission is to train and deploy personnel for contingency missions such as those in Iraq and Afghanistan. The CRFO began to provide personnel for deployments to Iraq in 2005.

Conclusion

The Global War on Terrorism has provided unique opportunities for Department of Defense criminal investigators to support the war effort around the globe. Deployments into Iraq and Afghanistan have been particularly challenging, necessitating changes in tactics, training, logistics and human resource processes.

Returning NCIS personnel are overwhelmingly positive about their deployment experiences. As federal law enforcement personnel, they have sworn to protect and serve others. During these deployments, DCIO personnel protect Iraqi civilians and U.S. military personnel and save lives on a daily basis.~

A Typical Homicide Investigation in Iraq

Special Agent Jennifer VanOoteghem was the case agent for a murder investigation in which a United States Marine Corps (USMC) Lieutenant was accused of killing two innocent Iraqi civilians without provocation.

As part of this investigation, which received intense worldwide media attention, Ms. VanOoteghem sought to obtain exhumation orders for the two Iraqi civilians who were killed. First, however, she had to locate the bodies. Without the benefit of an address system, Ms. VanOoteghem had to rely heavily on searching for landmarks and interviewing Iraqi citizens.

Her efforts to locate the bodies required her to travel via a heavily armed military convoy to the extremely dangerous and remote village of Al Mahmudiyah, Iraq, and a nearby primitive U.S. Army outpost, on several separate occasions. The outpost was under constant threat of mortar and rocket attacks by Iraqi insurgents.

On her first trip out to the crime scene, the convoy had to get off the highway and onto the frontage road where the incident occurred. When they left the highway, the convoy went down the entrance ramp the wrong way (the way they do in Iraq) and went a mile down to take some crime scene photographs.

Less than five minutes later, a different convoy came down the same highway and was hit by an improvised explosive device (IED). Apparently the IED was set up for the first convoy's return to the highway after they had passed through that area. The other convoy traveled the exact

path as Ms. VanOoteghem's, but hers made it through safely.

Ms. VanOoteghem traveled with copies of the Iraqi death certificates, photographs of the deceased Iraqis and an interpreter until bodies and families of the deceased men were located. On one of the trips to locate the grave sites, Ms. VanOoteghem's military convoy was forced to travel on alternate routes after several IEDs were discovered at the entrances and exits of the cemetery.

An Iraqi judge decided that, prior to issuing an order for the exhumation of the bodies, the families' consent to the exhumation would be required. The Iraqi burial rituals are very sacred, and their religion does not condone either autopsies or exhumations.

Ms. VanOoteghem visited the families to explain who she was and that she was investigating the death of their loved ones. She was very honest with them about the investigation and spent a great deal of time with them (five trips total), answering all of their questions and explaining what she was trying to do.

On each trip to visit the families, the Army Unit Ms. VanOoteghem worked and traveled with provided health care to sick children in the places they visited, and brought candy, snacks, clothes and toys to help ensure the families that their visits were with good intentions. When Ms. VanOoteghem explained to the families what U.S. forensic science could do, they were amazed. She told them that, unless they could determine for certain what had happened, that their loved one's name could be tainted as a terrorist.

As a result of her compassion and communication skills, both families provided consent for the exhumations, autopsies and transportation of the bodies to the Armed Forces Institute of Pathology in Dover, Delaware. One of the Fathers told her that he trusted her and to "please treat the remains of my son like they were your own brother."

Ms. VanOoteghem obtained the exhumation order from the Interim Iraqi Government, the first such order issued by the interim government. The bodies were then shipped to Delaware, where the autopsies were conducted.

The results of the autopsies corroborated the USMC Lieutenant's assertion that he shot the victims in self-defense, and all charges against him were dismissed. After the autopsies had been completed, Ms. VanOoteghem escorted

the bodies back to Iraq and, with her team, reburied the remains.

Then she visited the families to thank the families again, notify them of the reburials and advise them of the results of the autopsies. Even after Ms. VanOoteghem explained that the charges against the Marine lieutenant had been dismissed and that he would not be tried in the death of their loved ones, one of the fathers told her that he thought of her "as his daughter," and he prayed that God would send great blessings to her.

Both families also thanked her for her for all of her efforts and said that, although they were surprised at the findings, that they were satisfied that she had discovered the truth.



About the Author

Louis Beyer



Louis J. Beyer received a bachelor's degree in electrical engineering and was commissioned an ensign in the U.S. Navy upon his graduation from the U.S. Naval Academy in 1979.

Mr. Beyer served on active duty with the United States Navy from 1979 to 1988 as both a surface warfare officer and an intelligence officer. His first operational assignment was with the tank landing ship USS Bristol County (LST-1198) as the Damage Control Assistant and Gunnery Officer.

He attended the Defense Intelligence College and earned his Master of Science in strategic intelligence in 1983. Mr. Beyer served as a collection operations officer from 1983 to 1985. During this time, he provided support to U.S. military operations in Lebanon and Grenada, participated in wartime contingency planning and exercises, and conducted evaluations of U.S. intelligence collection programs.

Mr. Beyer joined the Naval Criminal Investigative Service in June 1985 and served as a terrorism analyst and the

operations officer in the Navy's Antiterrorist Alert Center. After separating from active duty, Mr. Beyer returned in 1989 as the deputy chief and, subsequently, chief of the Antiterrorist Alert Center. His accomplishments included executing the Navy's response to the terrorist threat during the Persian Gulf War.

From 1992 to 2004, Mr. Beyer served as Assistant Director for Administration, Assistant Director for Financial Management, special assistant on the NCIS Strategic Planning Group, program manager and special assistant within the NCIS counterintelligence Directorate in the areas of systems/technology protection, counterintelligence analysis and production, and resource management. He assumed his current duties in August 2004.

About the NCIS



In support of its mission - to prevent and solve crimes that threaten the warfighting capability of the U.S. Navy and Marine Corps - NCIS pursues three strategic priorities: Prevent Terrorism, Protect Secrets, and Reduce Crime.

NCIS is the primary law enforcement and counterintelligence arm of the United States Department of the Navy. It works closely with other local, state, federal, and foreign agencies to counter and investigate the most serious crimes: terrorism, espionage, computer intrusion, homicide, rape, child abuse, arson, procurement fraud, and more.

Access to Information by Offices of the Inspector General and Other Accountability Organizations

Glenn A. Fine

Inspector General, U.S. Department of Justice

and

Anne Sheppard

Evaluation Director, Office of the Inspector General, U.S. Department of Justice

Inspectors General and other government oversight organizations play a critical role in ensuring accountability of government agencies by evaluating, investigating, and auditing their operations. At all levels - federal, state, and local - accountability organizations help improve the effectiveness and efficiency of government, as well as detect and deter waste, fraud, and abuse.

But to do our jobs effectively, we need timely and full access to information from government agencies. If full information is withheld, or if we are continually battling for access to such information, our effectiveness is diminished. Under the Inspector General Act of 1978, federal

Inspectors General are granted full access to their agencies' documents and information. Similarly, many state and local accountability organizations work under laws mandating that they receive access to government information. Yet, despite such legal requirements, government agencies can make it difficult to obtain the timely and complete information that is needed for vigorous oversight.

To provide information to the accountability community about the types and extent of any

access to information problems, the Government Accountability Office (GAO) Domestic Working Group and the Department of Justice Office of the Inspector General (OIG) conducted a nationwide survey of federal, state, and local accountability organizations. The survey asked these organizations about access to information issues they had encountered during audits, inspections, and investigations. Most important, we asked for examples of the most successful strategies they used to overcome any access to information problems.


“Under the Inspector General Act of 1978, federal Inspectors General are granted full access to their agencies' documents and information.”

organizations said they experienced delays in the receipt of information, which also can significantly hamper the effectiveness of their oversight work.

The Survey

The GAO's Domestic Working Group is an informal group, organized by the Comptroller General of the United States, consisting of the Comptroller General, five federal Inspectors General, seven state auditors, and six local

This article summarizes the results of the survey. In general, we found that most survey respondents did not experience significant access problems in terms of denial of information. However, many



auditors from across the country. The Domestic Working Group meets annually to discuss matters of interest to accountability organizations.

Under the auspices of the Domestic Working Group, the Department of Justice OIG developed a survey that was sent to 355 accountability organizations throughout the country:

- GAO
- 59 federal Inspectors General
- 64 state audit organizations
- 231 county and city audit organizations

The survey population was compiled from membership lists maintained by the President's Council on Integrity and Efficiency; the National Association of State Auditors, Comptrollers and Treasurers; and the National Association of Local Government Auditors.

The survey was organized by financial audits, performance audits, evaluations and inspections, and investigations. It requested information about the organizations' legal authority for obtaining information, trends in any access problems, the main factors that affected access to information, and successful strategies for resolving access problems. The survey contained 47 questions, which included a mix of multiple choice and open-ended questions that requested narrative responses.

We received 128 responses to the survey request (a response rate of 36 percent). Federal OIGs provided the highest response rate (67 percent), followed by state audit organizations (34 percent), and local audit organizations (29 percent). Because of the response rate, we could not statistically project the survey results to the full survey population of 355 account-

ability organizations. However, we believe the responses provide insights on the current state of accountability organizations' access to information, along with the most common strategies used to overcome any problems.

Survey Results

The survey found that most respondents do not have significant access problems and are successful in obtaining the information they need. The survey responses indicated that it is rare for an accountability organization to be denied access to records or government employees. Rather, we found that the greater problem is delay in obtaining such access.

These findings were similar across all levels of government. They also were similar by the type of review seeking the information (financial audit, performance audit, evaluation and inspection, and investigation). In total, two-thirds of the respondents were "very satisfied" or "generally satisfied" with the current state of their ability to obtain access to records and people. Similarly, two-thirds of the respondents "never" or "rarely" face denials of access to records or people. Almost all of the respondents were satisfied with their legal authority for access to information. We found that the trend in access to information has been stable. Three-quarters of the respondents reported no change in their ability to access information over time during the last three years.

Yet, despite their general satisfaction with access to information, many respondents reported delays in obtaining access to records and people. More than three-quarters of survey respondents said they face delays in obtaining access to records, and almost two-thirds of respondents said they face delays in obtaining access to specific people.



Successful Strategies for Overcoming Access Problems

With few exceptions, most survey respondents said they resolved any access problems through a variety of strategies. The survey respondents provided various examples of successful strategies.

The reasons for the delays varied. Common factors for the access problems cited by the respondents included:

1. The government agency said it had too much work or insufficient personnel to satisfy the requests for information;
2. The government agency had privacy or confidentiality concerns about the requests for information;
3. The government agency had concerns about the security and safekeeping of the information;
4. The government agency was concerned about public issuance of the information in the final report;
5. The government agency did not understand the importance of the request;
6. The government agency thought the request was outside the scope of the review;
7. The government agency thought that providing the information would result in negative findings; and
8. The government agency could not provide the requested information because of incompatible data systems.

1. *Obtaining the support of management in providing access to information.* The support of top agency management in providing access to information is critical. If agency employees know that their top management supports the role of the accountability organization, and that management demands timely and full cooperation with the accountability organization, then obtaining access to information will be much smoother, fuller, and timelier. The expectation of cooperation and acknowledgement of the importance of the work of the accountability organization filters down from the top of the organization to employees who work with the accountability organization on a daily basis.

During my tenure as the Inspector General in the Department of Justice (DOJ), I have been fortunate to work with three Attorneys General (Janet Reno, John Ashcroft, and Alberto Gonzales) who have recognized the important role the OIG plays in the Department. They have understood and supported our need for access to information, including extremely sensitive DOJ information. The same is true of Robert Mueller, the Director of the Federal Bureau of Investigation (FBI). FBI employees know that he recognizes the importance of the OIG's oversight role, and they know that, in accordance with our statutory authority, they must provide us full access to FBI information. Without this support from Department leaders, our ability to obtain the information we need to perform our oversight role would be compromised.

2. *Communicating frequently with the government agency to explain your missions, authority, and information requirements.* Over time, protocols are developed to describe the way the accountability organizations operate and handle information from the government agency. However, it is important to communicate frequently with the government agency about the accountability organization's protocols, legal authorities, and requirements for timely access.

In the DOJ, we often find that new employees or new agency audit liaisons are not familiar with our processes and requirements, and it is critical that we constantly communicate and educate agency employees about the role and responsibilities of the OIG. This is especially true in organizations that experience significant turnover in management positions.

For example, in the FBI we regularly interact with new managers who do not have past experience with OIG reviews. We cannot take for granted that

because prior FBI reviews worked smoothly, the new reviews will progress in the same manner. Coordination and communication with the agency require constant attention. Consequently, OIG supervisors meet regularly with agency liaisons to reinforce our procedures and requirements and to discuss any issues with our access to information and the agencies' ability to respond timely to data requests. In this vein, survey respondents stated that their continual contact with agencies has improved working relationships and access to information.

3. *Addressing issues early in the review process to avoid access issues.* Equally important to avoiding problems is addressing access issues early in the review. The entrance conference is important for raising issues and establishing expectations about the agency's response to requests for information. Some survey respondents said they presented detailed information requests at the entrance conference and took time to discuss each requested item to ensure the agency understood what was needed. Other respondents stated that they hand-delivered engagement letters to ensure they were received timely by the appropriate agency personnel. Others said they made sure that the

engagement letters included a clear explanation of the review's objectives. Some respondents required all agency department heads involved in the review to attend the entrance conference. Others indicated that involving agency managers at the initiation of a review has reduced misunderstanding about the review's purpose

and the role of the agency in cooperating with the review.

4. *Providing examples of acceptable documentation.* Some respondents commented that access problems were avoid-

ed by making clear to the government agency what type of information they were seeking and providing examples of acceptable documentation. For example, one audit agency repeatedly had difficulty obtaining appropriate documentation that supported substantial adjustments that were made to financial statements. To address this situation, the auditors provided in-house instruction to agency employees about documenting such transactions.

5. *Having persons knowledgeable with information technology work with the agency undergoing the review to facilitate obtaining automated data.* Respondents required data maintained in agency automated databases. Several respondents stated that obtaining the correct data from those databases had been difficult. Some said they were not initially familiar with the data fields in the agency's databases and that they needed the technical capacity to ensure that the databases could be queried and information extracted in usable formats. To address problems with automated data, some respondents said they used their information technology staff to work directly with agency information technology staff to obtain needed data.

“Coordination and communication with the agency requires constant attention.”

Conclusion

In sum, we found general satisfaction with the survey respondents' ability to obtain information and records, although there was more widespread dissatisfaction with the time it took agencies to provide the information. Even if accountability organizations ultimately are not denied access to the information, delays in obtaining the information can affect the quality and usefulness of their work. The most successful strategies in overcoming access issues, including delays, were clear communication and early intervention with agency managers. While these strategies will not completely eliminate access problems, they can reduce the impact of access problems on accountability organizations' ability to perform their critical missions.~



6. *Assuring the agency undergoing review that sensitive data will be protected and that public reports will not include sensitive data inappropriate for public issuance.* A common theme from survey respondents was the concern by the government agency about the sensitivity of the information requested and the concern about public release of sensitive government information. Survey respondents said they addressed this concern by assuring the agency that they would handle the sensitive information carefully and take steps to ensure that it is safeguarded.

For example, the DOJ OIG often needs access to classified or law enforcement sensitive information in our reviews. We take great care to handle that information responsibly, and we stress to OIG employees that they are entrusted with another agency's sensitive information that must be carefully handled.

We also assure the agency whose information we obtain that it will receive an opportunity to review the final report for sensitivity concerns before any information is disclosed outside the Department of Justice.



About the Author

Glenn A. Fine



Glenn A. Fine was confirmed by the United States Senate as the Inspector General of the Department of Justice on December 15, 2000. He served as the Acting Inspector General since August 2000.

Mr. Fine has worked for the Department of Justice Office of the Inspector General (OIG) since January 1995. Initially, he was Special Counsel to the Inspector General. In 1996, he became the Director of the OIG's Special Investigations and Review Unit.

Before joining the OIG, Mr. Fine was an attorney specializing in labor and employment law at a law firm in Washington, DC.

Prior to that, from 1986 to 1989, Mr. Fine served as an Assistant United States Attorney in the Washington, DC, United States Attorney's Office. In that capacity, he prosecuted more than 35 criminal jury trials, handled numerous grand jury investigations, and argued cases in the District of Columbia and U.S. Courts of Appeals.

Mr. Fine graduated magna cum laude from Harvard College in 1979 with an A.B. degree in economics. He was a Rhodes Scholar and earned B.A. and M.A. degrees from Oxford University. He received his law degree magna cum laude from Harvard Law School in 1985.

About the Department of Justice



The mission of the Department of Justice is to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.

Officially coming into existence on July 1, 1870, the Department of Justice, pursuant to the 1870 Act, was to handle the legal business of the United States. The Act gave the Department control over all criminal prosecutions and civil suits in which the United States had an interest.

The Department of Justice has become the world's largest law office and the central agency for enforcement of federal laws.

Convincing Contractors to Report Their Own Procurement Fraud to the Inspector General

Alan S. Larsen, Esq.

Counsel to the Inspector General

and

Eric R. Feldman

Inspector General, National Reconnaissance Office

The government has always accomplished important parts of its work through the use of contractors, from Revolutionary War days to the present. Even back then, we are told, a few scoundrels delivered a mule instead of the horse that the government bargained for. Today, the use of contractors and the problems that arise are more complex than ever. There is even greater impetus today—formal and informal—for agencies to use contractors: to supplement government personnel; to research, develop, and adapt to government use the technological advances made in the commercial sector; and to build and deliver products of all sorts, from pencils to satellites.

At the National Reconnaissance Office (NRO), contractors are a huge part of what we do. Many NRO functions are staffed

by contractors. A large portion of our budget is spent on acquisitions (mostly satellites, rather than pencils, we would note). The NRO believes so strongly in this close relationship with our contractors that we capture it in our vision statement: Freedom's Sentinel in Space: One Team Revolutionizing Global Reconnaissance.



But this “one team” concept can only work if each member of the team is equally committed to the mission of the organization, and accountable for executing its role in accordance with the rules to which all have agreed. In the Inspector General community, we recognize that there can be problem employees who violate the rules, in both government positions and inside contractor companies. Agencies themselves have violated statutes and regulations, just as corporations have. Oversight organizations, such as the Offices of Inspector General (OIG) created by the Inspector General Act of 1978, have been established in recognition of these harsh realities.

At the NRO, our OIG certainly had purview over, and mechanisms to address, such issues when they arose in the contractor worlds. However, it was somehow consistently easier for us to get at the problems when they arose with our “govvies” than when it involved employees of our contractors. Piecing together statutes, federal regulations, and agency regulations, there was no doubt we had authority to pursue our audits and investigations, demand and obtain documents, and conduct interviews.

However, it was undeniable that as a practical matter, it was much more time consuming, and required more threats and more steps—indeed, more lawyers than acquisition people—to get the information and the cooperation we needed in matters involving our contractors.

A fairly predictable, often repeated, scenario went like this: OIG investigators came to OIG Counsel complaining that they had requested information from one of our contractors, only to be told (often by the legal staff) to go away because the contractor does not have to cooperate, let alone provide the information.

The OIG Counsel writes a letter to the company, citing three separate regulations, a statute, and some general language from the agency's contract with the company. The company's lawyer writes back, saying, that may be, but he wants to see a subpoena. We are confident that we do not need a subpoena and don't intend to jump through hoops for entertainment sake. The IG brings the matter to the attention of a senior agency official, who calls a senior company official and asks if their lawyer's position is the one the company really intends to defend. The OIG investigator gets his documents. What a way to do business - especially in an organization like the NRO that has so many contracts and contractors! The reader will be astounded to learn that the OIG's best sales job, even when combined with our assurance, "We're from the OIG and we're here to help," was just not yielding the results we needed in terms of cooperation from the contractors.

Just as this battle scenario was playing out over and over again, NRO OIG was developing and implementing an ambitious and comprehensive Procurement Fraud Initiative (PFI), designed to deter and detect contract fraud, whether stemming from action on the government side or the contractor side.

We identified our most significant vulnerabilities, and the indicators in those areas, and went after them in a concerted way.

Our PFI started from the premise that there is no greater tool in the detection of procurement fraud than knowledgeable government and contractor employees looking for, and reporting, potential procurement fraud indicators. The PFI uses a multifaceted methodology that combines several elements:

1. **Education** of contracting officers, contracting officers' representatives, program officials, and others in identifying the "red flags" of procurement fraud. This is done through lectures at training classes, special briefings, professionally produced video vignettes, and "Messages from the IG" distributed to the government and contractor workforce.
2. **Information Exchange** with other federal law enforcement agencies, the Defense Contract Audit Agency, and other IGs involved in procurement fraud investigations.
3. **Risk Analysis and Data Mining** of agency databases to identify possible anomalies in areas such as contractor billings, agency payments, and government employee behavior.
4. **Audit and Inspection Steps** used in all OIG projects to help detect "red flags," internal control weaknesses, and other vulnerabilities that may exist in agency contracting procedures.

Perhaps the most innovative and risky approach of our PFI was to develop and maintain

“What a way to do business—especially in an organization like the NRO that has so many contracts and contractors!”



an effective program of contractor self-referral of suspected fraud on their contracts through regular interaction with corporate business ethics and compliance officers and other corporate officials of the NRO's most important industrial partners.

The success of the NRO's PFI in helping to prevent and detect fraud, and bring forward cases for prosecution, was recognized when Deputy U.S. Attorney General Paul McNulty asked the NRO Inspector General Eric Feldman to be a founding member of the Eastern District's Procurement Fraud Working Group, designed to share investigative information, best practices, and trends in procurement fraud investigative techniques involving federal contracts.

“ . . . contractors viewed their overriding connection to us to be their contract - not an agency Directive . . . ”

The aspect of the PFI involving contractor self-referral was easier said than done. Despite oral pledges of cooperation, we found out through various back-channel mechanisms that several contractors continued to pursue their own internal inquiries involving allegations of fraud in NRO contracts, while rarely reporting them to the government. We concluded that we somehow needed to address contractor reporting and cooperation more aggressively as part of the larger PFI. It became evident that, not surprisingly, contractors viewed their overriding connection to us to be their contract - not an agency Directive, not a FAR provision, but the contract. When a question arose, “they” (especially a company front line manager) would say, “Show me where it says so in the contract.”

Boom! The lights went on in our OIG. Even though we may have already had all the authority we needed to be legally entitled to cooperation, reporting, etc., it was more difficult to obtain responsiveness because we could not point to a full-text statement that clearly articulated this obligation in the contract. With this epiphany, the NRO Acquisition Manual (NAM) reporting clause was born.

Inserting such a simple clause in the NAM would be an easy proposition, right? Well, not so fast. First, we encountered internal skepticism that we won't recount blow-for-blow in these pages so we can maintain the sanctity of our “one team” solidarity.

Suffice it to say that it is important, indeed critical, for an agency such as the OIG considering an approach similar to ours to work with the agency General Counsel, Office of Contracts, and senior-level management to convince them of the need for a procurement fraud reporting clause before ever floating anything outside the agency. It will be absolutely necessary to go forward with a united front—because the outside world will pick and probe, looking for a chink in the agency resolve to adopt and enforce such a clause.

What we created was a contract clause that would become part of the NAM, applicable by reference in essentially every prime and sub contract. The NRO's Office of Contracts then presented this contract clause, that had been fully vetted internally and agreed to throughout NRO, to our contractors for comment - and comments we did receive!

Many were helpful while identifying language in our draft that needed clarification, or questioning the need for provisions in the clause given other existing requirements. Some were hysterical, accusing NRO of violating four different amendments to the U.S. Constitution.

We modified the draft clause in response to those comments that raised legitimate concerns, but then we quickly moved forward, adopting the clause without feeling compelled to rebut some of the law review-styled tomes submitted by outside counsel, and without seeking full consensus among those who had staked out the more extreme positions.¹

Our clause states:

N52.203-001 NRO Inspector General and the NRO Hotline.

As prescribed in N3.101-72, use the following clause in all solicitations and contracts exceeding the simplified acquisition threshold:

NRO Inspector General and Hotline

(A) The contractor must report to the NRO Inspector General (IG) any and all possible violations of federal law or illegal intelligence activities related to this contract by individuals charging directly or indirectly to this contract.

(B) The IG shall have access to any individual charging directly or indirectly to this contract whose testimony is needed for the performance of the IG's duties. In addition, the IG shall have direct access to all records, reports, audits, reviews, recommendations, documents, e-mails, papers, or other material that relate to this contract with respect to which the IG has responsibilities. Failure on the part of any contractor to cooperate with the IG shall be

¹ Nothing in this clause requires a contractor to waive any privileges it may have, or to forfeit any right to assert such privilege. Further, nothing in the clause is inconsistent with or supersedes the Department of Defense "Voluntary Disclosure Program."

grounds for administrative action by the Director, Office of Contracts, including contractual remedies.

(C) NRO contractors and contractor personnel may report suspected instances of improper

conduct through the NRO IG Hotline at 703-808-1OIG (1644). Contractors shall make their employees aware of this Hotline.

(D) The contractor agrees to include the substance of this clause in all subcontracts exceeding the

simplified acquisition threshold except those for commercial items or components, and those where the NRO association must be protected.

There are thus two primary elements of the contractor obligations to the OIG under this clause. First, the contractor has a reporting obligation—to come to OIG on its own when it becomes aware of certain information. Second, it has a cooperation obligation, to provide information and access to employees, when OIG is performing a review and comes to the contractor. While these obligations do exist independent of the clause, by virtue of statute, regulation, and Executive order, the clause does result in additional enforcement mechanisms and remedies, by virtue of being a contract requirement.

Our jobs would be easier if we could say this was the end of the story. But actually, it is the beginning of the real story. In our view, a requirement, even a clear contractual requirement, does not constitute a procurement fraud program. It is the ongoing relationship, built on mutual trust and much communication that will eventually yield the results we are seeking.

“It is the ongoing relationship, built on mutual trust and much communication that will eventually yield the results we are seeking.”



Using this NAM clause as our statement of what is required and what we expect, we are in the process of building and solidifying ongoing relationships with our contractors. Certainly, we will now be able to obtain needed information more quickly from a contractor when we become aware of a procurement fraud and ask about it. But, we view as more important the contractor referral portion of our PFI. We are in the process of reaching understandings with our contractors about the circumstances in which we expect them to come to us with information, at what stage that should occur, and who should be talking to whom.

We have been conducting a series of one-on-one meetings to establish these expectations and understandings, to exchange business cards and phone numbers, and to put working-level people in both organizations in touch with one another. This has been occurring to some extent with our industrial partners in the Washington area, but is happening at a more intense pace at our West Coast OIG office, where many of the top NRO contractors reside within a mile radius of our operation. We also recently conducted our first ever Corporate Business Ethics and Compliance Officers Conference, bringing together the NRO OIG, other IGs (mostly from the Intelligence Community), and the self-selected “right” people from our contractors’ ethics, legal, security, and compliance shops.

Deputy Attorney General McNulty addressed the group and emphasized the high priority that the Justice Department is placing on procurement integrity at this critical juncture in our nation’s history, where procurement fraud stories hit the papers almost daily. Several companies also presented their Business Ethics and Compliance programs at the conference, and one even highlighted their new NRO OIG fraud reporting protocol in response to the new NAM clause!

We view this conference a success on many levels, not the least of which is the fact that several weeks later, the floodgates of fraud reporting mysteriously opened from companies that had previously had little interest in talking to us about potential vulnerabilities on their contracts. Nevertheless, we believe that we have barely scratched the surface in identifying possible fraudulent activity on our contracts, and much more needs to be done to solidify the OIG’s relationship with our contractor base.

There are also several other areas of our PFI, including data mining and risk analysis that offer more potential than concrete results to date. But our proactive procurement fraud prevention and detection efforts have, on the whole, provided us a window into fraudulent activity that would never have opened with more traditional, “wait for a complaint to come in” approach to fraud investigations.

Today’s procurement of satellites, major defense systems, and information technology costs far too much, and is too vulnerable to fraud and abuse, to warrant anything less than the development of an aggressive, proactive, and mutually supportive antifraud strategy that is pursued jointly with our contractor partners.~

About the NRO

The NRO designs, builds and operates the nation’s reconnaissance satellites. NRO products, provided to an expanding list of customers like the Central Intelligence Agency (CIA) and the Department of Defense (DoD), can warn of potential trouble spots around the world, help plan military operations, and monitor the environment. The mission of the NRO is to develop and operate unique and innovative space reconnaissance systems and conduct intelligence-related activities essential for U.S. National Security.

About the Author*Alan S. Larsen*

Alan S. Larsen became Counsel to the Inspector General of the National Reconnaissance Office on July 7, 2003. He previously served as Deputy Counsel and Acting Counsel to the Inspector General at the Central Intelligence Agency.

Mr. Larsen has spent most of his professional career in private law practice. He headed the Washington, D.C. office of his Pacific Northwest-based firm, after previously practicing in his firm's Portland, Oregon office.

Mr. Larsen has also served as Deputy General Counsel and Senior Vice President for an energy development company.

Mr. Larsen received his Bachelor of Science in Business Administration from Bucknell University where he was selected to Delta Mu Delta, the national business honorary. He received his Juris Doctor degree from the Northwestern School of Law at Lewis and Clark College, where he was selected articles editor of the law review.

About the Author*Eric R. Feldman*

Eric R. Feldman was appointed Inspector General of the National Reconnaissance Office (NRO), on March 24, 2003.

Mr. Feldman has over 25 years of experience in federal auditing and Inspector General oversight, in both the Executive and Legislative branches of government.

From 1991 to 1997, Mr. Feldman served as the first Assistant Inspector General for Audit at the Defense Intelligence Agency (DIA). In 1998, Mr. Feldman joined the CIA as the first Chief of Policy and Plans for the Office of the Inspector General (OIG). He was subsequently selected to join the OIG Audit Staff in February 1999. In July 2001, he became the Acting Deputy Inspector General of the CIA. In January 2002, he was assigned to the Executive Director's staff, where he served as Chair of the CIA Deployed Support Task Force.

Mr. Feldman graduated Magna Cum Laude from the American University in Washington, D.C. with a B.S. degree in Political Science/Public Administration.

Addressing Whistleblower Protection for Employees of Department of Defense Intelligence Agencies

Julie C. Kienitz

Auditor, Department of Defense Office of the Inspector General
Georgetown University Executive Masters of Policy Management Capstone Paper

The Problem

Employees of Department of Defense (DoD) intelligence agencies are not coming forward to report incidents of reprisals against those who report fraud, waste and abuse as often as employees of non-intelligence agencies and members of the armed services.



As of May 2005, only four cases of reprisal cases against DoD intelligence agency whistleblowers had been investigated by the DoD Office of the Inspector General (OIG) and Office of the Assistant to the Secretary of Defense for Intelligence Oversight in the last ten years.

In comparison, the OIG Directorate for Civilian Reprisal Investigations had a total of 16 active, open cases during the reporting period of April 1, 2004, to September 30, 2004,¹ and the Directorate for Military Reprisal closed 715 cases in Fiscal Year 2004.²

History of Whistleblower Protection

Congress has passed several laws to protect individuals who come forward to disclose fraud, waste and abuse within the federal

¹ Inspector General, United States Department of Defense, (2004). Semiannual Report to Congress, April 1, 2004-September 30, 2004(34).

² Inspector General, Department of Defense. (undated). DoD Whistleblower/MHE [Mental Health Evaluation] Case History Briefing Chart.

government. The Whistleblower Protection Act of 1989; the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (Public Law 107-174) and the Military Whistleblower Protection Act protect federal employees, members of the armed services from adverse consequences and reprisals in retaliation for reporting wrong doings.

The Whistleblower Protection Act of 1989 established the Office of Special Counsel as an independent federal agency to protect federal employees and applicants from prohibited personnel practices, especially as a result of whistleblowing. The Act refers to Section 2302, Title 5, United States Code (U.S.C), to delineate the protected individuals. Section 2302, Title 5 U.S.C., specifically excludes from the purview of the Office of Special Counsel individuals working for “the Federal Bureau of Investigation (FBI), the Central Intelligence Agency, the Defense Intelligence Agency (DIA), the Central Imagery Office³, the National Security Agency (NSA), and as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities.”

Since the Whistleblower Protection Act did not protect employees of DoD intelligence agencies, they were formally subject to sanctions for disclosing classified information or whistleblowing to Congress without authorization. However, there was an unspoken understanding between the intelligence community

³ The Central Imagery Office is now a part of the National Geospatial-Intelligence Agency.

and the intelligence committees concerning how employees who contacted Congress without prior authorization would be treated. While not encouraged by management, such meetings were not actively prohibited or penalized⁴.

Before 1995, when employees of DoD intelligence agencies had concerns they felt needed to be addressed, they would meet with members of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence unofficially. Whistleblowers would contact staffers at home and then meet them in secluded restaurants or bars.⁵

Everything changed in 1995 when a Department of State official involved in peace negotiations in Guatemala told a member of the House Permanent Select Committee on Intelligence that the Central Intelligence Agency was involved in human rights abuses in Guatemala. The Representative leaked the allegations to the New York Times. In response, for providing the Representative with classified information without the permission of his supervisors,⁶ the Director of Central Intelligence revoked the official's clearance for Sensitive Compartmented Information.

“... there was an unspoken understanding between the intelligence community and the intelligence committees concerning how employees who contacted Congress without prior authorization would be treated.”

The Director of Central Intelligence based his actions on an Office of Legal Counsel for the Department of Justice memorandum. The memorandum stated, “The President’s roles as Commander in Chief, head of the Executive Branch, and sole organ of the Nation in its external relations require that he have ultimate and unimpeded authority over the collection, retention and dissemination of intelligence and other national security information in the Executive Branch.”

There is no exception to this principle for those disseminations that would be made to Congress or its members.”⁷ The Senate Select

Committee on Intelligence responded by adding a whistleblower protection provision in the Intelligence Authorization Act for Fiscal Year 1998.

The Intelligence Community Whistleblower Protection Act (ICWPA) of 1998

enables civilian, military or contract employees of the DIA, National Geospatial Intelligence Agency, National Reconnaissance Office and NSA to report classified information about alleged wrongdoings of “urgent concern” to Congress.

Wrongdoings of urgent concern to Congress would include a serious abuse, violation of law or deficiency relating to funding, administration, or operation of an intelligence activity involving classified information.⁸

4 Thomas Newcomb, “In From the Cold: The Intelligence Community Whistleblower Protection Act of 1998,” *Administrative Law Review* (Volume 53, Number 4) (Fall 2001) 1237.

5 Thomas Newcomb, “In From the Cold: The Intelligence Community Whistleblower Protection Act of 1998,” *Administrative Law Review* (Volume 53, Number 4) (Fall 2001) 1238-1239.

6 Thomas Newcomb, “In From the Cold: The Intelligence Community Whistleblower Protection Act of 1998,” *Administrative Law Review* (Volume 53, Number 4) (Fall 2001) 1238.

7 Thomas Newcomb, “In From the Cold: The Intelligence Community Whistleblower Protection Act of 1998,” *Administrative Law Review* (Volume 53, Number 4) (Fall 2001) 1240.

8 Public Law 105-272, “Intelligence Community Whistleblower Protection Act of 1998,” September 25, 1998.



The Inspector General, DoD has issued a policy memorandum to implement the provisions of the ICWPA of 1998 within the Office of the Inspector General, DoD. The policy memorandum designated the Deputy Inspector General for Intelligence as the primary individual responsible for all DoD matters reported to the OIG under the ICWPA.

Although the ICWPA provides an avenue for reporting fraud, waste, and abuse within the DoD, individuals employed by DoD intelligence agencies do not have a means of directly reporting classified information outside of the Department.

Employees of DoD non intelligence agencies filed over 700 reprisal complaints in FY 2004 alone. Employees of DoD intelligence agencies have filed only four reprisal complaints in the last ten years.



If instances of fraud, waste and abuse are taking place but are not being reported, effective oversight of DoD intelligence agencies becomes much more difficult. Whistleblowers are needed to report wrongdoings that would never be known by any other means. These wrongdoings may include defective parts, overpricing by contractors, or even espionage.

Why is there a Difference?

The low rates of reprisal reporting by employees of DoD intelligence agencies may mean there are fewer incidents of fraud, waste and abuse occurring in DoD intelligence agencies; incidents may occur and are reported, however, no acts of reprisal are taken against whistleblowers; or incidents of fraud, waste and

abuse are occurring but are not being reported, therefore, there are no whistleblowers to retaliate against.

In addition, if a whistleblower's attempts to make his concerns known within his chain of command were unsuccessful, his frustration from a lack of action (perceived or actual) may prevent him from contacting an organization within the DoD.

Other reasons for under reporting may include the culture of secrecy and loyalty within the intelligence community and concern for the protection of classified information.

How can this Trend be Changed?

One solution is to create a secure avenue for DoD intelligence agency whistleblowers to directly submit complaints outside DoD. Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004, established a Director of National Intelligence (DNI) and amended the Inspector General Act of 1978 with the addition of a new section that provided the Director with the authority to establish an Office of the Inspector General.

The Act states that "If the Director of National Intelligence determines that an Office of Inspector General would be beneficial to improving the operations and effectiveness of the Office of National Intelligence, the DNI is authorized to establish, with any of the duties, responsibilities, and authorities set forth in this Act, an Office of Inspector General."⁹

⁹ Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," December 17, 2004

The Inspector General, Office of the DNI, could provide the employees of DoD intelligence agencies the opportunity to report their concerns outside of their chain of command, if necessary, while maintaining the security of the information.

In addition, the Inspector General, DNI, could provide training to DoD intelligence agency employees or participate in training classes at the DoD intelligence agencies, to explain the mission of the Office of the Inspector General, as well as the responsibilities of the employees to report fraud, waste and abuse. The Inspector General could also stress the employees' rights under the ICWPA of 1998, as amended.

If one concludes that four complaints of whistleblower reprisal do not accurately reflect the incidence of fraud, waste and abuse within the DoD intelligence agencies, then a way is needed to report acts of reprisal outside of the normal chain of command while protecting the source and maintaining the security of the information.

The trust of employees of the DoD intelligence agencies must be earned and maintained. People must feel secure before they will take the chance to report their concerns.~



About the Author

Julie C. Kienitz



Julie C. Kienitz has 17 years of audit experience within the DoD OIG. She is currently a Team Leader within the Office of the Deputy Inspector General for Intelligence, Audit Division.

During her years at the OIG, Ms. Kienitz has also been assigned to the Office of the Deputy Inspector General for Auditing, as well as the former Office of the Assistant Inspector General for Policy and Oversight. Her experience includes audits on the acquisition of major weapons systems, contracting, information technology security, intelligence programs, logistics, readiness issues, special access programs and export controls.

Ms. Kienitz graduated from Heidelberg College, Tiffin, Ohio, with Bachelor of Science degrees in Accounting and History in May 1989. She graduated with a Masters of Policy Management degree from the Georgetown Public Policy Institute in May 2005.

From Internal Controls to Audit Readiness

Mary L. Ugone

*Deputy Inspector General for Auditing, Department of Defense Office of Inspector General
and*

Judy Padgett

Program Director for Quality Assurance and Policy, Department of Defense Office of Inspector General

Speech delivered June 2, 2006, at the American Society of Military Comptrollers Conference in San Diego.

Thank you and good morning. Both Judy and I appreciate the opportunity to express our views on internal controls—a key to auditability. Today I am going to talk to you about why we need internal controls, and I will also talk briefly about the official guidance and the concepts and philosophy that the guidance is based on.

Judy is going to talk about the (1) relationships between internal controls and change, (2) the importance of meaningful controls, and (3) how those controls contribute to audit readiness for the Department.

When we were developing these briefing charts, I was challenged on my choice of the word “inevitable” (see Chart 1). “Necessary” was the word that was recommended to me because “inevitable” means something that cannot be avoided or prevented. You can avoid or circumvent internal controls if they are not properly designed and followed in daily business operations. However, controls also seem to be inevitable in that people naturally organize their work, develop procedures, and define duties around things they do repeatedly. At the heart of it, controls are fundamental to a society that wants order and is governed by laws.

From informal controls that either develop or evolve for convenience or protection, we institutionalize those controls that are “necessary”—controls that help us to operate effectively and efficiently, to report our financial information reliably, and to comply with laws and regulations.

Whether inevitable or necessary, internal controls must be a continuous part of any organization. Controls are needed at the beginning when an organization is forming and every day until it ends. Of course, the internal controls need to be continuous, but over time, they will not be the same.

Inevitable or necessary, beginning to end . . . and integral. Internal controls should be part of everything that we do. It is because internal controls are such an integral part of work and home life that we often do not recognize them.

How many of you park in the same assigned place every day? How many of you get towed if you do not? How many of you verify the charges on your credit card? Get authorization from your spouse for a major purchase or vacation decision? At work, we have a long list of things we “have to do,” and some of those things are, in fact, part of internal control.

Internal Controls

- Inevitable
- Continuous
- Integral part of life, business and government

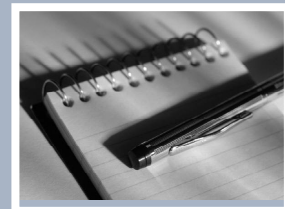


Chart 1



Timeline

1982	Federal Managers' Financial Integrity Act (FMFIA)
1985	Committee of Sponsoring Organizations
1987	OMB Circular A-123
1999	GAO Standards for Internal Control
2002	Sarbanes-Oxley Act
2004	OMB Circular A-123 and Appendix A
2005	Appendix B and OMB Guide to Implementing Appendix A
2006	DoD Instruction 5010.40
2006	OMB Bulletin 01-02 Revised

Chart 2

This is internal control for both operations and financial reporting. I want to emphasize that the arrival of Appendix A with its specific requirements for reporting on the internal controls over financial reporting doesn't make internal controls unnecessary in operations.

I would like to now refer you to the timeline on the screen (see Chart 2). This timeline shows how long the basic ideas for internal control have been around in terms of legal requirements for government entities. In 1982, the FMFIA, or Federal Managers' Financial Integrity Act, established the need for internal controls to operate efficiently and effectively, to report financial information reliably, and to comply with laws and regulations. The Office of Management and Budget (OMB) and the Government Accountability Office (GAO) developed the implementing framework for the public law. Subsequent iterations developed more detail and definition for internal control standards.

The 1999 GAO standards were very similar to those of the Committee of Sponsoring Organizations of the Treadway Commission. The

Committee is better known as COSO, which recommended a framework for internal controls primarily consisting of five standards. Judy will touch on those in her part of the presentation.

Then in 2002, Sarbanes-Oxley came along, and its influence was a major factor in adding Appendix A to the revised OMB Circular A-123. There are some key dates not listed here, but they certainly play a role. The only reason you do not see them listed is that it is difficult to get

everything on a slide that we can all still read. Two dates with significant laws are 1990 (the Chief Financial Officers Act) and 1996 (the Federal Financial Management Improvement Act). Those laws significantly impact agencies and re-emphasize the need for effective internal controls. OMB Circular A-123 Revised, page 21, paragraph 1, states that "Federal Agencies are subject to numerous legislative and regulatory requirements that promote and support effective internal control."

The paragraph goes on to describe those two laws: This is the only citation I plan to use, but because I am an auditor I needed to cite at least one specific criteria. I promise no more.

Let me emphasize here that internal control is for everyone and that theme is recurring in this presentation. You may call internal controls by another name, but it is that which helps in ensuring order, results, and governance. The addition of the requirements for financial reporting put an extraordinary focus on the financial arena, but it is still part of the Managers' Internal Control Program. The Managers' Internal Control Program is key to providing guidance on the annual statement of assurance



and telling us how the program should look in DoD. The Comptroller does that through the DoD Instruction 5010.40 and the annual guidance for preparing the statement of assurance (see Chart 3). The Comptroller is responsible for developing that guidance and for compiling the results, but that does not mean the Managers' Internal Control Program applies only to comptroller or financial types of organizations. DoD Instruction 5010.40 and the annual guidance clearly have requirements for operations too. Operations need internal controls or we may not have anything to reliably report financial information about.

In our audit function at my organization, we now find ourselves assessing internal controls in other parts of the world and in a combat environment. But the controls we encounter in our audit work should not be a surprise. These controls should not be any different from what we see every day in our work here. What is the bottom line objective when we use a fund, a resource, and an asset? The objective will continue to be the accomplishment of the mission.

Let me give you an example. The funds used to support U.S. efforts in Iraq and Afghanistan may be in the form of cash. It may not be the norm for Government operations stateside, but in countries particularly where there is either no banking infrastructure or a disrupted infrastructure, cash is used. Does cash require a different perspective and set of accounting controls in countries where there is no underlying information technology infrastructure? Yes, because the control environment is at higher risk, which warrants emphasis on fundamental controls based on physical safeguards as well as the written record, reconciliation, and verification. Remember, there are no banks to help record, reconcile, and verify. At the same time, remember, the funds are being used to accomplish a mission objective. Using this scenario, for example, we ask ourselves the question: Have the Iraqi security forces received the required training obtained by the funds? That is the mission objective, so yes, they should have received the required training using those funds. This is why comptrollers (you in the audience) are so important to the internal control process. Regardless of form, any payments that link the financial to the mission objective must be transferred under a system of controls so that it ends up where it should and satisfies the achievement of the mission at hand.

A-123 also has detailed requirements for areas of high interest from our lawmakers: financial reporting (Appendix A), government charge card program (Appendix B), and pro-

DoD Instruction 5010.40

- Implements OMB Circular A-123 and Appendix A
- Guidance for the DoD program
- Applies to all segments of DoD

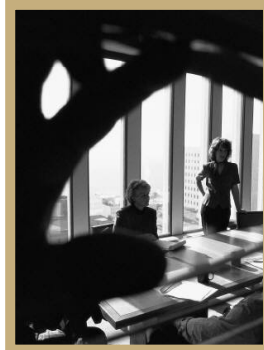


Chart 3

Returning to the timeline for a moment, let me point out that A-123 appeared more than once. A-123 gets updated periodically to better fit current conditions, but the foundation remains the FMFIA (Federal Managers' Financial Integrity Act). The most recent version of A-123 changes perspective rather than those basic principles of operational effectiveness and efficiency, reliable financial reporting, and compliance with laws and regulations. The current A-123 perspective is more detailed. It is modeled after the COSO and GAO standards for internal control—that is, it is built on the five standards for internal control.

posed improper payment guidance (proposed Appendix C). That last appendix title—last appendix title—seems to have been written by a poet where repetition of a consonant is often used in a poem. However, let me assure you, A-123 is definitely not poetry. Please note that the internal control requirements are not new—the additional focus is new. Reporting on the internal controls over financial reporting is what is new—what is a change in perspective. That certainly reflects the influence of the Sarbanes-Oxley Act.

Need for Change is Part of Standard



- Risk assessment
- Information/
Communication
- Monitoring

Chart 4

The theme of this conference is waves of change. Most certainly the changes we are experiencing thanks to Sarbanes-Oxley and A-123 Appendix A and our efforts to get to audit-ready financial statements can make it feel like we are caught in a nasty undertow. I suggest we regard those waves of change with the solid foundations of the underlying internal control concepts in mind.

I keep returning to this point—internal controls are not new ideas. Internal controls such as separation of duties, reconciliations, authorizations, standard operating procedures, and more have been around since long before the FMFIA or Sarbanes-Oxley or Appendix A. The very foundation of this nation is based on a system of checks and balances—one of the most

visible systems of internal control. Oftentimes we need to recognize what is already there. We do not need to invent something new with every new program—we just need a different perspective and perhaps emphasis, or even a re-emphasis. We need to continue reminding ourselves that internal control is for everyone and is part of everyday government function.

As financial personnel, you experience controls both at the operational and financial level. This experience can work for you and your organization. Tap into it in order to identify the internal controls we have but have not recognized. During that process, determine which controls require change and which areas require controls because there are none. Look at the controls from someone else's perspective. The process of identification and implementation is one that is already built into the standards for internal control and a process that Judy is now going to talk about.

Three of the five standards (environment, risk, control activities, information/communication, monitoring) are shown here (see Chart 4) but if you examine and think about the standards, all five are designed to accommodate change and continuous consideration. Risk is at the top of the list because it is one of the areas where major factors such as economics, politics and natural phenomena, are often out of our control. All five standards are intertwined. For example, a change in risk should result in a change in the activities to eliminate or minimize the risk and its effects. A change in the activities must be communicated to the organizational community—this could mean employees, customers, vendors or all of the above. Once a control activity is implemented, we need to monitor it to determine whether it actually achieves the control objective to minimize the effects of the risks identified, whether the control was effectively communicated—people are using the control, is it effective as designed



... the monitoring has to occur over time so adjustments can be made as conditions and risks change. Soon we will have a new administration and that could bring new ways of doing things. Yesterday marked the beginning of what is expected to be a very wicked hurricane season. Will that change our controls? So—change is very much a part of internal control.

Here we are back at internal control is for everyone (see Chart 5). The additional reporting requirements have created an added challenge for DoD. The overall reporting will include the material control weaknesses identified for both pieces of the statement of assurance, that is the operational and the financial reporting, to maintain visibility over the weaknesses. The financial reporting corrective actions are included in the Financial

Improvement Audit Readiness (FIAR) Plan and recognized by the Defense Business Modernization Program.

I am pointing out once again that although the focus has changed from OMB with the requirement for the financial reporting statement of assurance, the requirements for internal controls and a statement of assurance date back at least to 1982. Requirements have not changed—they have just had a makeover.

Dual reporting was levied on DoD and other departments. The approach each department has taken is different, as I learned at a

May 11th conference at which several departments had representatives speak. What DoD is doing is setting specific requirements in the DoD Comptroller’s annual guidance for evaluating the status of controls and submitting the two reports. A repeated theme in the annual guidance is that this is one program. The emphasis on implementing Appendix A is pervasive in the Federal community and the contractors who serve them and it will take work to keep operational leaders and managers engaged on this. We can’t have this be “Just a financial or just a comptroller exercise”—and there is no “just” about the financial piece of this.

My concern, it seems, is that to keep operations engaged, the financial piece gets minimized and that cannot happen either. We have two important pieces to this Managers’ Internal Control Program. I

want to say a bit more about the two pieces of the Managers’ Internal Control Program and the annual guidance that applies to the annual reporting.

Part I of the guidance, the directions for the Statement of Assurance on the effectiveness of internal control for programs, administrative activities and operations, is reasonably well developed. The dates and products are known, the evaluation and compilation procedures have been developed and followed for several years, the program managers for Managers’ Internal Control have experience with the process. Because Part I has been around for a while, the

Internal Controls for Everyone

- OMB Circular A-123 has financial reporting in an Appendix, standards apply to all
 - Emphasis - operations also need internal controls
 - Not simply financial reporting issue
- FMFIA addressed operational and financial internal controls in 1982 - requirements not new - simply had makeover








Chart 5

methodology and reporting are stable, slower to change, less radical changes.

Not so for financial reporting. Financial reporting is not familiar. No change is quite so radical as the first time meeting a requirement. Part II of the annual guidance has several key dates, most of them are already passed. In December, those subject to Part II guidance delivered process narratives, flow charts, and organizational charts for the focus areas, in February they delivered risk analysis, and in March internal control lists and test plan methodology. Most recently, the Part “IIers” delivered internal control review reports and corrective action plans. The documents and assessments from the Part II deliverables form the framework for producing the Statement of Assurance on financial reporting. As experience is gained and the focus list expands, those in financial reporting will probably experience considerable change in the assessment and reporting process as lessons are learned and until the financial reporting Part II guidance stabilizes. Once the guidance stabilizes, financial reporting entities will likely experience slower and smaller changes in the procedures to prepare the Statement of Assurance. As for the specific controls and the Managers’ Internal Control Program, financial reporting entities may experience less change than their operational counterparts because accounting procedure and reporting tend to vary less over time than do operations and programs.

Notice that I did not say change would stop for either operations or financial reporting. Although the pace and focus may differ for operations and financial reporting, it is important for a well-built program that both pieces be flexible, adaptable—dynamic for an effective Managers’ Internal Control Program.

We spoke earlier about recognizing what the Department already has and building on that. The goals and objectives of our systems of controls should be consistent with other programs

and initiatives that are underway. The Comptroller has fit the financial reporting Statement of Assurance and the deliverables leading up to it into the FIAR Plan. In the transmittal of the plan the Deputy Secretary of Defense, Gordon England, stated:

The Financial Improvement and Audit Readiness Plan, spearheaded by the Under Secretary of Defense (Comptroller), is the DoD roadmap to fix internal controls, correct processes, and obtain an unqualified audit opinion. The plan integrates solutions such as upgraded systems with improvements to processes.

The FIAR Plan is about understanding what we have and building on that and so is the Managers’ Internal Control Program with its assessments and documentation and statement of assurance for financial reporting. The assessments are about identifying the existing controls and about discovering where the controls need change, communication, commitment or creation. In this process we must—to the very best of our ability—be accountable to and protect both the taxpayer and the warfighter. This can be a challenging balancing act, one that Mr. England referred to in his message in the 2005 Performance and Accountability Report. His message ended with this: “The Department of Defense continues to transform itself into a more agile organization able to meet the challenges of the 21st century. The Department must continue to improve its financial accountability, shift resources from the bureaucracy to the warfighter, and improve the quality of life in our armed forces—and is committed to do so.”

What Mr. England’s message says to me is that we must use what we have rather than build yet another piece of bureaucracy. We do not want implementation of Statement of Assurance on financial reporting to take away badly needed resources from our armed forces. We need everyone’s involvement and we need to integrate and leverage plans in place. In addi-

tion to the FIAR Plan, there are other improvement plans and even informal procedures that we can use to arrive at the audit ready financial organization that is DoD.

The documents delivered over the last few months have recorded the controls already there. The opportunity to document “what is” might not be over—because this was the first year, we may need add to and embellish the deliverables next year.

In addition to offering an opportunity to analyze and document procedures, the Statement of Assurance on financial reporting is an opportunity to put results and progress on the FIAR and financial reporting improvements in the public view via the Performance and Accountability Report.

The analysis opportunity may also show that there among the “what is already there” is some “not there yet” that needs to be identified, designed, and implemented.

Those controls that “are not there yet,” the ones that need to be identified, designed, and implemented should have these features—

- Meaningful. Do not build a Potemkin Village. If you are wondering what a Potemkin Village is, well so was I when I heard it a few weeks back. Potemkin was a Russian Minister who, according to popular mythology, built empty structures to impress Catherine the Great and thus improve his standing because of the valuable assets added to her domain. We do not want to build empty structures simply to impress the auditors or other reviewers.
- Practical and simple—increases the likelihood of implementation and success.
- Cost beneficial—this is one of the underlying principles of controls. The taxpayer does not


want to pay for perfection. We cannot afford perfection.

- Effective—I have the word effective here twice but it probably needs that kind of emphasis. Not only must we avoid empty controls, those just for show, but we must monitor controls to make sure they work, that all the people affected by them understand them and are getting the intended benefits.

Effective internal controls have a cascading effect. Once again, it is difficult to figure out what comes first—the controls or the environment but as we work to get all standards together audit readiness becomes possible. That was conveyed in both messages I quoted from Mr. England.

The cascading effect might look something like this (see Chart 6). Of course, this is a simplistic presentation and doesn’t include internal controls over processes or over safeguarding assets—the other two internal control objectives. I hope that what you see here is a progression—one that might even get easier as we gain experience and as internal controls improve.~

Audit Readiness



- Reliable internal controls over transactions lead to reliable data entry to systems
- Reliable internal controls over systems lead to reliable processing of transactions
- Reliable internal controls over compiling results into financial reports leads to reliable financial statements
- Reliable financial statements are ready for audit

Chart 6

About the Author*Mary L. Ugone*

The Deputy Inspector General for Auditing serves as one of four Deputy Inspector General's within the Office of Inspector General (OIG), and reports directly to the Inspector General of the Department of Defense. Ms. Ugone assumed her duties January 3, 2006, and is responsible for providing audit functions within the Department of Defense on matters that involve efficiency in operations, contract management, and financial audits.

Ms. Ugone is a Certified Public Accountant, a member of the Virginia Society of Certified Public Accountants, a member of the Association of Government Accountants, and a graduate of the Federal Executive Institute.

In 2003, 2004, and 2005, Ms. Ugone received the President's Council on Integrity and Efficiency Awards for Excellence. Her superior leadership and outstanding accomplishments earned her the IG Distinguished Service Award and Medal in 2002 and the Secretary of Defense Exceptional Civilian Service Award and Medal in 2000.

About the Author*Judy Padgett*

Ms. Judith I. Padgett has a BA in English from the University of North Dakota, a BS in Accounting from the University of California, Sacramento, and an MBA from Golden Gate University.

Ms. Padgett has over 25 years of DoD auditing experience. In 1987, she joined the Office of Inspector General of the Department of Defense. She has audited a variety of issue areas including environment, contracting, IT and telecommunications, financial systems, and personnel security.

Ms. Padgett is currently the technical director for the Quality Assurance, Policy, and Electronic Documentation Division in the ODIG-Auditing. Her responsibilities include the areas of quality assurance reviews, policy, the Managers' Internal Control Program for the ODIG-Audit, and Team-Mate electronic documentation support. She serves as a liaison to the OSD Comptroller Risk Management Division, the division that prepares the Annual Statements of Assurance, and speaks on the importance of internal controls whenever possible.

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 Inspectors General community.

Articles should be approximately three to five pages, single-spaced, and should be submitted to:

Jennifer Plozai
Department of Defense Office of the Inspector General,
400 Army Navy Drive, Room 1034
Arlington, VA 22202.

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 correction action;

