



# Inspector General

United States  
Department *of* Defense

Semiannual  
Report *to the*  
Congress

April 1, 2002 - September 30, 2002

Required by Public Law 95-452

## The Inspector General of the Department of Defense Emblem

*The official emblem of the Office of Inspector General Department of Defense portrays the DoD eagle bearing the shield of the United States on its breast and holding in its beak a white (Argent) motto scroll doubled scarlet and inscribed with the words “Integrity” and “Efficiency,” also scarlet, grasping in its talons a perch formed by three arrows, which are bound together with scarlet bands and held tightly in the talons of the eagle, atop a two-headed axe with gold fascies, bound with scarlet bands, between two gold torches enflamed all gold, all between two green branches, olive to sinister and laurel to dexter, conjoined in base by a stylized granite foundation block inscribed “Sub Tutela Altissimi Semper,” all upon a light blue disc within a white collar edged gold on the outside with the inscription “Inspector General” above and “Department of Defense” below between, at either side two stars, all dark blue.*



Official DoD Seal



New OIG Emblem

Approved September 11, 2002



Old OIG Emblem

*The American bald eagle and shield, the rays and stars above the eagle, the laurel and olive branches, and the light and dark blue colors are adapted from the seal of the Department of Defense, which suggests the traditional role of a military Inspector General as “an extension of the eyes, ears, and conscience of the Commander.” The American bald eagle, long associated with symbolism representing the United States of America and its military establishment, was selected for the Department as an emblem of strength. The eagle is defending the United States, represented by the shield of thirteen pieces. The thirteen pieces are joined together by the blue chief, representing the Congress. The rays and stars above the eagle represent the original thirteen states, as do the bars of the American shield. The torches shedding light to either side and the fascies, an ancient symbol of authority, suggest the missions of promoting “economy, efficiency, and effectiveness in the administration of,” and preventing and detecting “fraud and abuse in,” the programs and operations of the Department of Defense. The binding together of the three arrows in the talons of the eagle, which on the DOD seal symbolize the three separate military departments, symbolize the Inspector General’s statutory duty to “give particular regard to the activities of the internal audit, inspection, and investigative units of the military departments with a view toward avoiding duplication and insuring effective coordination and cooperation.” The inscribed stone base denotes the historical foundation of the American Inspector General system and refers to George Washington’s first effective Inspector General, Baron Friedrich Wilhelm von Steuben, and depicts his family motto, which translates to “Always under the protection of the Almighty.” The motto scroll inscribed “Integrity” and “Efficiency” denotes the modern statutory qualities, exemplified in the “President’s Council on Integrity and Efficiency,” and represents these qualities respectively in the colors white (Argent) and crimson.*

## FOREWORD

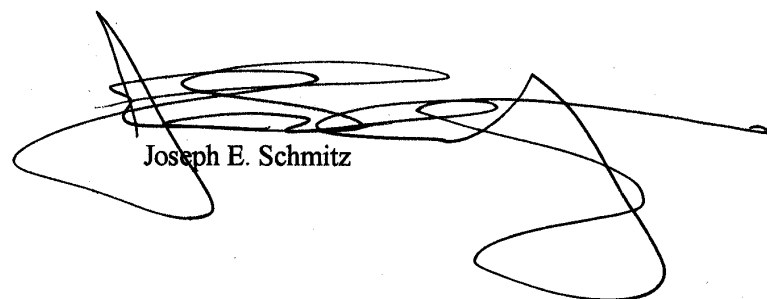
Having completed my first six months as Inspector General, I am pleased to report that a profound cultural transformation is underway not only in the Department of Defense (DoD) but also in the Office of Inspector General of the Department of Defense.

On September 10, 2001, Secretary Rumsfeld delivered an address at the DoD Acquisition and Logistics Excellence Week Kickoff in which he described an adversary that "poses a threat . . . to the security of the United States of America." Secretary Rumsfeld challenged the Department "to wage an all-out campaign to shift the Pentagon's resources from bureaucracy to the battlefield, from tail to tooth." While calling on the Department to transform the way it conducts business, the Secretary of Defense made it clear that his focus was "[n]ot the people, but the process. Not the civilians, but the systems. Not the men and women in uniform, but the uniformity of thought and action that we too often impose on them." While the horrific events of the next day have served to heighten our awareness of the importance of streamlining the processes to support the warfighters, it has not derailed the other process; the concurrent battle to streamline bureaucracy wages on.

In the tradition of what Army Inspectors General call the "Von Steuben Model," named after the American military's first effective "Inspector General," upon Senate confirmation I undertook immediate efforts to transform the Office of the Inspector General into a paradigm for the Secretary's "Bureaucracy to the Battlefield" initiative -- so that, having transformed my own organization, I could more effectively make contributions to the Secretary of Defense's broader efforts to combat fraud, waste, and abuse throughout the Department of Defense.

At the beginning of my tenure, I commissioned a bottom-to-top assessment of the Office of Inspector General to get an unvarnished picture of the fitness of this Office for deployment in the ongoing "campaign to shift the Pentagon's resources from bureaucracy to the battlefield." The independent assessment team's report is complete and is available on our website. After studying the independent assessment report and in light of guidance from both the Secretary of Defense and Congress, I have undertaken an internal transformation consonant with Secretary Rumsfeld's call to "transform not just the way we deter and defend, but the way we conduct our daily business." As this Semiannual Report to Congress is being produced, that transformation is fully underway.

In the end, I envision the Office of Inspector General, simply stated, as the paradigm for the leaner, more agile fighting force it purports to support.



Joseph E. Schmitz

This page left blank intentionally

## TABLE OF CONTENTS

	<b>Page</b>
<b>CHAPTER ONE - SIGNIFICANT ACTIVITIES.....</b>	<b>1</b>
Introduction .....	1
Criminal Investigations .....	1
Terrorism .....	2
Criminal Investigative Policy and Oversight.....	14
Voluntary Disclosure Program.....	15
Administrative Investigations .....	15
Auditing.....	19
Information Technology Management .....	20
Information Security .....	20
Acquisition.....	21
Chemical and Biological Defense .....	22
Quality Assurance .....	23
Cooperative Threat Reduction Program .....	23
Web Site Management.....	23
Significant Open Recommendations .....	24
OIG DoD Testimony .....	25
Intelligence Review.....	25
 <b>CHAPTER TWO - OFFICE OF THE INSPECTOR GENERAL TRANSFORMATION .....</b>	 <b>27</b>
 <b>APPENDICES</b>	
A. OIG Indicators of Potential Terrorist Threats .....	31
B. Reports Issued by Central DoD Internal Audit Organizations .....	37
C. OIG DoD Audit Reports Issued Containing Quantifiable Potential Monetary Benefits .....	47
D. Followup Activities .....	49
E. Contract Audit Reports Issued.....	51
 <b>FIGURES</b>	
1. Judicial and Administrative Actions .....	3
2. DoD Total Senior Official Cases - FY 99 - FY 02.....	18
3. Nature of Substantiated Allegations Against Senior Officials During 2nd Half FY 02.....	18

This page left blank intentionally

## CHAPTER ONE – SIGNIFICANT ACTIVITIES

### INTRODUCTION

The President’s Management Agenda (PMA) provides a “results-oriented” strategy for improving the management and performance of the federal government. The Agenda targets the following five critical areas for improvement:

- Strategic Management of Human Capital;
- Competitive Sourcing;
- Improved Financial Performance;
- Expanded Electronic Government; and
- Budget and Performance Integration.

A key challenge to the Department of Defense (DoD) is the need to establish appropriate measures and milestones, also known as “metrics,” that will provide DoD leadership with the key information necessary to track progress and make sound decisions in the business of national defense.

The Office of Management and Budget (OMB) rates each of the above areas for improvement as green, yellow, or red, depending upon measurable improvements. In the October 2001 baseline score card, the Department was rated red or unfavorable for all five critical areas. In its fiscal year 2003 Mid-Session Review, the OMB recognized the Department’s progress in Strategic Management in Human Capital; Improved Financial Performance; and Expanded Electronic Government, and assigned ratings of green. The OMB rated DoD’s improvements in Competitive Sourcing and Budget and Performance Integration yellow for making progress.

The Office of the Inspector General of the Department of Defense (OIG DoD) and audit agencies of the Military Departments contribute to the Department’s implementation of the President’s Management Agenda by examining operations and identifying improvements that can assist the Department in achieving success for the initiatives.

### CRIMINAL INVESTIGATIONS

The four Defense Criminal Investigative Organizations (DCIOs) continue to combat crime affecting the DoD. The Defense Criminal Investigative

Service (DCIS) focuses on procurement fraud, health care fraud, computer crimes, major thefts, and significant crimes impacting Defense Agencies. The U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service (NCIS), and the Air Force Office of Special Investigations (AFOSI) also investigate procurement fraud, but focus mostly on crimes against persons and property within their respective Military Departments, as well as force protection. The AFOSI and NCIS also conduct counterintelligence investigations and operations. The DCIOs have also been supporting anti-terrorism investigations and participating as members of Joint Terrorism Task Forces. The DCIOs work cooperatively to solve cases involving more than one Service.

Monetary recoveries and fines related to all criminal investigations throughout the Department of Defense totaled more than \$79 million. Figure 1 (page 3) displays other statistical results achieved by the four investigative organizations during the semiannual reporting period. The following are examples of significant fraud cases.

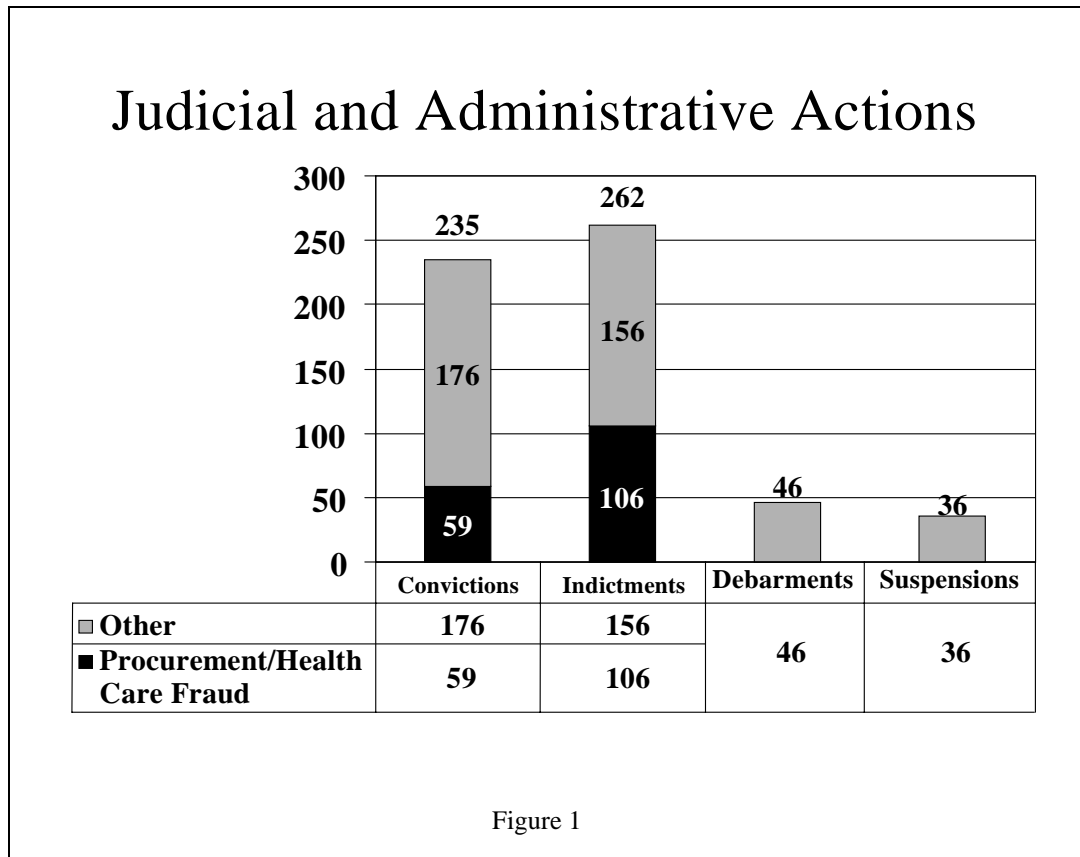
## **TERRORISM**

Presidential Decision Directive 39 (PDD 39) states “it is the policy of the United States to deter, defeat, and respond vigorously to all terrorist attacks on our territory and against our citizens, or facilities....”

After the tragic events of September 11, 2001, the Office of the Inspector General of the Department of Defense (OIG DoD) moved to enhance law enforcement efforts in the prevention of terrorist attacks. Defense Criminal Investigative Service (DCIS) special agents are working at Joint Terrorism Task Force (JTTF) locations, in addition to doing their traditional work of ensuring our warfighters have the best and safest equipment to accomplish their missions. Currently, 19 DCIS agents are assigned full time to JTTFs in 19 different locations. Another 60 agents are assigned part-time or as needed to support the 56 JTTFs around the country.

Through a combined effort of the OIG DoD, the Defense Criminal Investigative Organizations, and other DoD Components, and coordination with the FBI Counter-terrorism Unit, the OIG DoD developed a list of Potential Indicators of Terrorist Threats. The brochure is being distributed to the DoD investigative and law enforcement community, but the information is also useful to everyone and reminds us to be alert to potential threats and to report them to appropriate authorities. The brochure is included as Appendix A of this report and has been posted to the internet: <http://www.dodig.osd.mil/PressReleaes/Brochure-BiFold.pdf>.





The OIG Defense Hotline has designed and procured posters and business cards that identify the DoD Hotline as a vehicle for individuals to report instances of threats to homeland security and unauthorized disclosures of classified information. To better assume this mission, the Hotline staff received intelligence-specific training from subject matter experts from within and outside the DoD. Several members of the Hotline staff have coordinated with Federal agencies outside the DoD to properly manage information obtained through one of the Hotline mediums.

A former civilian contract employee with the U.S. Army at Fort Monmouth, New Jersey, was sentenced to 210 months in prison, 36 months of supervised release, and ordered to pay a \$300 special assessment for violating the Federal Firearms Act and fraudulently using a social security number. The former employee, using fraudulent identification, purchased semi-automatic handguns in Virginia, Tennessee, and West Virginia. He also sent fictitious faxes threatening terrorist attacks on Fort Monmouth, a municipal court judge, and a number of local police officers. The sentencing judge found that the employee’s activity constituted an act of terrorism that warranted long-term incarceration.

**Financial Crimes**

Offenses considered to be financial crimes generally involve contract mischarging or defrauding DoD pay systems.

A major Defense contractor in Falls Church, Virginia, agreed to a civil settlement and paid the government \$530,000 to settle claims that it overcharged the DoD. Between October 1, 1998 and November 19, 2001, the contractor billed the National Imagery and Mapping Agency (NIMA), Bethesda, Maryland, for information technology services it provided to NIMA under contract. An investigation revealed that approximately 23 employees working on the contract did not meet the minimum qualifications for their positions. Consequently, the contractor charged and billed NIMA a higher hourly rate for the employees than was allowed.

A Defense contractor paid \$310,000 in damages as part of a civil settlement agreement with the government. In addition, the contractor agreed to remedy potential areas of ordnance and explosive contamination identified by the government's investigation relating to a contract for the removal of ordnance and explosives from land at Bellows Air Force Station (BAFS), Waimanalo, Hawaii. It was alleged that the contractor failed to properly clear the ordnance and explosives, and improperly used heavy equipment for grading purposes. An investigation determined that heavy equipment was used extensively throughout the BAFS site to grade areas before the use of metal detection equipment by contractor personnel. This compromised areas of the project by burying the ordnance and explosives beneath the clearance depth specified in the contract.

A home health care worker in Fredericksburg, Virginia, pled guilty to a single count of theft of government funds and was sentenced to 5 years probation and ordered to pay \$19,553 restitution and a \$100 special assessment fee. An investigation revealed the individual completed and submitted multiple fraudulent Certificates of Eligibility for Government Annuity payments originally payable to her deceased mother, a beneficiary of a Military Service member. The Defense Finance and Accounting Service Operation Mongoose, which is designed to detect ineligible beneficiaries of government funds, provided the initial fraud alert.

An administrative assistant with the Pentagon Force Protection Agency (PFPA), the civilian police force at the Pentagon, pled guilty to making a false claim to the government and was sentenced to 36 months supervised probation and ordered to pay full restitution of \$40,123. From January 1997 through December 2000, this employee claimed compensation totaling \$41,123.81 for overtime hours she did not work. The employee

would project overtime and weekend hours to work in advance of the pay period, submit the hours to the PFPA Records and Compensation Section, not work the projected overtime, and improperly collect the overtime pay.

A major defense contractor in Florida paid \$343,500 in a civil settlement to resolve a former employee's claim that the contractor supplied the Air Force with 30 Automated Depot Inertial Navigation Test Set Stations that did not comply with contract specifications. The contractor substituted non-approved parts, falsified test and inspection reports, and mischarged direct costs. The former employee had filed a *qui tam* and received \$68,700 of the settlement.

Information contained in a voluntary disclosure led to an investigation of mischarging on DoD contracts by a Top 100 defense contractor. The contractor purchased a company that charged costs related to firm fixed price contracts to Independent Research and Development, resulting in additional subsidy from the government. The contractor agreed to pay the United States \$2.8 million to settle its civil liability.

A Seattle shipyards company employee was sentenced to 6 months confinement with 3 years probation and ordered to pay \$147,000 in restitution after pleading guilty in U.S. District Court to filing false claims against the Department of Defense. The employee created a bogus company and then submitted five purchase orders for work not performed. Investigators discovered that the account number on the back of the checks payable to the bogus company was the same as that of the employee's personal bank account.

Two civilian employees assigned to an Army military medical center in Texas, who are also retired military officers, pled guilty in Federal District Court to conflict of interest and conspiracy charges. The employees shared a limited partnership with a medical contracting firm and received kickbacks after requesting \$505,626 worth of medical supplies through a sole source contract with the firm. Both employees were ordered to pay \$36,035 each in restitution and sentenced to 3 years probation.

Two civilian employees and the owner of a distributing company pled guilty in Federal District Court to theft, conspiracy, receiving kickbacks, and bribery charges. One of the civilian employees agreed to purchase tools and other items from the contractor. The employee would alter the quoted price on the legitimate Bill of Materials or prepare a fraudulent Bill of Materials and then make the purchases using his government

purchase card. The second employee received approximately \$3,000 in bribes in exchange for suggesting the company as a source of supply. The company owner paid \$50,000 in restitution as a result of a plea bargain and was sentenced to 3 years probation to include 4 months home confinement and 100 hours of community service. The employee who placed the contracts was sentenced to 3 years probation, 4 months home confinement, fined \$5,000, ordered to perform 100 hours of community service, and forbidden to apply for credit during the next 3 years. Sentencing of the second employee is pending.

### **Government Purchase Card Crimes**

The Military Criminal Investigative Organizations (MCIOs) continue their investigations into the illegal use and misuse of government issued purchase and travel cards.

A Navy enlisted person was found guilty at a general court-martial of five specifications of stealing. The member used his government issued purchase card for personal transactions to include the purchase of an airline ticket to Puerto Rico, hotel rooms, rental cars, and car towing services for his personal vehicle. Sentencing included a reduction in rank, a \$5000 fine, 1-year confinement, and a Bad Conduct Discharge. Pursuant to a pre-trial agreement, the member will pay \$5,900 in restitution in lieu of a fine and serve only 60 days confinement. Total loss to the government was \$32,723.

A Navy Petty Officer Second Class, who was the government purchase cardholder for his command's supply office pled guilty at a general court-martial to theft of government property by illegal use of a government purchase card. He was sentenced to 2 years confinement, fined \$12,000 and awarded a Bad Conduct Discharge. Total loss to the government was \$81,000.

A Navy enlisted person was sentenced by court-martial to 24 months confinement, reduced in pay grade, and given a Bad Conduct Discharge for theft of government property. The military member used credit cards assigned to a maintenance activity to purchase \$71,000 worth of property that he distributed to civilian and military personnel.

### **Medical Fraud**

Efforts to combat fraud against TRICARE and other government health care programs resulted in many successes during this 6-month period. The following sample cases were jointly investigated by multiple federal law enforcement agencies, and the recovered amounts will be apportioned among the agencies' programs that were victimized, including the DoD.

A dentist from Freehold, New Jersey, pled guilty to health care fraud and income tax evasion and was sentenced to 27 months in prison, 3 years probation, and restitution of \$264,363, in July 2002. Since early 1994, the dentist routinely billed the DoD TRICARE program and private dental insurance programs for services he did not provide. To conceal this, he made false notes in patients' files and falsely reported patients' addresses to insurance providers, thereby causing the dental explanation of benefits forms to be diverted to him.

Two former owners of a blood testing laboratory in Carmel, Indiana, pled guilty to health care fraud, mail fraud, and conspiracy and were sentenced to 23 and 29 months confinement respectively, 3 years supervised release, and each was ordered to pay \$2 million in restitution and a \$100,000 fine for submitting false claims to government health benefits programs, including TRICARE. The false claims included billing for tests that were not medically necessary and not ordered by doctors, and billing patients who were not seen by doctors.

A major pharmacy agreed to a \$9 million civil settlement to resolve allegations of making false claims, receiving unjust enrichment, and breach of contract with respect to payment of prescription medication claims to the TRICARE, Medicaid, and Federal Employees Health Benefits Programs. An investigation was initiated based on allegations that the pharmacy defrauded the government by filing false claims for prescription payments. The investigation identified numerous instances in which the pharmacy was unable to completely fill the prescription presented by the patient, and the patient was instructed to return at a later date for the balance. When a patient did not return for the balance, the prescription drug was returned to stock or resold to other customers; however, the pharmacy did not credit the government program account for the cost of the portion not provided to the patient.

A health care facility in Sacramento, California, entered into an \$8.5 million settlement agreement with the Department of Justice as a result of a *qui tam* civil lawsuit. It was alleged the facility defrauded the DoD TRICARE program and Medicare program by filing false cost reports for fiscal years 1991 through 1999. One of the aspects of the fraud was the inclusion of unallowed square footage of unused hospital space in its annual cost reports submitted to the government.

A physician was convicted of 33 counts of health care fraud, 7 counts of mail fraud and 3 counts of perjury and was sentenced in U.S. District Court, Kansas City, Kansas, to 72 months incarceration, 36 months of

supervised probation on release and ordered to pay a \$4,300 special assessment. The physician also agreed to a 15-year exclusion from Medicare, TRICARE, Medicaid, and all Federal health benefits programs. Testimony at trial established that the physician defrauded Federal and private health care benefits programs and illegally enriched himself by submitting false claims for services. The scheme to defraud included subjecting TRICARE patients and others to unnecessary surgery, billing for multiple complex surgical procedures he did not perform, and falsifying tests to justify unnecessary surgeries.

A dialysis service agreed to pay a civil settlement of \$1,658,923 to settle allegations of fraud. An investigation disclosed that the dialysis service billed Federal health care programs, including TRICARE, for Epogen (EPO). The dialysis service received EPO free of charge for use in a clinical study approved by the Food and Drug Administration.

### **Product Substitution**

Counterfeit materials, and other forms of unauthorized substitution of products into DoD inventories, are one of our highest priorities for deterrence, investigation and prosecution.

A Defense contractor in Newington, Connecticut, reached a \$150,000 settlement with the Department of Justice to settle issues raised in a *qui tam* suit. The suit alleged that the contractor knowingly falsified test documents pertaining to aerospace parts, including parts used in military aircraft. The scheme involved balancing operations that were to be performed by a certified balancing operator. When the in-house certified inspector was disabled due to injury, the contractor continued to certify parts by using a balancing trainee. Test documents were then prepared using the inspection stamp of the injured certified balancer.

The president of an aviation company in Fort Lauderdale, Florida, was sentenced to 12 months confinement, 24 months probation, restitution of \$19,100, a \$10,000 fine, and a \$100 special assessment fee. The president pled guilty to one count of fraud involving aircraft or space vehicle parts, covered by a newly enacted law. The law was specifically enacted to combat the dangers posed by the installation of defective parts in civil, public, and military aircraft. It contains enhanced criminal penalties. This is the first time a DoD contractor was successfully prosecuted under this law. The president certified repairs by using the Federal Aviation Administration license number of a company in Farmingdale, New York, knowing that his company was not approved to repair any aircraft part. The investigation further determined the president certified that printed

circuit boards were replaced when a subsequent report disclosed that the original printed circuit boards were still being used.

The former president of a manufacturing company in Ronkonkoma, New York, was sentenced to 2 years probation and a \$100 special assessment fee. In addition, the company was sentenced to 2 years probation, a \$400 special assessment fee, and a \$31,199 fine. The president and company pled guilty to one count of mail fraud. The company manufactures various aircraft components for the DoD and the commercial aircraft industry, including critical products for the F-14, F-15, and F-16 fighter aircraft. An investigation disclosed that the president falsely certified that aircraft components passed dimensional inspection requirements when, in fact, such products were not inspected or had failed inspection. These parts were also sold to commercial aircraft companies.

A manufacturing company in Tulsa, Oklahoma, was sentenced to 5 years probation and ordered to pay \$251,722 in fines, \$68,048 in restitution, and an \$800 special assessment fee. The company pled guilty to two counts of making false statements to the government. The charges resulted from the production of nonconforming spoiler-actuator attachment fittings for the Teledyne Ryan Aerospace Tier II+ Global Hawk, an unmanned reconnaissance aircraft. The company also produced nonconforming battery guides for operational use in the Space Station.

## **Environmental Crimes**

Investigations in this area address matters such as the removal, transport, and disposal of hazardous material from DoD installations and contractors.

The owner of a hazardous waste disposal company in Kansas City, Kansas, pled guilty to making a false statement and was sentenced to 3 years probation, ordered to pay a \$2,500 fine, and assessed a \$100 special assessment fee. The disposal company, a DoD subcontractor, stored hazardous waste without a permit. The owner misrepresented this fact to the Environmental Protection Agency.

The owner of an erosion control company pled guilty to 16 counts of making false claims to the State of Oklahoma and was sentenced to serve 60 days in the county jail, to pay \$350 per month restitution for 27 years, and received a 32-year suspended sentence. In conjunction with a U.S. Army Corps of Engineers project, the company installed river erosion control devices using a mattress of waste tires. An investigation determined that the owner falsified the number of waste tires on the manifests he submitted.

The owner of a non-hazardous waste disposal company and the company pled guilty to making false statements under the Clean Water Act. The company was sentenced to 5 years probation, a \$400 special assessment, and ordered to pay restitution of \$871,366. The president was sentenced to 9 months home detention, 1 year probation, and ordered to pay a \$10,000 fine and a \$100 special assessment. The company and president admitted submitting false Industrial Wastes Discharge Self Monitoring and Certification Forms for wastewater discharged into a U.S. Army Corps of Engineers managed waterway.

An asbestos removal company, its president and vice-president pled guilty to making false statements and possessing false documents in connection with DoD and other government contracts. The company was sentenced to 1 year probation, a \$100,000 fine, and ordered to pay \$30,000 restitution and an \$800 special assessment. The president and vice-president were each sentenced to 1 year probation, 6 months home confinement, ordered to each pay a \$50,000 fine and a \$200 special assessment fee. The investigation was based on information that the company obtained false asbestos training certifications for some of their employees and used those certifications to obtain licenses from the Virginia Department of Professional and Occupational Regulations. The company then submitted the false training certifications and licenses as part of their proposals on contracts with the DoD Pentagon Renovation Project and the District of Columbia Public Schools Asbestos Abatement Response Action for the U.S. Army Corps of Engineers.

A California portable services Navy contractor was sentenced to 3 years probation, fined \$100,000, and ordered to pay \$10,220 in restitution to the City of San Diego Metropolitan Wastewater Department for illegally dumping grease and septic waste at various San Diego County locations. This investigation was prompted by information received through the San Diego Environmental Task Force. According to the terms of a plea agreement, the company is prohibited from contracting with the government until the Environmental Protection Agency determines that conditions that caused the illegal activity have been corrected.

## **Bribery and Kickbacks**

The Anti-Kickback Act of 1986 addresses government employees and contractors who engage in bribery and kickbacks in exchange for government contracts and subcontracts.

The former manager of a DoD contractor in Tacoma, Washington, pled guilty to accepting kickbacks and was sentenced to 1 month incarceration, 5 months home confinement, 3 years probation, \$50,000 restitution and a



\$100 special assessment. An investigation disclosed that from May 1997 through December 1998, the manager, a prime contractor employee, accepted kickbacks totaling \$50,000 from a subcontractor. In return for the kickbacks, the subcontractor received favorable treatment in the award of government subcontracts from the prime contractor.

The two owners of a subcontractor in Chalmette, Louisiana, pled guilty to providing kickbacks and were sentenced to 6 months in a halfway house, 5 years probation, ordered to pay \$60,000 restitution to the Navy Military Sealift Command, and a \$200 special assessment fee for violating the Anti-Kickback Act. The owners paid kickbacks to the employee of a government prime contractor in exchange for favorable treatment in the awarding of subcontracts for repair work aboard U.S. naval ships.

## **Theft**

Theft of DoD material and munitions from the supply system and at the base level has a direct effect on the military operational readiness. Another vulnerability is theft of funds and property using government charge cards.

A contractor from Mapleville, Rhode Island, agreed to pay \$12,100,890 as part of a civil settlement resulting from the theft of precious metals being recovered under DoD contracts. Additionally, several key officers of the company were convicted of conspiracy and false statements and were sentenced to varying lengths of confinement, and all were ordered to pay substantial fines. Various schemes were devised that resulted in the theft of precious metals from a DoD contractor and its commercial customers. Diversion of these metals generated cash that was used, in part, to pay kickbacks to a DoD contractor employee. The kickbacks were made in return for favorable settlements relative to the processing of precious metals scrap.

The owner of a Federal Aviation Administration certified repair station in Millington, Tennessee, pled guilty to wire fraud and money laundering and was sentenced to 6 months in prison, followed by 6 months house arrest, 3 years supervised release, and a forfeiture of \$165,108. An investigation disclosed that this individual fraudulently obtained DoD property, including aircraft and aircraft parts and components, and converted the property to his own use. He fraudulently represented that the property would be used by State and local law enforcement agencies. Acting on behalf of the Mississippi County Sheriff's Department (MCSD), Osceola, Arkansas, he obtained helicopters and helicopter spare parts in excess of those needed to maintain and operate the MCSD's helicopter. He subsequently sold some of the parts for his personal benefit.

A former quality assurance representative (QAR) for the Defense Contract Management Agency, Pittsburgh, Pennsylvania, pled guilty to making false claims against the government and was sentenced to 63 months incarceration, 3 years supervised release, ordered to pay \$1,553,320 to the Department of the Army along with a \$900 special assessment fee. The false claims relate to a contract between a prime contractor and the U.S. Army for the disposal of military munitions fuses through demilitarization. The QAR entered into an agreement with various contractor officials to accept the false certifications to allow the contractor to be paid for the certification work when the QAR knew the fuses had not been demilitarized. The prime contractor subsequently submitted false claims to the DoD based on the false certifications and was paid approximately \$346,630. It will cost the Army an estimated \$1.5 million to make these fuses safe.

A former director of the Defense Automated Printing Service, New Orleans, Louisiana, was sentenced to 30 months confinement, 3 years supervised release, restitution of \$581,997 and a \$100 special assessment fee for theft of government funds. The former director used his privately owned business to make \$310,410 in fraudulent charges to government charge cards held by his subordinates. In addition, he embezzled \$271,587 in government funds by allowing other businesses to make fictitious charges to the government charge cards and then dividing the proceeds with him.

An individual from California was sentenced to 27 months confinement, 24 months supervised release and a special assessment of \$100 for his role in the attempted theft of \$1.6 million in gold from a Massachusetts company. An individual who identified himself as a DoD employee contacted a manufacturer of precious metals in order to purchase gold for use on the space shuttle. The individual provided the manufacturer with documents reported to be DoD requisition forms. The individual was arrested when he attempted to take possession of the gold.

## **Computer Crimes**

Criminal activity in the cyber environment continues to grow, with viruses, denial of service attacks, and hacker attacks being the most notorious crimes. Easy access to the Internet led to another type of computer crime--accessing child pornography using DoD computers. Such pornography is often discovered while examining DoD computers for evidence in other criminal matters or is detected and reported by network administrators.

An individual from Matawan, New Jersey, was sentenced to 20 months incarceration, 3 years probation, a \$5,000 fine and a \$100 special assessment fee for knowingly transmitting a computer virus. A joint federal investigation revealed that this individual created the “Melissa” computer virus and knowingly transmitted it over the Internet on March 26, 1999. “Melissa,” which is a Microsoft Word macro virus, propagates over the Internet by using the e-mail programs of computers it has infected. The investigation found that by subverting e-mail in this manner, the virus overloaded and caused the shutdown of the computer networks of numerous major corporations and government agencies, including the DoD. “Melissa” cost the DoD in excess of 33,000 work hours.

A U.S. Army private first class (PFC) stationed at Fort Sam Houston, Texas, was sentenced in U.S. District Court, Eastern District of Virginia, to 27 months incarceration, 24 months supervised release, and ordered to pay a \$100 special assessment for possession of child pornography. In March 2001, Network Solutions notified the Herndon Police Department, Herndon, Virginia, that it had discovered images of child pornography on a computer belonging to an employee during routine network maintenance. This information was passed on to a Crimes Against Children Federal Task Force sponsored by the Federal Bureau of Investigation (FBI) in the Washington metropolitan area. In May 2001, this individual enlisted in the U.S. Army. Subsequent investigation revealed that the PFC possessed over 300 pornographic images of children on his work and home computers.

A PFC stationed at U.S. Army, Fort Myer, Virginia, was sentenced in U.S. District Court, Eastern District of Virginia, to 27 months incarceration, 3 years supervised release and ordered to pay a \$200 special assessment for interstate transportation of obscene matters and possession of child pornography. The PFC admitted logging into an Internet chat room from his barracks room on Fort Myer and receiving and distributing images of child pornography. He also admitted to knowingly receiving and viewing approximately 75 images of child pornography that were recovered from a computer seized from his residence in January 2002.

### **Recent Management Actions**

In July 2002, the Inspector General requested that the Deputy Assistant Inspector General for Criminal Investigative Policy and Oversight (CIPO) develop a single process for handling OIG subpoenas requested by the Military Criminal Investigative Organizations (MCIOs) and the Defense Criminal Investigative Service (DCIS). The new process, which centralizes subpoena processing within CIPO, avoids duplication, eliminates

horizontal and vertical levels of review, and ensures efficiency and consistency in operations.

Following the events of September 11, 2001, CIPO formed the Enduring Freedom Support Group (EFSG), consisting of senior CIPO, DCIS, MCIO, and law enforcement organization policy experts. At quarterly meetings, the EFSG addresses emerging issues faced by the DoD criminal investigative and law enforcement community, seeking to concentrate resources in areas that provide the greatest assistance to the DoD. Through the EFSG, CIPO strives to reduce barriers, develop strategies, and forward or coordinate major areas of concern facing the law enforcement community. Notable accomplishments have been the coordination of civilian arrest authority implementation; broadened application of investigative authorities; implementation of new subpoena processes; elimination of outdated regulatory requirements; and coordination on new language for significant policy issuances.

On June 21, 2002, the Inspector General issued DoD Instruction 5505.3, "Initiation of Investigations by Military Criminal Investigative Organizations." The Instruction updates responsibilities and procedures to ensure the independence, objectivity, and effectiveness of the MCIOs, while ensuring that criminal allegations or suspected criminal allegations are referred promptly to the appropriate MCIO or law enforcement organization.

## **CRIMINAL INVESTIGATIVE POLICY AND OVERSIGHT**

The Office of Criminal Investigative Policy and Oversight issued two evaluations reports during this period: *Evaluation of the Policies and Practices for the Utilization of DNA Technology within the Military Criminal Investigative Organizations*, May 17, 2002; and *Evaluation of DoD Correctional Facility Compliance with Military Sex Offender Notification Requirements*, June 26, 2002.

The DNA report indicated that the MCIOs' use of DNA technology as an investigative tool has achieved effective results. The DNA technology helps solve crimes by identifying the perpetrators of violent crimes and by clearing blameless suspects. The report recommended improvements for submitting DNA evidence for analysis in unknown subject cases; for reducing the backlog of rape kits in unknown subject cases; for training to enhance agent awareness of DNA database capabilities; and for the use of certified forensic laboratories to ensure DNA evidence profiles are entered into the FBI forensic evidence index.

The military sex offender notification requirements report noted that while DoD has published guidance providing for sex offender notifications, the Services do not fully implement the guidance and generally do not meet the notification requirements. In addition, military confinement facilities frequently do not receive documentation alerting them to victim and witness notification requirements, and they do not always satisfy the requirements even when they receive the documentation. As a result, some victims and witnesses do not receive notifications from military confinement facilities when an inmate is released from confinement. The report recommended a number of management actions to improving the notification process.

### **VOLUNTARY DISCLOSURE PROGRAM**

The Voluntary Disclosure Program encourages contractors to disclose potential criminal or civil fraud that may affect their contractual relationship with the DoD or the contractor's responsibility under the Federal Acquisition Regulation. During this reporting period, the government recovered \$1.7 million in disclosure settlements and received three requests for admission to the program. Since its inception in 1986, the program has recovered more than \$420 million.

In one case during this reporting period, a company stated that it transferred costs from two firm fixed price contracts to its independent research and development accounts, thus increasing costs related to other contracts. In another case, a company reported that it failed to properly monitor certain contractually required activities. However, the company charged the government as though the monitoring activity was thoroughly accomplished.

### **ADMINISTRATIVE INVESTIGATIONS**

The OIG DoD Departmental Inquiries Office conducts investigations and also performs oversight of investigations conducted by the Military Departments. Those investigations pertain to:

- Allegations of reprisal against military members, Defense contractor employees, and nonappropriated fund employees.
- Allegations that military members were referred for mental health evaluations without being afforded the rights prescribed in the DoD Directive and Instruction pertaining to mental health evaluations of members of the armed forces.
- Noncriminal allegations against senior military and civilian officials.

**Whistleblower  
Reprisal Activity**

During the reporting period, the Special Inquiries Directorate and the Military Department Inspectors General received 249 complaints of whistleblower reprisal. During this period, 193 cases were closed. Of those, 157 were closed after preliminary analysis determined further investigation was not warranted and 36 were closed after full investigation.

Of the 36 cases closed after full investigation, 10 (28 percent) contained one or more substantiated allegations of whistleblower reprisal. These cases were referred to commanders and supervisors for corrective action.

**Examples of  
Substantiated  
Whistleblower  
Reprisal Cases**

An Army major rendered an unfavorable Officer Evaluation Report to a subordinate captain in reprisal for the captain's complaints to the chain of command, an IG, and the Equal Employment Opportunity office concerning discrimination and harassment by the major. The major received a letter of reprimand as a result of the discrimination and harassment disclosure. Corrective action regarding the substantiated reprisal finding is pending.

A Navy chaplain received a non-punitive Letter of Instruction and an adverse fitness report, and was relieved of his duties and detached for cause, in reprisal for reporting to his chain of command the inappropriate use of religious offering funds. Among the inappropriate uses reported was payment for a religious social gathering that featured an open bar for alcoholic beverages. The investigating officer recommended, and the higher command endorsed, the following corrective actions: that the adverse fitness report and detachment be expunged from the chaplain's official record; that he be reassigned to a position commensurate with his rank and experience; and additional measures be taken to restore the reputation and standing of the chaplain among his parishioners and the religious community.

An Army colonel, captain (company commander), and command sergeant major reprised against a sergeant first class (SFC) by recommending the downgrade of his award nomination because they believed he made a protected communication to a Member of Congress. The SFC (complainant) allowed another sergeant to use his home computer to send an email communication to a Member of Congress. When the ensuing congressional request for information was forwarded to the company commander, the supporting documentation showed the SFC's email address, causing responsible officials to believe the SFC made the protected communication. Corrective action is pending.

A Navy rear admiral and captain reprimanded against a Navy commander by issuing her an unfavorable fitness report because she complained about the discrimination of female officers to an IG inspection team. The Vice Chief of Naval Operations verbally admonished the rear admiral; the captain received a verbal counseling and a nonpunitive letter of caution.

**Referrals for Mental Health Evaluations**

Eighteen cases closed during the reporting period contained allegations of improper referrals of military members for mental health evaluations. In 12 of those cases, it was substantiated that commanders failed to follow the proper procedures for referring a Service member for a mental health evaluation under DoD Directive 6490.1, "Mental Health Evaluations of Members of the Armed Forces." We continue our efforts with Military Department IGs to improve commanders' knowledge of the Directive's requirements.

**Senior Official Inquiries**

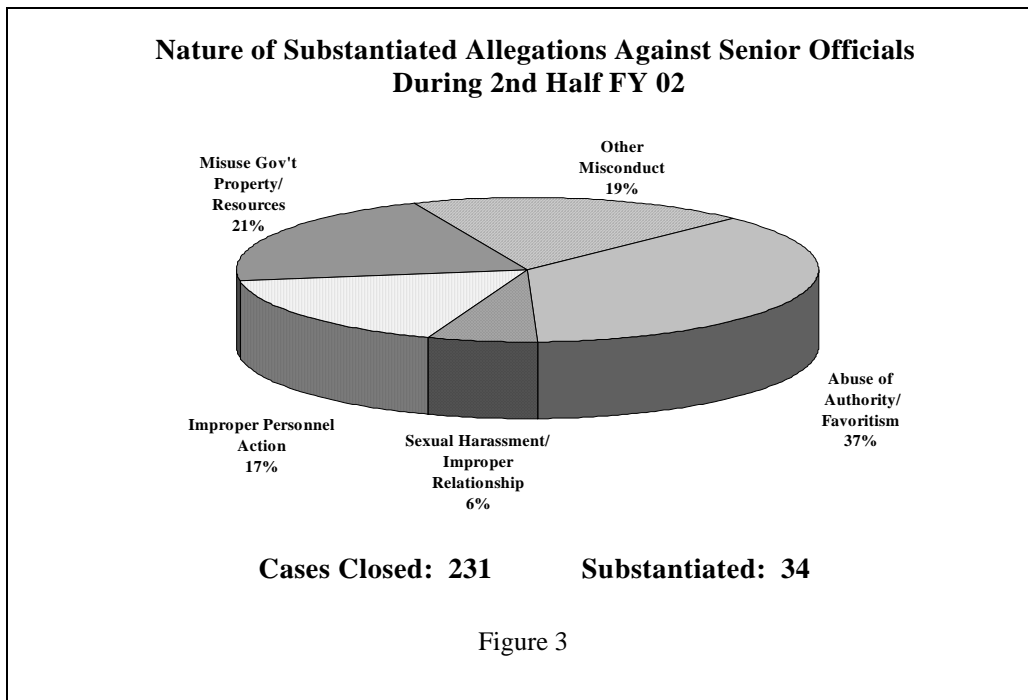
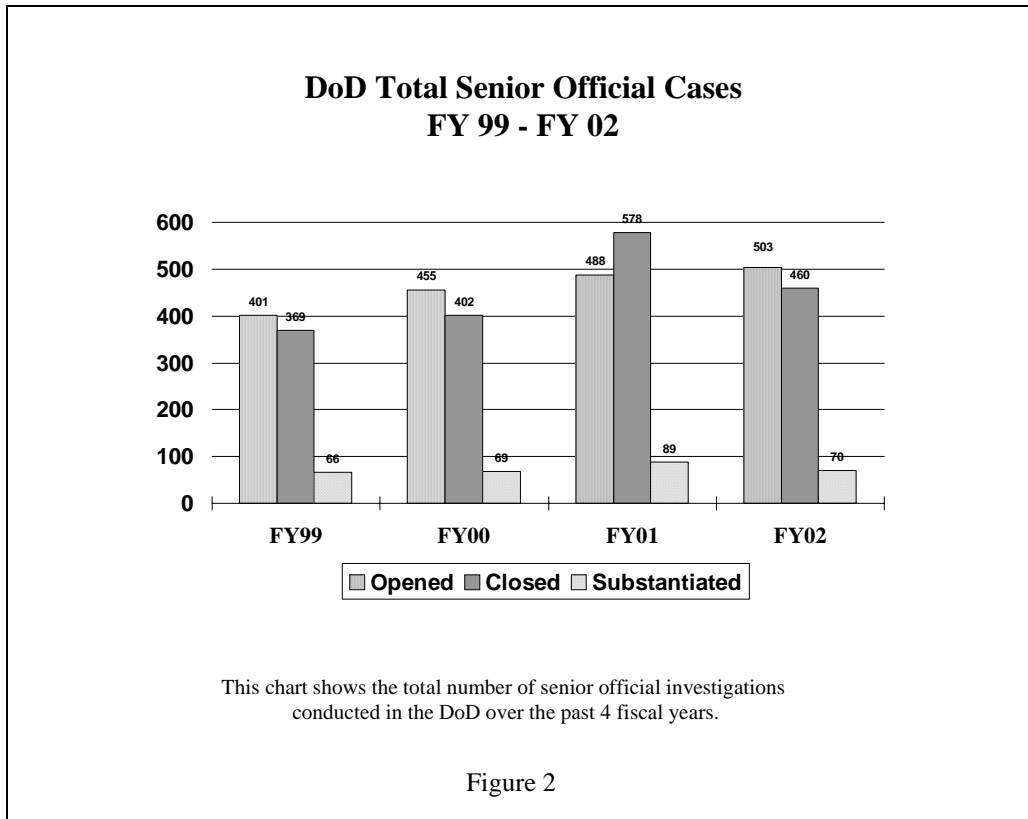
Figures 2 and 3 (page 18) show results of activity on senior official cases during the period. On September 30, 2002, there were 224 ongoing investigations into senior official misconduct throughout the Department, which represented a moderate increase from April 1, 2002, when we reported 195 open investigations. Over the past 6 months, the Department closed 231 senior official cases, of which 34 (15 percent) contained substantiated allegations.

**Examples of Cases Involving Senior Officials**

We substantiated allegations that a senior DoD official engaged in a leadership style that was inconsistent with applicable DoD guidelines, and which contributed, in part, to continuing management problems at the George C. Marshall Center for European Security Studies in Garmisch, Germany. The investigation was initiated in response to several complaints of mistreatment made by DoD personnel who were serving at the Marshall Center. Although we did not substantiate complaints of discrimination, reprisal, or gender discrimination, we determined that the senior official's conduct contributed to a persistent state of apprehension on the part of numerous employees at the Marshall Center.

In two separate investigations, we concluded that senior military officers allowed their enlisted aides to perform personal services in violation of DoD regulations that limit enlisted aide duties to those that are related to military and other official responsibilities. Unauthorized services included preparing and serving food at personal entertainment functions and maintaining a senior officer's personal vehicle.

In another case, we substantiated allegations that a senior DoD official accepted a reserved parking space in a government-leased building at a





price that was reduced by the parking vendor in deference to the official position held by the DoD employee. We concluded that the senior official's actions in the matter violated ethics regulations that prohibit the acceptance of gifts that are given because of official position. When advised of that conclusion, the senior official reimbursed the vendor over \$2,300.

We also examined allegations that improper influence tainted the results of a Navy Selection Board for promotion to rear admiral. We concluded that the board itself was conducted in accordance with statutory and regulatory guidance and that no board member was subjected to improper influence. However, we found that senior Navy officials disclosed proceedings of the Selection Board to persons who were not authorized to receive that information in violation of applicable DoD guidelines. Additionally we found that before the board convened, a senior Navy official released information from one candidate's record to another candidate in violation of the Privacy Act as implemented by DoD regulation. The results of the foregoing five investigations were provided to cognizant management officials for consideration of corrective action.

We also substantiated allegations that a senior DoD official improperly authorized a Navy installation to host a large convention sponsored by a major association. The convention, held in August 2000, caused military operations at the installation to be suspended for a period of 11 days and significantly interfered with the performance of official duties. We concluded that the Navy's hosting of the convention on this occasion violated regulations that govern DoD support to non-federal entities. We provided the results of our investigation to the Secretary of the Navy for consideration in evaluating future requests for support to non-federal entities, but we found insufficient basis to recommend further corrective action because we considered the event an isolated incident and the responsible DoD official left government service.

## AUDITING

The central audit offices of the DoD are the OIG DoD, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency. The organizations all together issued 228 reports, identifying the opportunity for \$1.4 billion in monetary benefits. Appendix B lists internal audit reports by issue area. Appendices C and D, respectively, list OIG DoD reports with potential monetary benefits and statistically summarize audit followup activity.

The Defense Contract Audit Agency (DCAA) provided financial advice to contracting officers in 22,790 reports issued during the period. Contract

auditing resulted in approximately \$3,234 million in questioned costs and funds put to better use. Further details are at Appendix E.

## **INFORMATION TECHNOLOGY MANAGEMENT**

The key to success on the modern battlefield and in internal business activities is the ability to produce, collect, process, and distribute information. Data must be accurate, timely, secure, and usable. The huge scale, unavoidable complexity, and dynamic nature of DoD activities make them heavily dependent on automated information technology. This dependence has proven to be a major challenge, because DoD management techniques have not kept pace with the continual growth in information user requirements and the shortened life spans of technologies before obsolescence.

Seventeen audits during the reporting period continued to indicate a wide range of management problems in systems selected for review. The important systems for which management improvements were recommended included the Defense Travel System, Preventive Health Care Application, Global Command and Control System, Computerized Accounts Payable System, and Military Airspace Management System. A \$452 million seat management contract for information technology services and equipment was cancelled as a failure this year because planning for the contract did not identify the return on investment, benefits, or prescribe performance measures.

## **INFORMATION SECURITY**

The information security threat to DoD systems and to other public and private sector systems on which national security depends is greater than ever. Its sources include foreign governments, terrorist groups, disgruntled government or contractor employees, vandals, criminals with financial motives, and mere curiosity seekers. This extraordinarily diverse population also has a wide variety of constantly improving techniques and tools at its disposal. The challenge to DoD is to minimize vulnerabilities without losing the advantages of open, interconnected systems with large numbers of users. Because of the constantly evolving threat and the sheer size of DoD information operations, the Department needs to be both highly flexible and systematic in its approach to information security. Although the DoD is a leader in many aspects of this complex problem, we continue to find a wide range of security weaknesses.

During the reporting period, the DoD audit community issued 14 reports on information security. Subtitle G, Government Information Security Reform, of Title X of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, Public Law 106-398, requires that each agency obtain an independent assessment of its security posture.

The OIG is required to evaluate the security posture based on an independently selected subset of information systems. A summary of the OIG review was provided to DoD for inclusion in the annual information security report to the OMB. The review assessed the accuracy of the data DoD used to report the security status for 560 information technology systems. The DoD reported invalid data on the security status of systems in 2001 for an estimated 370 systems. The OMB and DoD managers did not have dependable information to ascertain the degree to which information security controls exist in systems. Further, although the requirement for systems to obtain security certification and accreditation has existed since 1997, we estimate that only 101 of 560 systems met the requirement.

## **ACQUISITION**

No other organization in the world buys the amount and variety of goods and services such as those purchased by the DoD. In fiscal year 2001, the Department spent \$175 billion through contracts and other instruments, using about 19,000 transactions per day. There are about 1,500 weapon systems acquisition programs, valued at \$1.8 trillion over the collective lives of these programs. The amount spent to procure services, \$56 billion in fiscal year 2001, is increasing as DoD Components continue to expand outsourcing pursuant to the Federal Activities Inventory Reform Act of 1998 and the Presidential Management Initiative on Competitive Sourcing. The management challenge is, despite this huge scale, to provide materiel and services that are superior in performance, high in quality, sufficient in quantity, and reasonable in cost.

During the reporting period, the DoD audit community issued 49 reports that addressed a range of continuing acquisition issues. There has been particular concern over the past two decades about the length of the acquisition cycle and the high per unit cost of weapon systems. For example, the V-22 Advanced Tiltrotor Aircraft (Osprey) has been under development since 1981, and the currently estimated production cost is \$65 million per plane. Despite years of development, we reported that the V-22 hydraulics system performed at reliability rates significantly lower than predicted. Other audits have continued to reveal the lack of competition for service contracts. One report identified where the Navy exceeded the 5-year regulatory time limit for \$1 billion of environmental service contracts and thus did not benefit from re-competing the requirements. Abuse of the \$9.7 billion charge card programs recently emerged as another special concern and there were 12 reports issued about controls for charge cards. The Department convened a special task force that included OIG auditors and investigators and issued a report calling for

additional controls and instituting new policies of zero tolerance for abuse of credit cards.

Requirements computations and pricing continue as problems for spare parts. A report on the Defense Logistics Agency aviation investment program identified spare parts purchases that exceeded program performance requirements. Acquisition audits provided continued indications that many of the acquisition reforms initiated over the past few years have not been fully or effectively implemented, often because the acquisition workforce is both under staffed and under trained. Senior managers at the OIG believe that problems in the acquisition area are due largely to mismatches between requirements and available funding, inadequate internal management information systems, and the relatively low priority given to improvement in contracting for services until very recently.

## **CHEMICAL AND BIOLOGICAL DEFENSE**

The proliferation of biological and chemical technology and material has provided potential adversaries with the means to challenge directly the safety and security of the United States and our military. The anthrax letters sent last fall made manifest the danger of terrorists armed with biological weapons. The probability of military personnel encountering chemical and biological agents remains high. The Chemical and Biological Defense program is to ensure that military personnel are the best equipped and best prepared forces in the world for operating in battle space that may feature chemically and biologically contaminated environments.

The OIG has continued its strong presence in ensuring adequate oversight of chemical and biological defense issues. Since we started working on this issue in 1994, the Department has made great strides in improving the quality of chemical and biological defense equipment, the individual and unit training, and equipping military units. However, additional improvements are needed. The OIG reported on problems with the logistics and maintenance of chemical and biological protective equipment in the European Command and Central Command, acquisition of the chemical agent detector and controls at DoD laboratories, and medical facilities that use and ship biological agents. The Army Audit Agency reported on the need to improve unit-level training for chemical and biological defense and provide additional support for chemical and biological defense to forward stationed DoD civilians and contractors..

## **QUALITY ASSURANCE**

It is vital that the DoD quality assurance programs ensure that the products delivered to our warfighters are of the highest quality. Recent

reviews have shown that reductions in personnel and funds adversely affected the quality assurance programs.

The Defense Logistics Agency Quality Manufacturer's List and Quality Products List Program aim to increase product quality and reliability and buying productivity, and to enhance logistics management operations by establishing a list of vendors that received manufacturing line audits and are certified as providing high quality critical items. An OIG report showed that 42 percent of the audits were not accomplished for 1,196 vendors manufacturing lines needing certification. Some certifications were 8 years overdue. A lack of staff to perform the audits and certifications resulted in a higher risk of receiving nonconforming parts. Similarly, a lack of staff for the Navy Product Quality Deficiency Program resulted in as many as 1.4 million potentially nonconforming items in the inventory. Another report identified where the Navy and Defense Logistics Agency failure to enforce contract specifications resulting in the purchases of \$12 million of mattresses for ships that were not fire resistant.

#### **COOPERATIVE THREAT REDUCTION PROGRAM**

The Cooperative Threat Reduction Program was initiated to reduce the threat posed by weapons of mass destruction in the former Soviet Union. Under the program, the United States provides funds to build facilities and operate programs to safeguard, transport, and ultimately destroy chemical and nuclear weapons. Adequate controls for the program are vital to ensuring that the limited program funds are used effectively. However, a review showed that a recently completed \$95 million facility in Siberia for converting rocket fuel to nonmilitary purposes now sits idle because Russia used the rocket fuel for its commercial space program. Because of a lack of written agreement to provide the rocket fuel and inadequate inspections, the DoD was unaware that Russia diverted the rocket fuel for other purposes.

#### **WEB SITE MANAGEMENT**

The heads of DoD Components are responsible for establishing a process to identify appropriate information for posting to web sites and to review all information placed on publicly accessible web sites for security levels of sensitivity before the information is released. The Component heads are also responsible for management oversight, resource support, and annual security assessment of their web sites.

OIG reports on web site management identified a lack of attention to information made available to the public and inadequate oversight of the programs. The Army's publicly assessable web sites contained inappropriate information, which was inconsistent with Army web policy.

Between April and September 2001, the Joint Web Site Assessment Cell identified and reported to DoD web site owners, 200 disclosures of inappropriate information that were available for public viewing. As of May 2002, 30 of the 200 disclosures remained available for public viewing.

## **SIGNIFICANT OPEN RECOMMEN- DATIONS**

Managers accepted or proposed acceptable alternatives for 708 (97 percent) of the 731 OIG DoD audit recommendations made during fiscal year 2002. Many recommendations require complex and time-consuming actions, but managers are expected to make reasonable efforts to comply with agreed-upon implementation schedules. Although most of the 1,222 open actions being tracked in the OIG DoD follow-up systems are on track for timely implementation, there were 226 reports over 12 months old, dating back as far as 1991, for which management has not completed actions to implement the recommended improvements.<sup>1/</sup>

We are concerned that DoD was not benefiting from the recommended improvements and was not meeting the intent of the Inspector General Act to complete corrective actions within 12 months. To accelerate implementation of the corrective actions, the Inspector General recently wrote to each Component head responsible for the delinquent recommendation and requested their assistance in completing the needed actions.

Significant open recommendations that have yet to be implemented include the following:

- Recommendations made in 1997 for a detailed methodology to be developed for cross-organizational and cross-functional coordination of DoD Joint Technical Architecture implementation plans for information technology systems.
- Recommendations made in 1999 for better monitoring of leased commercial satellite capacity to enable more intensive planning

---

1. Section 6009 of the Federal Acquisition Streamlining Act, as amended, provides: "If the head of the agency fails to complete final action with regard to a management decision within the 12-month period, the inspector general concerned shall identify the matter in each of the inspector general's semiannual reports pursuant to section 5(a)(3) of the Inspector General Act of 1978 (5 U.S.C. App.) until final action on the management decision is completed." A list of OIG reports on which management decisions have been made but final action has not been taken is contained in the Secretary of Defense Report issued pursuant to section 5(b) of the Inspector General Act.

for various scenarios requiring mixes of DoD-owned and commercial satellite support.

- Recommendations made in 1999 to update, clarify, and standardize policy to define security requirements, especially those pertaining to identification and authentication in order to provide more consistency in the Defense Information Assurance Program.
- Recommendations made in 2000 to implement a process for prioritizing security clearance requests to improve the efficiency of the DoD personnel security clearance investigative efforts.

## **OIG DOD TESTIMONY**

On June 4, 2002, Inspector General Joseph E. Schmitz, accompanied by Deputy Inspector General Robert J. Lieberman, testified before the House Government Reform Subcommittee on National Security, Veterans' Affairs and International Relations at a hearing entitled, "Transforming Defense Financial Management: A Strategy for Change." The Inspector General testified that based on audit opinions of fiscal year 2001 DoD financial statements, the Office of Inspector General was unable to report progress for the DoD-wide financial statement or for major component funds. The OIG DoD issued an unqualified (clean) opinion for the Military Retirement Fund's statement; however, disclaimers of opinion were necessary for all other major funds.

For several years, the OIG DoD has reported that the lack of adequate financial reporting systems and a variety of internal control problems prevent those systems from being able to consistently produce either useful day-to-day financial information or commercial-type financial statements. The Department of Defense has taken a major step to transform financial management through a new effort to establish a comprehensive financial system architecture.

The Inspector General stated that the OIG would continue to support the Department's efforts to strengthen its financial systems by providing timely and useful audit advice as well as through proactive fraud prevention and detection efforts and the aggressive investigation of financial crimes.

## **INTELLIGENCE REVIEW**

See the Classified Annex to this report for summaries of the 80 intelligence-related and other sensitive reports.

This page left blank intentionally



## CHAPTER TWO - OFFICE OF THE INSPECTOR GENERAL TRANSFORMATION

On the one-year anniversary of Secretary of Defense Rumsfeld's "War on Bureaucracy," the Inspector General released the results of an independent assessment that points the way to a transformation of the Office of the Inspector General. The IG had commissioned the independent assessment as one of his first actions after being sworn into office on April 2, 2002, in the spirit of the Secretary's call on September 10, 2001, to reform wasteful processes and systems in Pentagon organization. The assessment team was assembled by Military Professional Resources, Incorporated, (MPRI) of Alexandria, Virginia, and was assigned the objective of conducting "an independent review to assess the overall effectiveness of the Office of Inspector General," including how the office "satisfies its legal, ethical, and oversight obligations within the Department of Defense."

The Assessment Team was composed of retired military personnel and attorneys with extensive Inspector General experience. Starting its 90-day assessment on April 21, 2002, the team conducted a "bottom-to-top" review that involved 316 individual interviews, 34 seminars with junior, middle, and senior grade staff that reached approximately 643 of the 1,257 employees, including visits to 26 field locations. The assessment included a not-for-attribution survey that received 527 voluntary written responses. The team made ten major recommendations ranging from ways to restructure and carry out the mission of the Inspector General to transforming and reinvigorating the internal ethical culture of both employees and senior management.

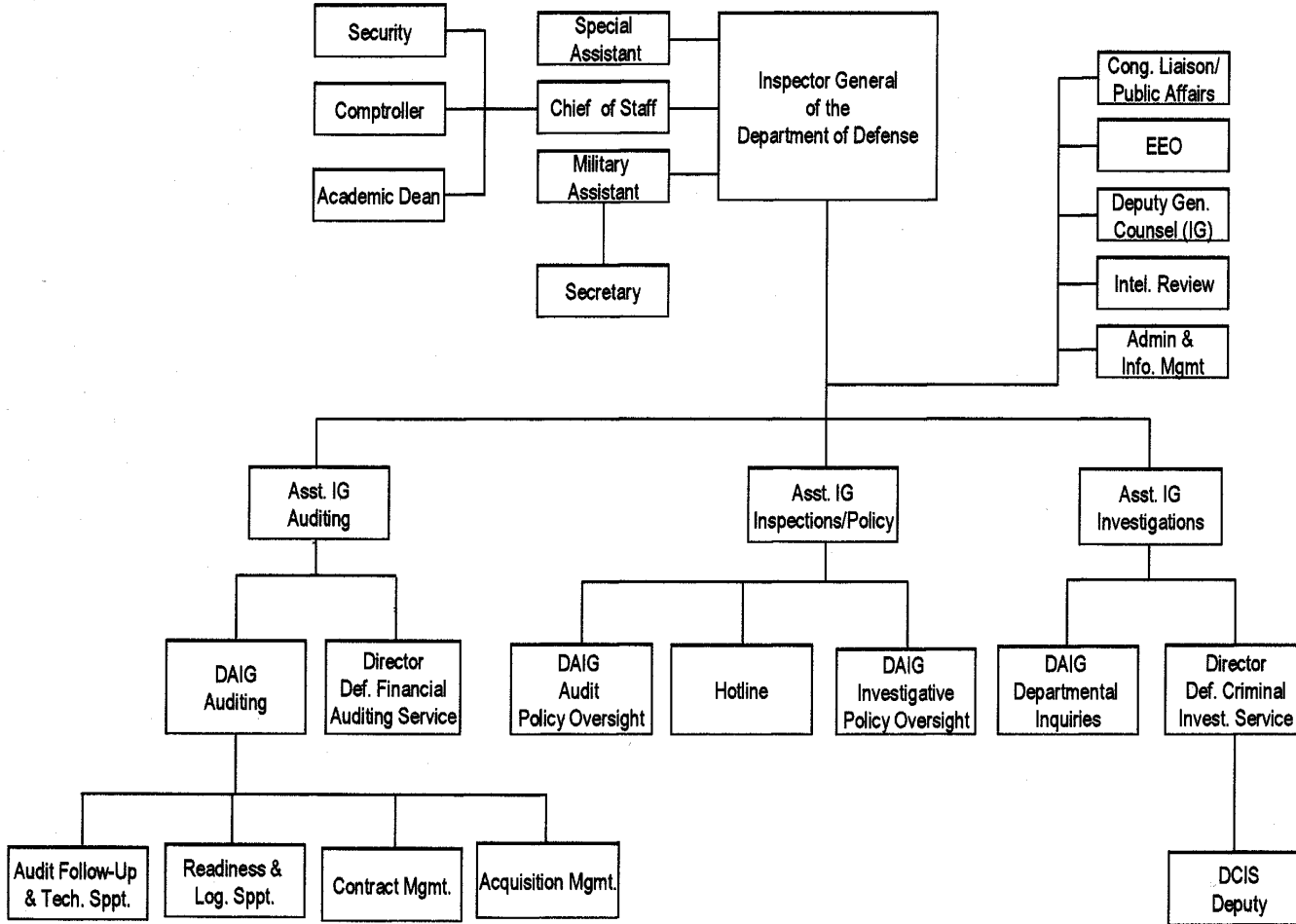
Ongoing efforts to transform the Office of the Inspector General have built upon many of the recommendations proposed by the assessment team as well as the IG's own observations gained after months of hands-on-experience in working with both the Department and the Congress. Phase I of the transformation effort includes eliminating a layer of management, creating a three "deputy structure" for greater organizational depth and improved continuity of operations, implementing unifying and transcending principles throughout the organization, establishing a new, dedicated public affairs function, creating an elite financial auditing service to provide the DoD with audited financial statements, and integrating three operational directorates including a new Assistant IG for Inspections and Policy. A planned Phase II of the transformation effort

will eliminate another layer of management and fully integrate the DoD IG Office of Intelligence Review. A future Phase III could include, among other things, a brick-and-mortar IG Academy, where only a "virtual academy" exists today.

In working to transform the Office, the IG has called to mind the applicability of the words of Secretary Rumsfeld's "War on Bureaucracy" speech one year ago: "Just as we must transform America's military capability to meet changing threats, we must transform the way the Department works and what it works on. We must build a Department where each of the dedicated people here can apply their immense talents to defend America, where they have the resources, information and freedom to perform."

A copy of the assessment team's report is available at [<https://intra.dodig.mil/fo/newsfromig/index.html>].

# OIG Organization



This page left blank intentionally

---

**APPENDIX A**  
**INDICATORS OF POTENTIAL TERRORIST THREATS**  
**OCTOBER 2002**

***Message from the Inspector General***

None of us will forget the horrific events of September 11, 2001, at the Pentagon and the New York World Trade Center. During those attacks and in their aftermath, we witnessed the remarkable efforts of our nation's law enforcement personnel to protect us and prevent future terrorist acts. We also witnessed the unification of Americans everywhere, as they resolutely supported efforts to combat terrorism.

We all play an important role as Department of Defense employees in contributing to the Force Protection mission and the effort to enhance Homeland Defense. In protecting the men and women of the Department of Defense, our facilities and programs, and other national assets, law enforcement personnel in particular need to be alert for activities that may be precursors to terrorist acts. DoD law enforcement personnel are especially well trained and disposed to provide this vigilance and are specifically guided by DoD Directive 5200.27.

To assist their efforts, we offer this listing of activities or conditions that may be "Indicators of Potential Terrorist Threats." The activities and conditions listed are by no means all-inclusive. Further, some activities may reflect innocent behavior or relate to other types of criminal behavior. However, we must be aware that even outwardly innocent activities may be part of a larger scheme with the ultimate goal of harming our people and resources and disrupting our vital mission of protecting our citizens and our way of life.

If you observe these activities/conditions or they are reported to you, you must share them immediately with other appropriate law enforcement or intelligence agencies.

Joseph E. Schmitz

## Suspicious activities near, on, or about Government buildings or installations

- > Theft of badges, credentials, ID cards, Government/military/emergency vehicles, military apparel, etc. Discovery of false identifications.
- > Photographing, sketching, or surveillance of military facilities.
- > Trespassing near key facilities, particularly by multiple persons.
- > Uncommon or abandoned vehicles, packages, or containers.
- > Person(s) observed searching trash containers or placing items in trash containers adjacent to a Government facility or residence of Government personnel.
- > Large thefts of sensitive military property such as computers and particularized deployment equipment (gas masks/cold weather gear).
- > Purchase through Government sales of military hardware with intent or indications to refurbish to working condition.
- > Purchase/attempted purchase, theft, or possession of large numbers of weapons or of heavy weapons.
- > Purchase/theft/possession of explosives or supplies necessary for the manufacture of explosive devices.
- > Increase in cyber attacks/probes.
- > Increase in the number of threats to Government facilities that require evacuation.
- > Theft of Government vehicles, vehicle passes, uniforms, or standard operating procedures.
- > Unknown workers trying to gain access to facilities for repairs, installation of equipment, etc.
- > E-mail attempting to obtain information regarding the facility, personnel, or operating procedures.
- > Unusual patterns of seemingly unimportant activity: patterns of travel (vehicle, foot, boat, air) or routes of travel that seem to serve no purpose may be used as a means to observe targeted individuals, activities, installations, or ports. For example, a boater who routinely passes along the Ft. Belvoir Potomac River waterfront, yet he is clearly not a fisherman, water skier, etc.
- > Individual's establishing businesses or roadside food stands adjacent or in proximity to Government facilities.
- > Unknown persons or occupied vehicles loitering in vicinity of a Government facility for an extended period of time.



---

## **Conversations about Government facilities, programs, or personnel**

- > Unknown persons attempting to gain information about facilities by engaging DoD personnel or their families in conversation.
- > Person(s) expressing support for the September 11, 2001, attacks.
- > Person(s) advocating violence against certain religious, racial, or ethnic groups.
- > Person(s) sympathetic to groups who advocate the violent overthrow of the U.S. Government.
- > Suspicious requests for purchase or lease of or training in potentially dangerous instrumentalities, e.g., airplanes, large trucks, underwater gear near naval installation.
- > Remarks threatening or potentially threatening Government personnel, facilities, and equipment.
- > Intrusive questions posed by strangers about personal information or information about Government duties and responsibilities.



## Delivery of suspicious mail, packages, or other items

- > Mail that has no return address.
- > Mail addressed only to title of prospective recipient or using an incorrect title.
- > Misspelled words or defective address.
- > Restrictive markings such as "confidential" or "personal for."
- > Excessive postage.
- > Stains, discoloration, oiliness, crystallization, or strange odor.
- > Abnormal size; excessive wrapping.
- > Wires, metal foil, or string protruding.
- > Unusually heavy or unbalanced.
- > Lopsided or uneven envelope.
- > Very rigid envelope.
- > Springiness.
- > Suspicious package drop-offs/attempted drop-offs.





## **General suspicious activity that may cause concern**

- > Large group of persons (particularly men) occupying a house, apartment, motel room(s) with no apparent purpose or the leasing of highrise dwellings or office space overlooking Government facilities. No apparent patterns of departure/arrival, e.g., consistent with work commute.
- > Establishment of large bank accounts by recent arrivals in the United States.
- > Personnel in possession of large amounts of cash for no apparent reason.
- > Personnel attempting to purchase in cash expensive means of transportation (vehicles, boats, etc.).
- > Suspicious general aviation aircraft operating in proximity to Government facilities.

This page left blank intentionally

## APPENDIX B\*

### REPORTS ISSUED BY CENTRAL DOD INTERNAL AUDIT ORGANIZATIONS

Excludes base level reports issued by the Air Force Audit Agency and memorandum reports and consulting reports issued by the Army Audit Agency. Includes evaluation reports issued by the OIG DoD.

For copies of reports that are not classified or otherwise sensitive from a national security or legal standpoint, contact:

OIG DoD  
(703) 604-8937

Army Audit Agency  
(703) 681-9863

Naval Audit Service  
(202) 433-5737

Air Force Audit Agency  
(703) 696-8027  
(703) 696-8014

### Summary of Number of Reports by Issue Area<sup>1</sup>

**April 1, 2002- September 30, 2002**

	OIG DoD	Military Depts.	Total
Financial Management	14	50	64
Acquisition	17	32	49
Logistics	8	26	34
Readiness	3	14	17
Information Technology Management	10	7	17
Infrastructure and Environment	6	10	16
Information Security	10	4	14
Human Capital	2	5	7
Health Care	3	3	6
Other Security Concerns	2	1	3
Cooperative Threat Reduction	1	--	1

\*Partially fulfills requirements of the Inspector General Act of 1978, as amended, 5 U.S.C., Appendix 3, Section 5(a)(6) (see Appendix C).

---

## FINANCIAL MANAGEMENT

---

### IG DoD

**D-2002-078** Navy and Marine Corps Military Equipment Reporting (FOR OFFICIAL USE ONLY) (4/3/02)

**D-2002-082** Promptness of FY 2002 Third Quarter DoD Payments to the Department of the Treasury for District of Columbia Water and Sewer Services (4/15/02)

**D-2002-096** Major Deficiencies in Financial Reporting for Other Defense Organizations-General Funds (5/31/02)

**D-2002-115** The Defense Security Service Cost Accounting System to Support Fee-For-Service (FOR OFFICIAL USE ONLY) (6/24/02)

**D-2002-116** Review of the FY 2001 Financial Statements for the National Security Agency (CLASSIFIED) (6/25/02)

**D-2002-117** Review of the FY 2001 Financial Statements for the Defense Intelligence Agency (CLASSIFIED) (6/25/02)

**D-2002-118** Review of the FY 2001 Financial Statements for the National Imagery and Mapping Agency (CLASSIFIED) (6/25/02)

**D-2002-127** Department of Defense's Compliance With Internal Use Software Accounting Standards (7/9/02)

**D-2002-128** Promptness of FY 2002 Fourth Quarter DoD Payments to the Department of the Treasury for District of Columbia Water and Sewer Services (7/15/02)

**D-2002-130** Accounting and Reporting Processes at Defense Finance and Accounting Service San Antonio (7/22/02)

**D-2002-140** Measurement of Water Usage by DoD Components Served by the District of Columbia Water and Sewer Authority (8/20/02)

**D-2002-141** Implementation of the Data Quality Management Control Program for the Military Health System (8/29/02)

**D-2002-145** Effect of the Raytheon Defense Business Acquisitions on Pension Plans and DoD Funded Pension Assets (9/11/02)

**D-2002-147** Allegation to the Defense Hotline on the Use of Funds by Navy Region Southeast (9/16/02)

### Army Audit Agency

**A-2002-0276-FFB** The Army Executive Dining Facility Fund FY 01 Financial Statements (4/12/02)

**A-2002-0305-IMH** Financial Controls--Rod and Gun Club (4/17/02)

**A-2002-0304-AMW** Selected Internal Controls Over Inventory, Army Working Capital Fund (4/19/02)

**A-202-0254-FFG** Army's General Fund Principal Financial Statements for FY 2001, Accuracy of Real Property Data Reported in the Real Property Systems (4/22/02)

**A-2002-0306-FFP** Morale, Welfare and Recreation Use of Appropriated Funds (4/24/02)

**A-2002-0274-FFB** Secretary of Defense Executive Dining Facility Fund FY 01 Financial Statements (4/25/02)

**A-2002-0313-IMU** Nonappropriated Fund Payroll (4/26/02)

**A-2002-0366-AMI** Reimbursements for Materiel Provided Through the Army Sensitive Support Program, Technology Management Office (5/6/02)

**A-2002-0357-IMU** Laundry and Dry Cleaning Services (5/10/02)

**A-2002-0365-AMW** Compilation of Army Working Capital Fund FY 01 1307 Accounting Report (5/13/02)

**A-2002-0367-AMW** Materiel Returns, Army Working Capital Fund (5/22/02)

**A-2002-0418-AMW** Accounts Payable, Corpus Christi Army Depot, Army Working Capital Fund (6/10/02)

**A-2002-0446-AMW** Reduction of the Army Working Capital Fund FY 01 Cash Balance (6/24/02)

**A-2002-0465-AMW** Accounts Payable, Depot Maintenance and Ordnance Activity Groups, Army Working Capital Fund (7/2/02)

**A-2002-0475-FFF** Controls Over Operating Tempo Funds (7/15/02)

**A-2002-0484-IMU** Execution of Morale, Welfare and Recreation Funding for Family Support Programs (7/18/02)

**A-2002-0518-AMI** Financial Management of Special Access Programs, Ordain Quest Project Office (7/24/02)

**A-2002-0512-IMU** Stored Value Card (7/26/02)

**A-2002-0499-AMW** Accounting Adjustments (7/26/02)

**A-2002-0513-IMU** Travel Claims, Logistics Assistance Group-Europe (7/29/02)

**A-2002-0452-FFG** Military Pay and Benefits: The Army's Contribution to the Military Retirement Trust Fund (8/14/02)

**A-2002-0536-IMU** Military Interdepartmental Purchase Requests (8/21/02)

**A-2002-0516-FFP** Validating the Program and Budget for Headquarters Activities (8/30/02)

**A-2002-0569-AMI** Financial Management of SAPS – Secretary of the Army (9/6/02)

**A-2002-0562-IMH** Management Controls for Reimbursable Orders (9/16/02)

**A-2002-0584-FFG** Management Controls Over the Exchange or Sale of Nonexcess Property (9/16/02)

**A-2002-0566-IMH** Followup Issues, Morale, Welfare and Recreation Activities – Financial Controls, Fort Bliss Centennial Club (9/23/02)

**A-2002-0577-IMH** Financial Controls – Golf Course Operations (9/27/02)

**A-2002-0588-FFB** Budget Model for Civilian Personnel Requirements (9/30/02)

### Naval Audit Service

**N2002-0039** Reimbursable Work Orders (CLASSIFIED) (4/8/02)

**N2002-0055** Insufficient Appropriated Fund Support of Morale, Welfare, and Recreation Increases Cost to Individual Marines (6/14/02)

**N2002-0057** Validation of Unliquidated Obligations for Selected Appropriations at the Naval Supply Systems Command (6/20/02)

**N2002-0078** Validation of Selected Unliquidated Obligations at Naval Air Systems Command (9/25/02)

**N2002-0082** Validation of Selected Unliquidated Obligations at Naval Sea Systems Command (9/30/02)

### Air Force Audit Agency

**F2002-0004-B05300** Memorandum Report, Fiscal Year 2001 Review of Field Site Accounting Adjustments, Air Force General Fund (4/9/02)

**F2002-0006-C06800** Air Force Working Capital Fund, Statement of Budgetary Resources - Information Services Activity Group, Internal Control Review (4/11/02)

**F2002-0004-C06200** Depot Maintenance Budgets and Sales Prices (4/18/02)

**F2002-0007-C06800** Air Force Working Capital Fund Fiscal Year 2001 DoD Field Accounting Site Review (5/20/02)

**F2002-0006-B05400** Official Representation Funds (5/21/02)

**F2002-0009-B05800** Air Intelligence Agency Financial Management - Unliquidated Obligations (6/19/02)

**F2002-0007-B05400** Followup Audit, Controls Over Air Force Cash (6/20/02)

**F2002-0008-B05400** Civilian Permanent Change of Station Reimbursements (7/8/02)

**F2002-0008-C06800** Fiscal Year 2001 Other Assets, Air Force Working Capital Fund (7/26/02)

**F2002-0005-B05300** Accounting for Air Force Liabilities, Fiscal Year 2001 (7/29/02)

**F2002-0009-C06800** Air Force Working Capital Fund, Fiscal Year 2001 Statement of Budgetary Resources - Retail Supply, Internal Control Review (7/29/02)

**F2002-0009-B05400** Office of Special Investigations Confidential Investigative Contingency Funds (8/6/02)

**F2002-0007-C06400** Air Force Scientific Advisory Board Financial Management Review (8/20/02)

**F2002-0007-B05300** Accounting for Property, Plant, and Equipment - Personal Property (9/11/02)

**F2002-0008-B05300**

Accounting for Air Force Real Property, Fiscal Year 2001 (9/18/02)

**F2002-0010-C06800** Air Force Working Capital Fund, Fiscal Year 2001 Statement of Budgetary Resources, Wholesale Supply Management Activity Group, Operations, Internal Control Review (9/26/02)

---

## ACQUISITION

---

**IG DoD**

**D-2002-083** Acquisition of the MK 54 Lightweight Hybrid Torpedo (CLASSIFIED) (4/19/02)

**D-2002-088** Acquisition of the Joint Service Lightweight Standoff Chemical Agent Detector (5/10/02)

**D-2002-090** Evaluation of the Defense Supply Center Columbus Qualified Products List and Qualified Manufacturers List Program (5/14/02)

**D-2002-097** Contract Administration Services Function at Edwards Air Force Base (6/4/02)

**D-2002-100** The Acquisition of the National Exploitation System (CLASSIFIED) (6/11/02)

**D-2002-105** Fire Performance Tests and Requirements for Shipboard Mattresses (6/14/02)

**D-2002-106** Allegations Concerning the Defense Logistics Agency Contract Action Reporting System (6/14/02)

**D-2002-107** Army Transition of Advanced Technology Programs to Military Applications (6/14/02)

**D-2002-109** Army Claims Service Military Interdepartmental Purchase Requests (6/19/02)

**D-2002-110** Policies and Procedures for Military Interdepartmental Purchase Requests at Washington Headquarters Services (6/19/02)

**D-2002-114** V-22 Osprey Hydraulic System (6/24/02)

**D-2002-120** Air National Guard Decision on the Asynchronous Transfer Mode Installation Contract (6/26/02)

**D-2002-126** Acquisition of the Evolved SEASPARROW Missile (7/5/02)

**D-2002-139** Naval Facilities Engineering Command Environmental Services Contracting (8/20/02)

**D-2002-143** Acquisition of the Army Land Warrior System (9/5/02)

**D-2002-150** Procedures for Selecting Contractor Personnel to Perform Maintenance on Army Aircraft in Bosnia (9/18/02)

**D-2002-152** Defense Hotline Allegations Concerning the Procurement of the Seat Management Initiative (9/25/02)

**Army Audit Agency**

**A-2002-0361-AMW** Government Purchase Cards (5/13/02)

**A-2002-0377-IMU** Controls Over Morale, Welfare and Recreation Equipment Down-range (Bosnia and Kosovo) (5/17/02)

**A-2002-0464-AMA** Test and Evaluation - Nuclear, Biological and Chemical Systems (7/3/02)

**A-2002-0477-IME** Administering Service Contracts (7/8/02)

**A-2002-0491-AMW** Government Purchase Cards (7/25/02)

**A-2002-0492-AMW** Government Purchase Cards, Army Working Capital Fund (7/26/02)

**A-2002-0514-AMA** Common Missile Program (8/7/02)

**A-2002-0535-IMU** Controls for the International Merchant Purchase Authorization Card Program (8/21/02)

**A-2002-0580-AMA** Managing Service Contracts (9/23/02)

**Naval Audit Service**

**N2002-0042** Department of the Navy Commercial Purchase Card Program (CLASSIFIED) (4/25/02)

**N2002-0043** Department of the Navy Commercial Purchase Card Program (CLASSIFIED) (4/25/02)

**N2002-0044** Independent Review: Photographic Optics Branch Functions at the Naval Air Warfare Center, Weapons Division, Point Mugu and China Lake, CA (4/26/02)

**N2002-0045** Independent Review: Ocean Terminal Operations, Fleet and Industrial Supply Center Norfolk, VA (4/29/02)

**N2002-0046** Independent Review: Facilities Support Services Function at Marine Corps Air Station, Beaufort, SC (5/6/02)

**N2002-0051** Naval Sea Systems Command Commercial Purchase Card Program (5/28/02)

**N2002-0052** Management of Emergency Combat Use Only Ordnance (6/3/02)

**N2002-0060** Department of the Navy Commercial Purchase Card Program (CLASSIFIED) (7/8/02)

**N2002-0062** Naval Air Systems Command Award Fee Management (7/24/02)

**N2002-0068** Naval Facilities Engineering Command's Process to Identify and Recover Contractor Debts (8/8/02)

**N2002-0070** Naval Facilities Engineering Command Commercial Purchase Card Program (8/14/02)

**N2002-0074** Department of the Navy Commercial Purchase Card Program (CLASSIFIED) (9/4/02)

**N2002-0075** Independent Review of Centralized Visual Information, Administrative Support, and Centralized Facilities Operations and Maintenance Services at the Corona Division, Naval Surface Warfare Center, Corona, CA (9/10/02)

**N2002-0076** Classified Contracts (CLASSIFIED) (9/27/02)

**N2002-0077** Department of the Navy Commercial Purchase Card Program (CLASSIFIED) (9/27/02)

**N2002-0081** Auditor General Advisory Naval Personnel Command Nonappropriated Fund Construction Contracting (9/30/02)

### **Air Force Audit Agency**

**F2002-0003-C06400** F-22 Integrated Product Team Participation, Phase III (4/29/02)

**F2002-0005-C06400** Airborne Laser Program Integrated Product Team Participation, Phase III (7/30/02)

**F2002-0004-C06400** U-2 Acquisition Management (8/6/02)

**F2002-0006-C06400** Air Force Purchase Card Program (8/6/02)

**F2002-0008-C06100** Night Vision Imaging System Management (8/13/02)

**F2002-0008-B05100** Most Efficient Organization Eglin AFB Civil Engineering (9/2/02)

**F2002-0008-C06400** Memorandum Report, Air Mobility Command's Programming and Budgeting Actions Associated With Office of Management and Budget Circular A-76 Reviews (9/18/02)

---

## **LOGISTICS**

---

### **IG DoD**

**D-2002-079** Delivery and Receipt of DoD Cargo Inbound to the Republic of Korea (4/5/02)

**D-2002-080** Quality Deficiency Reporting Procedures for Naval Repair Parts (4/5/02)

**D-2002-091** Accountability and Control of Materiel at the Corpus Christi Army Depot (5/21/02)

**D-2002-104** Military Traffic Management Command Handling of Container Detention Charges (6/12/02)

**D-2002-112** Industrial Prime Vendor Program at the Air Force Air Logistics Centers (FOR OFFICIAL USE ONLY) (6/20/02)

**D-2002-131** Terminal Items Managed by the Defense Logistics Agency for the Navy (7/22/02)

**D-2002-136** Defense Logistics Agency Aviation Investment Strategy Program (7/31/02)

**D-2002-149** Defense Logistics Agency-Managed Items Supporting Air Force Weapon Systems (9/18/02)

### **Army Audit Agency**

**A-2002-0262-AML** Global Combat Support System-Army Program Lessons Learned (4/2/02)

**A-2002-0245-FFP** Space Utilization of Classroom and Training Facilities (4/5/02)

**A-2002-0333-AML** Logistics Integrated Database (5/7/02)

**A-2002-0404-AMI** Cover Support Program, Site D (5/16/02)

**A-2002-0381-IME** Transportation Motor Pool (5/17/02)

**A-2002-0376-AMW** Accounting for Real Property (5/22/02)

**A-2002-0423-AML** Repair Parts Support to Alert Forces (6/7/02)

**A-2002-0441-FFP** Trucks Refurbished by Depot Support Activity Far East for Distribution to Foreign Countries (6/18/02)

**A-2002-0443-AMA** Executing the Army's Recapitalization Program (6/20/02)

**A-2002-0460-IMU** Followup Audit of the Reserve Storage Activity (6/28/02)

**A-2002-0445-AMW** Accounting for Real and Personal Property (7/1/02)

**A-2002-0476-IMU** Ammunition Accountability-- Reserve Storage Activity, Miesau (7/12/02)

**A-2002-0530-AMI** Army Cover Program, Site E (8/2/02)

**A-2002-0444-AMA** Formulating the Army's Recapitalization Program (8/30/02)

### Naval Audit Service

**N2002-0049** Contractor Logistics Support at the Naval Sea Systems Command (5/17/02)

**N2002-0067** Management of the Navy's Sustainment, Restoration, and Modernization Program (8/6/02)

**N2002-0069** Contractor Logistics Support at the Space and Naval Warfare Systems Command (8/8/02)

### Air Force Audit Agency

**F2002-0008-B05800** Aircraft Fuels Servicing Equipment (4/2/02)

**F2002-0005-C06200** C-141 Aircraft Engine Maintenance Support Operations (4/29/02)

**F2002-0006-C06200** Material Management Transition (4/29/02)

**F2002-0005-C06100** Air National Guard Small Arms Management (5/20/02)

**F2002-0006-C06100** Equipment Additive and Replacement Program Requirements (6/17/02)

**F2002-0007-C06100** Air Force Repair Enhancement Program (6/20/02)

**F2002-0007-C06200** Antenna Preventive Maintenance Inspections (7/8/02)

**F2002-0008-C06200** Asset Variance (9/18/02)

**F2002-0009-C06100** Air Mobility Command Forward Supply System (9/26/02)

---

## READINESS

---

### IG DoD

**D-2002-095** Chemical and Biological Defense Individual Protective Equipment in Central Command and Euro Command Areas (CLASSIFIED) (5/30/02)

**D-2002-102** Summary Report on Homeland Defense, Chemical and Biological Defense, and Other Matters Related to Counterterrorist Military Operations (CLASSIFIED) (6/11/02)

**D-2002-111** Readiness of Intelligence, Surveillance, and Reconnaissance Aircraft (CLASSIFIED) (6/20/02)

### Army Audit Agency

**A-2002-0486-IME** Unit-Level Training for Chemical and Biological Defense (7/10/02)

**A-2002-0517-IME** Chemical and Biological Support for Forward Stationed DA Civilians and Contractors (8/2/02)

**A-2002-0555-FFF** Advanced Individual Training Courses (9/16/02)

### Naval Audit Service

**N2002-0038** Risk Assessment of the Navy's Strategic Sourcing Program (4/8/02)

**N2002-0050** Marine Corps AV-8B Harrier Readiness Reporting (5/22/02)

**N2002-0054** Marine Corps Equipment Deployment Planning (6/12/02)

**N2002-0056** Marine Corps AH-1 Cobra and UH-1N Huey Readiness Reporting (6/19/02)



**N2002-0058** Opportunities to Improve the Marine Corps Total Force System (6/25/02)

**N2002-0061** Business Risk Assessment of Navy and Marine Corps Presence Located Outside the Continental United States (7/17/02)

**N2002-0066** Key Navy P-3 Aircrew Positions (8/5/02)

**N2002-0073** Marine Corps Ground Forces Training (8/26/02)

**N2002-0079** Readiness Training Status Reporting for 1st Battalion, 3rd Marines (CLASSIFIED) (9/26/02)

**N2002-0080** Navy Submarine Readiness Reporting (9/27/02)

#### **Air Force Audit Agency**

**F2002-0010-B05800** Personnel Deployment Planning (FOR OFFICIAL USE ONLY) (6/20/02)

---

## **INFORMATION TECHNOLOGY MANAGEMENT**

---

#### **IG DoD**

**D-2002-081** The Preventive Health Care Application and an Associated Upgrade (4/12/02)

**D-2002-084** Guidance for the Global Command and Control System Common Operational Picture (FOR OFFICIAL USE ONLY) (5/1/02)

**D-2002-086** Defense Hotline Allegations on the Procurement of a Facilities Maintenance Management System (5/7/02)

**D-2002-103** Certification of the Reserve Component Automation System (6/14/02)

**D-2002-113** Controls Over the Computerized Accounts Payable System at Defense Finance and Accounting Service Columbus (6/21/02)

**D-2002-119** Defense Hotline Allegations Regarding the Military Airspace Management System (6/25/02)

**D-2002-123** Acquisition and Clinger-Cohen Act Certification of the Defense Integrated Military Human Resources System (6/28/02)

**D-2002-124** Allegations to the Defense Hotline on the Management of the Defense Travel System (7/1/02)

**D-2002-133** Global Command and Control System Readiness Assessment System Output Tool (7/24/02)

**D-2002-146** The Defense Advanced Research Projects Agency's Transition of Advanced Information Technology Programs (9/11/02)

#### **Army Audit Agency**

**A-2002-0461-FFF** Computer-Based Training for Information Technology (3/29/02)

**A-2002-0600-AMI** Information Technology Acquisition Workload Management, Technology Application Office (9/27/02)

#### **Naval Audit Service**

**N2002-0047** Department of the Navy Status of Resources and Training System (5/8/02)

**N2002-0048** Improvements to the Visibility and Management of Operating and Support Costs System (5/15/02)

**N2002-0071** The Compliance Process for the Navy's Standard Labor Data Collection and Distribution Application System (8/21/02)

#### **Air Force Audit Agency**

**F2002-0005-B05400** Air Force Equipment Management System Systems Controls (4/8/02)

**F2002-0010-B05400** Tempo Management and Tracking System Interface Controls (8/13/02)

---

## **INFRASTRUCTURE AND ENVIRONMENT**

---

#### **IG, DoD**

**D-2002-077** Bulk Fuel Infrastructure Military Construction Project Review Process: Air Force (4/3/02)

**D-2002-085** Audit Coverage of DoD Energy Management (5/1/02)

**D-2002-089** Department of Defense Policies and Procedures to Implement the Rural Development Act of 1972 (5/10/02)

**D-2002-122** DoD Environmental Community Involvement Programs at Test and Training Ranges (6/28/02)

**D-2002-125** General and Flag Officer Quarters at Pearl Harbor, Hawaii (7/1/02)

**D-2002-137** Bulk Fuel Infrastructure Military Construction and Maintenance, Repair, and Environmental Project Review Process: Navy (8/9/02)

### Army Audit Agency

**A-2002-0289-IMO** Energy Savings Performance Contracts (5/23/02)

**A-2002-0395-IMO** Electrical Distribution System Contract (5/23/02)

**A-2002-0382-IME** Management of Chemical Stockpile Sites (5/24/02)

**A-2002-0288-IMO** Energy Savings Performance Contracts (7/24/02)

**A-2002-0527-IMO** Privatization of Family Housing (8/9/02)

**A-2002-0500-IME** Projected Supply and Use of Halon 1301 (8/16/02)

**A-2002-0578-IME** Management of the Impact Area Groundwater Study Program, Camp Edwards, Massachusetts (9/23/02)

### Air Force Audit Agency

**F2002-0005-B05200** Followup Audit, Installation Support of the Environmental Restoration Program (4/23/02)

**F2002-0006-B05200** Military Family Housing Privatization - Kirtland AFB (FOR OFFICIAL USE ONLY) (6/14/02)

**F2002-0007-B05200** Family Housing Requirements Determination (6/19/02)

---

## INFORMATION SECURITY

---

### IG DoD

**D-2002-093** Government Information Security Reform Act Implementation: Noncombatant Evacuation Operations Tracking System (5/23/02)

**D-2002-098** Army Web Site Administration, Policies, and Practices (6/5/02)

**D-2002-108** Standard Procurement System Certification and Accreditation Process (FOR OFFICIAL USE ONLY) (6/19/02)

**D-2002-129** DoD Web Site Administration, Policies, and Practices (7/19/02)

**D-2002-132** Implementation of Government Information Security Reform by the Defense Finance and Accounting Service for the Civilian Personnel Resource Reporting Systems (FOR OFFICIAL USE ONLY) (7/23/02)

**D-2002-134** Implementation of Government Information Security Reform by the Defense Finance and Accounting Service Nonappropriated Fund Information Standard System (FOR OFFICIAL USE ONLY) (7/24/02)

**D-2002-135** User Authentication Protection at Central Design Activities (7/29/02)

**D-2002-142** Government Information Security Reform Act Implementation: Defense Security Assistance Management System (8/30/02)

**D-2002-148** Defense Information Systems Agency Defense Enterprise Computing Center St. Louis Information Security Program (FOR OFFICIAL USE ONLY) (9/17/02)

**D-2002-151** Implementation of Government Information Security Reform by the Defense Finance and Accounting Service Electronic Funds Transfer Computerized Accounts Payable System Bridge System (FOR OFFICIAL USE ONLY) (9/19/02)

### Army Audit Agency

**A-2002-0540-FFF** Government Information Security Reform Act Requirement (8/30/02)

**A-2002-0587-FFB** The Army's Implementation of the Government Information Security Reform Act – Lessons Learned (9/30/02)

### Air Force Audit Agency

**F2002-0002-C06600** Controls Over Classified Computer Systems (FOR OFFICIAL USE ONLY) (4/1/02)

**F2002-0003-C06600** Certification and Accreditation of Air Force Systems (4/22/02)

---

## HUMAN CAPITAL

---

### IG DoD

**D-2002-101** Compensation Policies and Procedures for Selected Nonappropriated Fund Childcare Providers (6/10/02)

**D-2002-144** Civilian Personnel Processing by Regional Service Centers That Service Multiple DoD Agencies (9/11/02)

**Army Audit Agency**

**A-2002-0422-AMI** Army Foreign Language Program (6/12/02)

**A-2002-0585-FFF** Manning Priorities for Army Transformation (9/30/02)

**Naval Audit Service**

**N2002-0041** Improper Use of Boot Camp Recruits Contributes to Fleet Understaffing (4/19/02)

**Air Force Audit Agency**

**F2002-0007-B05100** Civilian Firefighter Pay and Leave (6/17/02)

**F2002-0011-B05800** Air Reserve and Guard Intelligence Force Support (8/16/02)

---

**HEALTH CARE**

---

**IG DoD**

**D-2002-087** DoD Medical Support to the Federal Response Plan (5/10/02)

**D-2002-094** Pricing of Pharmaceutical Items in the Medical Prime Vendor Program (5/23/02)

**D-2002-153** Reprocessed Medical Single-Use Devices in DoD (9/30/02)

**Army Audit Agency**

**A-2002-0397-FFP** DoD/Veterans Affairs Joint Physical Examination Program (6/28/02)

**A-2002-0488-IMU** Child Care Operations (7/24/02)

**A-2002-054-FFP** Resources Sharing Agreement with the Department of Veterans Affairs (9/9/02)

---

**OTHER SECURITY CONCERNS**

---

**IG DoD**

**D-2002-121** Security: Controls Over Biological Agents (CLASSIFIED) (6/27/02)

**D-2002-138** Allegations Concerning the Management and Business Practices of the Defense Security Service (8/9/02)

**Air Force Audit Agency**

**F2002-0012-B05800** Antiterrorism/Force Protection Program (FOR OFFICIAL USE ONLY) (8/20/02)

---

**COOPERATIVE THREAT REDUCTION**

---

**IG DoD**

**D-2002-154** Cooperative Threat Reduction Program Liquid Propellant Disposition Project (9/30/02)

---

**AUDIT OVERSIGHT REVIEWS**

---

**IG DoD**

**D-2002-6-005** Defense Contract Audit Agency Regional Quality Assurance Review of the Incurred Cost Sampling Initiative (4/16/02)

**D-2002-6-006** Summary of Risk Assessment Methodologies (5/6/02)

**D-2002-6-007** Defense Contract Audit Agency Quality Assurance Review of Internal Control System Audits (8/6/02)

**D-2002-6-008** Quality Control System at U.S. Special Operations Command Inspector General Audit Division (8/21/02)

**D-2002-6-009** The Army Contract Audit Followup Process (9/18/02)

**Naval Audit Service**

**N2002-0040** Quality Control Review of Report Marking (4/17/02)

**N2002-0053** Quality Control Review of Selective Referencing (6/7/02)

**N2002-0059** Quality Assurance Review of the Local Audit Function at the Navy Exchange Service Command (7/1/02)

**N2002-0063** Quality Control Review of Audit Report N2001-0030: "Management of the Navy's Individual Ready Reserve Program" (7/30/02)

**N2002-0064** Peer Review of the Air Force Audit Agency (7/30/02)

**N2002-0065** Quality Control Review of Audit Report N2001-0024, "Ordnance Inventory Statistical Sampling Methodology" (7/31/02)

**N2002-0072** Quality Assurance Review of the Local Audit Function at Selected Chief of Naval Education and Training Activities (8/22/02)

This page left blank intentionally

**APPENDIX C\***  
**OIG DoD AUDIT REPORTS ISSUED CONTAINING**  
**QUANTIFIABLE POTENTIAL MONETARY BENEFITS**

Audit Reports Issued	Potential Monetary Benefits	
	Questioned Costs <sup>1</sup>	Funds Put to Better Use
<b>D-2002-088</b> Acquisition of the Joint Service Lightweight Standoff Chemical Agent Detector (5/10/02)	N/A	\$57,000,000
<b>D-2002-091</b> Accountability and Control of Materiel at the Corpus Christi Army Depot (5/21/02)	N/A	90,000,000
<b>D-2002-104</b> Military Traffic Management Command Handling of Container Detention Charges (6/12/02)	N/A	463,157
<b>D-2002-109</b> Army Claims Service Military Interdepartmental Purchase Requests (6/19/02)	N/A	2,800,000
<b>D-2002-110</b> Policies and Procedures for Military Interdepartmental Purchase Requests at Washington Headquarters Services (6/19/02)	N/A	5,700,000
<b>D-2002-112</b> Industrial Prime Vendor Program at the Air Force Air Logistics Center (6/20/02)	N/A	9,045,847
<b>D-2002-131</b> Terminal Items Managed by the Defense Logistics Agency (7/22/02)	N/A	69,000,000
<b>D-2002-136</b> Defense Logistics Agency Aviation Investment Strategy Program (7/31/02)	N/A	111,600,000
<b>Totals</b>	<b>0</b>	<b>\$345,609,004</b>
<sup>1</sup> There were no OIG audit reports during the period involving questioned costs.		

\*Partially fulfills the requirement of the Inspector General Act of 1978, as amended, 5 U.S.C., Appendix 3, Section 5(a)(6) (see Appendix B).

This page left blank intentionally

**APPENDIX D\***  
**FOLLOWUP ACTIVITIES**

<b>DECISION STATUS OF INSPECTOR GENERAL ISSUED REPORTS WITH RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE (\$ in thousands)</b>		
<b>Status</b>	<b>Number</b>	<b>Funds Put to Better Use<sup>1</sup></b>
A. For which no management decision had been made by the beginning of the reporting period.	28	\$43,000 <sup>2</sup>
B. Which were issued during the reporting period.	76	345,609
Subtotals (A+B)	104	388,609
C. For which a management decision was made during the reporting period.	80	115,209
(i) dollar value of recommendations that were agreed to by management		
- based on proposed management action		5,700
- based on proposed legislative action		
(ii) dollar value of recommendations that were not agreed to by management		109,509 <sup>3</sup>
D. For which no management decision has been made by the end of the reporting period.	24	273,400
Reports for which no management decision was made within 6 months of issue (as of March 31, 2002).	0	0
<sup>1</sup> There were no OIG DoD audit reports issued during the period involving "disallowed costs." <sup>2</sup> Previously claimed potential monetary benefits of \$215,000 were subsequently withdrawn. <sup>3</sup> On 5 audit reports with a total of potential funds put to better use of \$109.5 million, management has agreed to take the recommended actions, but the amount of agreed monetary benefits cannot be determined until those actions are completed.		

\*Fulfills requirements of the Inspector General Act of 1978, as amended, 5 U.S.C., Appendix 3, Section 5(a)(8)(9)&(10).

This page left blank intentionally



**APPENDIX E**  
**CONTRACT AUDIT REPORTS ISSUED<sup>1</sup>**  
**(\$ in millions)**

Type of Audit <sup>2</sup>	Reports Issued*	Amounts Examined	Questioned Costs <sup>3</sup>	Funds Put to Better Use
Incurring Costs	16,043	\$48,987.7	\$689.4	\$236.7 <sup>4</sup>
Forward Pricing Proposals	5,016	\$77,046.6	--	\$2,200.9 <sup>5</sup>
Cost Accounting Standards	1,301	\$378.7	\$71.4	--
Defective Pricing	430	<u>6</u>	\$35.7	--
<b>Totals</b>	<b>22,790</b>	<b>\$126,413.0</b>	<b>\$796.5</b>	<b>\$2,437.6</b>

<sup>1</sup>This schedule represents Defense Contract Audit Agency (DCAA) contract audit reports issued during the 6 months ended September 30, 2002. Both "Questioned Costs" and "Funds Put to Better Use" represent potential cost savings. Because of limited time between availability of management information system data and legislative reporting requirements, there is minimal opportunity for the DCAA to verify the accuracy of reported data. Accordingly, submitted data is subject to change based on subsequent DCAA authentication.

<sup>2</sup>This schedule represents audits performed by DCAA summarized into four principal categories, which are defined as:

Incurring Costs - Audits of direct and indirect costs charged to Government contracts to determine that the costs are reasonable, allocable, and allowable as prescribed by the Federal Acquisition Regulation, Defense Federal Acquisition Regulation, and provisions of the contract. Also included under incurred cost audits are Operations Audits, which evaluate a contractor's operations and management practices to identify opportunities for increased efficiency and economy; and Special Audits, which include audits of terminations and claims.

Forward Pricing Proposals - Audits of estimated future costs of proposed contract prices, proposed contract change orders, costs for redeterminable fixed-price contracts, and costs incurred but not yet covered by definitized contracts.

Cost Accounting Standards - A review of a contractor's cost impact statement required due to changes to disclosed practices, failure to consistently follow a disclosed or established cost accounting practice, or noncompliance with a CAS regulation.

Defective Pricing - A review to determine whether contracts are based on current, complete, and accurate cost or pricing data (the Truth in Negotiations Act).

<sup>3</sup>Questioned costs represent costs that DCAA has questioned because they do not comply with rules, regulations, laws, and/or contractual terms.

<sup>4</sup>Represents recommendations associated with Operations Audits where DCAA has presented to a contractor that funds could be used more effectively if management took action to implement cost reduction recommendations.

<sup>5</sup>Represents potential cost reductions that may be realized during contract negotiations.

<sup>6</sup>Defective pricing dollars examined are not reported because the original value was included in the audits associated with the original forward pricing proposals.

\*Applies to Army Corps of Engineers and DCAA only.

**Waivers of Advisory and Assistance Service Contracts**

**A review is made of each waiver granted by the Department for advisory and assistance services contracts related to testing support. This review is required by Section 802, Defense Authorization Act for Fiscal Year 1990.**

**The Department made no waivers during the period and therefore, no reviews were made by the OIG.**

*If you suspect Fraud, Waste, Abuse, or Mismanagement in  
the Department of Defense, please contact us at:*

*Hotline@dodig.osd.mil*

*or*

*www.dodig.osd.mil/hotline*

*or call:*

**800-424-9098**



**The Hotline is available 24 hours per day. The caller can remain anonymous.  
If you prefer, you may send written complaints to:**

**Office of the Inspector General  
Department of Defense  
Room 929  
400 Army Navy Drive  
Arlington, Virginia 22202-4704**



Friedrich Wilhelm Augustus von Steuben was the Inspector General of the Continental Army and served under General George Washington. He is recognized as the "Father of the Inspector General System" of the United States Military.



Inspector General  
Department of Defense



This report, as well as audit report and testimony text, are available on the Internet at: [www.dodig.osd.mil](http://www.dodig.osd.mil)  
Additional information on or copies of this report may be obtained by writing or contacting:

Office of the Inspector General of the Department of Defense  
Office of Congressional Liaison/Public Affairs  
400 Army Navy Drive, Arlington, VA 22202-4704  
Mr. John R. Crane 703-604-8524; DSN 664-8524

NO MONEY SHALL BE DRAWN FROM THE TREASURY, BUT IN CONSEQUENCE OF APPROPRIATIONS MADE BY LAW,  
AND A REGULAR STATEMENT AND ACCOUNT OF THE RECEIPTS AND EXPENDITURES OF ALL PUBLIC MONEY SHALL BE  
PUBLISHED FROM TIME TO TIME. U.S. CONSTITUTION - ARTICLE I, SECTION 9