Testimony

STATEMENT OF
ELEANOR HILL
INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
BEFORE THE SUBCOMMITTEE ON
NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
COMMITTEE ON GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES
ON DOD VULNERABILITIES TO WASTE, FRAUD AND ABUSE

Report Number 99-088 DELIVERED: February 25, 1999

Office of the Inspector General
Department of Defense

Mr. Chairman and Members of the Subcommittee:

I am pleased to have this opportunity to discuss Department of Defense (DoD) vulnerabilities to waste, fraud and abuse, as well as opportunities for continuing the momentum developed over the past few years toward management reforms and improvements. My testimony today will cover the ten areas where we believe further management improvement is particularly important, based on recent audit and investigative results. As requested in your invitation letter, my remarks will parallel my office's response of December 3, 1998, to a joint request from the House Majority Leader and the Chairman, House Government Reform Committee, to identify those problem areas.

We estimate that about 98 percent of the audits conducted by my office and most of our approximately 1,700 open criminal investigative cases relate directly or indirectly to the 10 high risk areas. In each of those areas, there are numerous problems that are interrelated, complex and involve a wide range of organizations. Many specific problems, such as inaccurate financial information, are relatively long-standing. Others, such as large scale computer intrusion, have emerged only recently. Let me briefly summarize for you our concerns, and our efforts, in each of these areas.

Top 10 DoD Problem Areas

Financial Management. The DoD remains unable to comply with the various laws requiring auditable financial statements for its major component funds and for the Department as a whole. For fiscal year 1997, only the Military Retirement Trust Fund financial statements received a clean audit opinion; we were unable to provide favorable opinions on any other major statement. We anticipate similar results when we issue opinions next week on the DoD statements for FY 1998. Due to the underlying system problems, we cannot forecast a significant difference in overall financial statement audit opinions for several more years. The inability of DoD systems to produce reliable annual financial statements also means that DoD managers and commanders lack much of the timely, accurate and useful financial information that they need for program decision making on a day to day basis.

I am pleased to be able to report, however, that the past year has brought considerably improved focus on the problem. The Secretary of Defense has explicitly directed the increased involvement of all functional managers. A successful joint effort by senior OMB, GAO, and DoD accounting and auditing

personnel has resolved many questions that had impeded progress toward compliance with the new Federal accounting standards. For the first time, the Department has an agreed-upon action plan, with explicit milestones and delineation of responsibility, to address the new standards and the “show stoppers” blocking compliance with those standards and the financial reporting statutes.

Although progress has been made, the DoD remains unable to avoid having several billions of dollars of disbursements remain unmatched to valid contracts or orders at any given time. Recent Senate hearings also raised legitimate concerns about the vulnerability of DoD finance operations, especially to fraud in the vendor pay area. The Defense Criminal Investigative Service, the criminal investigative arm of my office, is working with the Defense Finance and Accounting Service to decrease that vulnerability through such measures as increased fraud awareness training and we have about 80 open criminal investigations related to finance operations.

The recent case of Staff Sergeant Robert Miller illustrates the threat and vulnerability to fraud in this area. Miller and an accomplice were the subjects of a joint investigation by my office and the Office of Special Investigations, U.S. Air Force.

Miller was sentenced to 12 years in prison, dishonorable discharge, reduction in rank to E-1 and forfeiture of all pay and allowances for stealing or attempting to steal $938,535 in Treasury checks from a DoD finance office in Dayton, Ohio, where he supervised a finance branch.

The efforts of the Defense Criminal Investigative Service over the past 5 fiscal years have resulted in 73 convictions and recoveries of $4.9 million from cases related to DoD finance operations. Despite those successes, the lack of adequate audit resources to assess finance operation controls on a continual basis hampers efforts to minimize risk in this area. Although we issued 91 financial audit reports since October 1997, the great majority of those were on required financial statements, not the high risk vendor pay area.

On a positive note, the DoD ended several years of indecision and implemented a new procedure in October 1998 to improve safeguards for appropriation integrity in the contractor progress payment process. Likewise, at our urging, an effort was made to discourage the Military Departments and Defense agencies from unnecessarily creating overly complex contracts and accounting requirements that increase the likelihood of accounting errors. It is not yet evident, however, that those

organizations are aggressively carrying out the Department's guidance.

Weapon System Acquisition. New weapon systems are needed by all Military Services to avoid block obsolescence, keep pace with technological change and reduce life cycle costs. The Joint Chiefs of Staff, other DoD leadership, and the Congress have acknowledged the significant gap between modernization requirements and planned funding. Increasing the weapons procurement share of the budget is a high priority DoD budget goal. In addition, there are compelling technological and financial reasons to accelerate the acquisition cycle and cut per unit costs, especially overhead costs.

The Department is relying on very substantial near and long term savings from reengineered logistics practices and civilian personnel reductions to enable the planned migration of funds into the procurement accounts. Despite the recent increases in the DoD topline budget, it is by no means certain that support costs can be cut enough to sustain a robust modernization effort. In addition, despite many positive acquisition reform initiatives, we have seen no significant across-the-board improvement yet in cycle time and unit cost. It is also by no

means clear that the ongoing deep cuts in the DoD acquisition corps will result in better program management.

We have issued 29 audit reports on weapon system acquisition since October 1997. Findings were related to such matters as the processes used to determine the types and quantities of systems needed, acquisition strategy and upfront planning for logistical support.

Other Procurement Issues. The vast majority of the several million annual DoD contracting actions involve equipment, ammunition, supplies and services, rather than major weapon end items such as new ships and missiles. The sheer volume and great variety of DoD contracting activity make this a high risk area. Acquisition reform initiatives such as promoting electronic commerce and encouraging the use of commercial purchasing practices are focused on expediting procurements, cutting red tape and reducing overhead costs. However, much more needs to be done to ensure that the DoD acquisition work force is capable of transitioning to new practices and that those new practices include reasonable controls to safeguard against the continuing threat of procurement fraud and mismanagement.

We have issued 33 audit reports in this area since October 1997, approximately half of the coverage that we were able to provide before our resource cutbacks began. We currently have over 800 open criminal cases on bribery, conflict of interest, mischarging, product substitution, false claims and other procurement matters. Over the past 5 fiscal years, our cases related to procurement have resulted in 948 convictions and $1.1 billion in recoveries.

Three audits during 1998 on prices being paid for DoD aviation spares under commercial type contracts illustrated the difficulty of adopting buying and pricing practices that were not yet well understood by Government personnel. The audits indicated that the DoD was paying up to several times more per item, when purchasing from commercial catalogs, than when previously contracting under traditional procedures. The Defense Authorization Act for Fiscal Year 1999 included provisions requiring the Department to address the problem identified by the audits and we have worked with DoD acquisition officials to develop an extensive training program for DoD procurement personnel. We do not believe that this problem is solved yet, however, and we are doing further audit work on spares pricing.

We strongly support further refinement of the acquisition rules and practices that are in place, as well as aggressively seeking new opportunities for genuine reform. It is particularly important to put more emphasis on reducing costs for procuring services, because the DoD actually spends more on services, including research, than on procuring hardware. However, we caution that all reform initiatives must be carefully crafted to safeguard the taxpayers' interest. The DoD administers over $800 billion in open contracts and plans to award $135 billion of new contracts in the current fiscal year. This massive and extremely diversified program requires careful oversight. We do not support broad attacks on such essential safeguards as contract audits, the Cost Accounting Standards, the False Claims Act and the Truth in Negotiations Act.

Health Care. The Defense Health Program serves 8.2 million eligible beneficiaries through a combination of DoD inhouse and outsourced care. Most of the latter is purchased through managed care support contracts under the TRICARE Program. Total health care costs are nearly $16 billion annually.

As in the overall health care sector of the US economy, the Defense Health Program is attempting to quell strong cost growth pressure without compromising the quality of care. The DoD

flexibility is constrained because its system must be capable of shifting to a wartime mobilization mode at any time. Obviously there are major differences in the medical skills and supplies needed to treat peacetime patients, who are mostly retirees and dependents, and wartime casualties. The Defense Health Program's cost containment challenges also are exacerbated by the continued lack of good cost information and significant levels of fraud, particularly by some private sector providers. We have issued 6 audit reports since October 1997 on health care issues, including alcohol and tobacco related DoD health care costs and DoD reluctance to put malpractice information into the National Practitioners Data Base. Given the size and complexity of the Defense Health Program, this is marginally adequate audit coverage, but all that available resources allow.

To combat health care fraud, the Defense Criminal Investigative Service has an active partnership with the TRICARE Program Office. This high degree of cooperation and the special priority that we have given to health care fraud have led to a significant increase in the number of criminal cases in this area. We currently have about 500 open criminal investigations on health care fraud. The efforts of the Defense Criminal Investigative Service in this area over the last 5 fiscal years have resulted in 343 convictions and $1.0 billion in recoveries.

Supply Inventory Management. The DoD logistics community has always been a proactive user of audit support and we have issued 19 audit reports on inventory management since October 1997. The Department has reduced wholesale supply stocks by nearly a third and is pursuing a number of logistics reform initiatives to reduce warehousing requirements, implement more direct vendor delivery, and reduce the time between when a user puts a request into the logistics pipeline and when the needed item is delivered to that user. Processes for recalculating what quantities need to be stocked and for distributing items most efficiently need additional work, however.

Spare parts shortages are being reported more frequently by operational units and audits continue to show that war reserves are overstocked in some locations, but short of critical items in others. The Department also has not overcome problems identified by auditors on the inaccurate demilitarization coding of items before disposal. Fraud and inappropriate disposal practices remain particular problems in the disposal area, where we have about 70 open criminal investigations. This is an intrinsically high risk area, but the working relationship between my office and the Defense Logistics Agency is very good. Over the past five fiscal years, our efforts on property

disposal related cases have resulted in 46 convictions and $.7 million in recoveries.

An example of a successful investigation involving DoD excess property was Operation Breechblock, a joint investigation by my office and the Federal Bureau of Investigation. A number of obsolete combat vehicles and various equipment, including operational TOW missile launchers, were stolen from Fort McCoy, Wisconsin. The vehicles were destined to be used as targets on military firing ranges, but Government employees responsible for the vehicles accepted bribes and diverted the vehicles to private individuals. Documentation was falsified to reflect that the vehicles were destroyed on the firing range, although they were never placed on the ranges. The investigation resulted in the indictment of seven individuals (2 Government employees and 5 private citizens), individual prison terms of up to 8 years, and fines and penalties totaling over $1.2 million.

Year 2000 Conversion. The DoD depends heavily on automated information processing by about 28,000 systems, 2,274 of which are considered mission critical. In addition, weapon systems, facilities and equipment have millions of embedded microprocessor chips. Because of hardware and software limitations, many systems and processors whose functions are

date sensitive will not work properly when post-December 31, 1999, dates are introduced. In addition, systems that are linked to other systems are vulnerable to failures if all data exchange partners have not made their systems “Y2K compliant” and preserved interoperability when making those fixes. Data exchange partners for DoD systems include allies, coalition partners, states, other Federal agencies, the National Command Authority and private sector suppliers.

Identifying and fixing computer code that is not Y2K compliant are generally not difficult from the purely technical perspective; however, DoD faces a $2.5 billion cost and a monumental management challenge because of the scale of the conversion problem, a belated start in seriously addressing it, and the legacy of past inattention to good information technology management principles. As of January 1999, approximately 77 percent of mission critical systems have been certified as Y2K compliant. The Department is intensively managing the remaining non-compliant systems and other facets of the problem, such as determining the readiness of suppliers and other countries. During the past few months, the pace of the DoD effort has accelerated significantly and the critical system end-to-end testing and operational evaluations are now beginning. We believe that the number and severity of the

remaining Y2K conversion issues will not be readily apparent until at least June 1999, when more testing results are available. This is our top discretionary audit priority and we have issued about 50 reports on it over the last year and a half.

Other Information Technology Issues. As indicated in 21 recent audit reports, the DoD faces major problems related to the acquisition of computer systems and the security of both old and new systems. Currently the Department is attempting to develop a new generation of better integrated automated systems. Virtually every business sector--procurement, supply, transportation, finance and others--is significantly changing its processes and relies heavily on the introduction of new systems to support those new processes. The number of system acquisition migration and modification projects therefore is huge. This poses a formidable management challenge, because the DoD track record for automated system development has not been good for many years. Projects have tended to overrun budgets, slip schedules, evade data standardization and interoperability requirements, and shortchange user needs. The huge effort needed to develop an accurate inventory of DoD information systems and their interfaces in order to assess vulnerability to the year 2000 computing problem has underscored the need to

revamp the lax management controls that led to the runaway proliferation of systems.

With passage of the Clinger/Cohen Act, the DoD has been challenged, like other Government agencies, to improve its processes for information technology resource investments. The Department has sought to implement both the Clinger/Cohen Act and other acquisition reform measures simultaneously. We have concerns that a good balance has not yet been found to allow system program managers enough flexibility to promote innovation, while maintaining an effective management oversight structure to assure that DoD priorities are met and the $10 billion annual DoD information technology budget is wisely spent. For example, audits have indicated that cost, schedule and performance baselines are not always established for information system development projects.

The conflicting priorities confronting system developers and users, the technology-driven trend toward open systems, and the still unproven new management oversight mechanisms appear to be complicating the already difficult DoD information assurance problems. Audits continue to show lax security measures and inadequate focus by program managers on the threat, despite clear awareness at senior levels of the need for a very high

priority for information assurance. Estimates of the number of intrusions attempted by hackers into DoD systems each year run as high as 250,000. It is likely that Y2K conversion is temporarily distracting both resources and management attention from security concerns.

Positive developments in this area include the recent formation of the Computer Network Defense Joint Task Force, which is led by the Deputy Director, Defense Information Systems Agency. The Task Force will coordinate and spearhead DoD efforts to detect and react effectively to hacking and other attacks on DoD automated systems. The Defense Criminal Investigative Service has established a Defense Information Infrastructure Intrusion Investigation Team, which works with Military Department agents in what we term the DoD Law Enforcement and Counterintelligence Cell to support the Joint Task Force. Common criminal schemes involve unauthorized individuals or groups gaining access to DoD systems for purposes of theft of technological information, defacement of websites or other vandalism, including denial of service. Due to the global nature of the threat, we coordinate extensively with the National Infrastructure Protection Center and other Federal law enforcement agencies on significant computer intrusions which affect the Defense Information Infrastructure. Information is also provided to other

governmental law enforcement agencies when it is determined that systems under their investigative cognizance have been compromised.

Other Infrastructure Issues. Disagreements between the DoD and Congress over additional base closures and the distribution of workload between DoD and private sector maintenance facilities are major impediments to driving down the Department's support costs. As with supply management, other key infrastructure areas such as transportation, maintenance and facilities offer many opportunities to cut costs; however, many logical measures are highly controversial and it is important not to create readiness shortfalls when trimming infrastructure.

The DoD is attempting to control overall environmental costs through a wide variety of measures, including more upfront emphasis during weapon system or facility design on avoiding the use of hazardous materials. At our urging, the Department also began a pilot program at 18 installations to test the feasibility of using ISO 14001, which is an international standard on environmental management systems to improve their effectiveness, especially in identifying emerging requirements. The pilot program includes partnerships with environmental regulators. Despite these positive actions, however, this

remains an area where cost containment is difficult and there is a significant criminal threat in matters such as hazardous waste handling. Currently we have about 50 open criminal investigations related to environmental matters. Defense Criminal Investigative Service cases in this area over the past five fiscal years have lead to 56 convictions and $14.2 million in recoveries.

Difficulty in collecting reliable cost information with which to make outsourcing or restructuring decisions is another major infrastructure management problem. Audits also indicate continued problems in determining facility requirements, especially for housing, where estimates of the cost of modernizing DoD facilities run as high as $30 billion. The Department also continues to struggle with finding the correct sequence between business process reengineering, outsourcing decisions and staff reductions. We have issued 49 audit reports in the diverse infrastructure area since October 1997.

Readiness. The difficulties in maintaining sufficient military readiness recently have been the subject of congressional hearings, public dialogue and the President’s budget themes for FY 2000. My office has not performed any recent evaluations of military personnel recruiting or retention. We have, however,

assessed how readiness posture is affected by the changing threat environment, which now includes bona fide information warfare threats and concerns about weapons of mass destruction in the hands of terrorists. Accurate reporting of unit level readiness status remains a major concern. In addition, audits have indicated weaknesses related to chemical and biological defense preparedness and communications capability. We have issued 12 reports on matters directly related to readiness since October 1997. Our audit coverage of readiness issues has been severely impacted by resource constraints and audit requirements related to the year 2000 problem.

Turbulence From Change. For most of the past decade and for perhaps the first time, all functional areas within the DoD have been engaged in fundamental reform and process reengineering efforts at the same time. This is a promising trend, because those areas are interlinked and piecemeal reform has generally failed in the past. The Department confronts a huge task, however, in coordinating and integrating the hundreds of reform initiatives so that they do not work at cross purposes with each other or overwhelm the work force. In addition, the turbulence created by wholesale change brings additional difficult challenges.

Conflicting priorities, downsizing, outsourcing, dependence on new and unproven systems or processes, deemphasis on management controls and oversight, reorganization, sustained requirements growth despite resource constraints, and the continued, unexpectedly intensive, need for frequent US military deployments are putting considerable strain on the Department's human resources. This turbulent period is one of increased vulnerability to waste, fraud and mismanagement.

The Department can best mitigate that increased risk by paying careful attention to the need to improve, not eliminate, internal controls. One of the best ways to do so is to maintain a robust DoD audit and investigative effort. Until recently the trend has been in the wrong direction. Severe cutbacks in my office's audit and investigative resources between 1995 and 1999 have reduced coverage in most of the high risk areas discussed in this testimony. Fortunately, the Department recently altered its plan for further resource reductions in my office, but we remain stretched very thin at a time of critical change within the Department.

Summary

As the largest and most complex government agency in the world, the DoD faces huge management challenges. In all of the areas that I have discussed, there is a mix of significant recent progress toward reform and continuing major problems. Generally, the Department has been very supportive of our anti-fraud activities and also responsive to audit advice on how to improve management in these risk areas. Managers have agreed with about 96 percent of our audit recommendations and have completed action on over 5,200 audit recommendations over the past five years, realizing estimated monetary benefits of $18.6 billion.

To assist the Congress in its oversight role, we will continue to provide copies of all audit and evaluation reports to about a dozen congressional committees and subcommittees, including yours. Summaries of examples of our individual audit reports and closed criminal cases are attached to this statement. In addition, we will continue highlighting DoD high risk areas in the semiannual reports from my office to the Congress.

Thank you again for your interest in and support for our work at the Department of Defense.

Attachment

Examples of Recent Inspector General,
Department of Defense, Reports on
Defense High Risk Areas and
Closed Criminal Investigations

Report No. 99-069, Summary of Audit Results—DoD Information Assurance Challenges, January 22, 1999.

The DoD Annual Statements of Assurance for FYs 1996 through 1998 identified a material management control weakness in the area of information systems security. Audits have been an important tool in identifying that weakness. In February 1997, the General Accounting Office designated information security as a high risk area throughout the Federal Government, because weaknesses in information security, in the face of the growing threat, could cause critical Government operations to be highly vulnerable to waste, fraud, abuse, and mismanagement. Some DoD estimates of the number of annual hacker attacks on DoD systems run as high as 250,000. This report summarizes 79 reports and reviews pertaining to DoD organizations or functions and their information assurance efforts. The most common finding was poor internal access control. The results of the audits support the need for a more sustained DoD information assurance effort.

Report No. 99-061, M41 Protection Assessment Test System Capabilties, December 24, 1998.

The M41 Protection Assessment Test System is a portable instrument designed for face-fit-testing nuclear, biological, and chemical protective masks. The Army has procured 5,954 M41 Protection Assessment Test Systems for the Army, Navy, Air Force Marine Corps, and surety sites.

The audit followed up on our previous work concerning the adequacy of protective equipment and related test criteria. We concluded that, while progress had been made, several issues remained open. Those issues included the suitability of the M41 tester as an operational or combat condition tester, Army fit-factor criteria, uncalibrated testers and training for users of the system.

The Office of the Secretary of Defense generally concurred with the report, but the Army comments to the draft report were nonresponsive and we requested reconsideration. We await additional Army comments to the final report. If open issues remain, DoD audit followup procedures provide for the Deputy Secretary of Defense to adjudicate such matters.

Report No. 99-059, Summary of DoD Year 2000 Conversion—Audit and Inspection Results, December 24, 1998.

This report summarizes 142 audit and inspection reports, reviews and memorandums pertaining to DoD organizations or functions and their year 2000 conversion progress. The reports were issued from August 1997 to December 1998. The most commonly identified problems were initial lack of management attention to the conversion challenge, poor contingency planning, insufficiently rigorous assessment of system vulnerability, premature certification of system compliance, lack of information on suppliers and other countries, infrastructure issues, insufficient coordination of test plans and inaccurate status reports. Management concurred with virtually all findings and took numerous corrective actions.

Report No. 99-012, Use of Funds Appropriated for Major Defense Systems, October 14, 1998.

Nine of ten major program offices in the audit sample lacked cost accounting systems to track and report program costs by functional categories, such as systems engineering, program management, logistics, departmental assessments, test and evaluation, and acquisition of weapon-systems hardware and software from prime contractors. Because the nine programs that we reviewed did not have cost accounting systems, we used budget execution reports to identify functional cost categories within the various appropriations and detailed cost activities associated with those cost categories.

The program offices for the 10 systems reviewed used an average of about 69 percent of their program dollars to fund prime contractors for the development and acquisition of weapon systems hardware and software. Those offices also used an average of about 31 percent of their funds for other than weapon systems hardware and software acquisition. The other costs involved management tasks prescribed by DoD regulations and mission support. In addition, Congress and various DoD management levels directed realignment of program funds for a wide range of other requirements. Examples were small business innovative research, working capital fund cash shortfalls, Bosnian operations and anti-terrorism initiatives. Because the DoD has several initiatives under way to reduce overhead, improve cost accounting, and achieve better acquisition program stability, we made no additional recommendations. However, the report illustrates some of the reasons why procurement funds do not stretch as far as initially planned for most programs. Management concurred with the report.

Report No. 99-009, Coordination of Electromagnetic Frequency Spectrum and International Telecommunications Agreements, October 9, 1998.

At least 89 weapons and telecommunications systems were deployed within the European, Pacific, and Southwest Asian theaters without the proper frequency certification and host-nation approval. In addition, the Military Exchanges were selling products that were not covered by or compliant with host-nation frequency agreements. As a result, much equipment deployed without host-nation approval and frequency assignments cannot be utilized to full capability for training, exercises, or operations without risking damage to host-nation relations and degraded performance. The program costs associated with 15 of the 89 systems, whose use is hampered in foreign nations, totaled almost $39.5 billion.

The DoD did not periodically evaluate the validity of international telecommunications agreements with allied nations, providing a strategy of coordinating accountability of international telecommunications agreements throughout the communications management community, or ensure that the unified commands and Defense Information Systems Agency complied with existing policies and guidelines governing international telecommunications agreements. The most recent register of telecommunications agreements published by the Defense Information Systems Agency was over 4 years old. As a result, the ability to plan, manage, and properly allocate scarce telecommunications resources is hampered and telecommunications support to the two major theater war scenarios may be impaired.

Management generally concurred and corrective actions are being initiated.

Report No. 98—168, DoD Implementation of the National Practitioner Data Bank (NPDB) Guidelines, June 26, 1998.

At the request of the Assistant Secretary of Defense (Health Affairs), we reviewed procedures for reporting DoD health care practitioners associated with malpractice payments or subjected to adverse privileging actions.

Although DoD reporting of malpractice payments to the NPDB was incomplete, it conformed to DoD policy, which mandated only partial reporting. Of the 124 malpractice payment records reviewed, 87 (70 percent) had not been reported to the NPDB, and those reported had not been submitted in a timely manner. As a result, the NPDB had incomplete and untimely information and health care entities did not have all relevant information available for making credentialing and privileging decisions.

We did not believe that the DoD partial reporting policy conforms to congressional intent or Department of Health and Human Services preference. Management comments to the report were responsive and corrective action is being taken.

Report 98-155, Depot Source of Repair Code, June 15, 1998.

The audit was suggested by the Joint Logistics Commanders. The overall objective was to evaluate controls over the depot source of repair (DSOR) coding process. Specifically, we reviewed the procedures and controls DoD personnel used to ensure accurate code input and transfer to the Federal Logistics Information System. The intent of DSOR coding is to facilitate efficient logistics support planning.

Of 410,308 coded nonconsumable items, an estimated 268,104 (65.3 percent) were inactive. For the remaining active items, an estimated 108,973 (26.7 percent of 410,308 total items) had erroneous DSOR codes. Consequently, DoD maintenance managers were not always aware of established depot repair capabilities including duplicate maintenance facilities for 38 of 145 active items reviewed. This situation contributes to the excess capacity in the DoD depots and hampers the efficiency of the maintenance program. Management concurred.

Report No. 98-072, Defense Business Operations Fund Inventory Record Accuracy, February 12, 1998.

This was the fourth in a series of reports on Defense Business Operations Fund (DBOF) inventory issues. The overall objective of the audit was to determine whether inventory amounts on the FY 1996 DBOF consolidated financial statements were presented fairly in accordance with the comprehensive basis of accounting described in OMB Bulletin No. 94-01.

The DBOF inventory records were not accurate. An estimated 15.8 percent, or about one of every six inventory records represented by our sampling, was in error. The errors caused inventory records to be misstated (overstated and understated) by an estimated $3.9 billion. The net misstatement resulting from those errors was an estimated $336.3 million understatement of the $89 billion of on-hand inventory used to prepare FY 1996 DBOF financial statements. That net amount of error made the value of DBOF inventory on the financial statements appear accurate because the overstated amounts offset most of the understated amounts. However, the 15.8 percent error rate represented a material management control weakness. The inaccurate records greatly limited the reliability of the financial data. Inaccurate inventory records also distorted the reports used by inventory managers. Additionally, the inaccurate records can

reduce the effectiveness of logistics support when military customers urgently need inventory. The DoD Inventory Control Points and Retail Storage Activities did not implement a plan to conduct an annual statistical sample of the FY 1996 DBOF inventory as required by DoD policy.

Management concurred with the report, which illustrates one of the many impediments to favorable audit of opinions on DoD financial statements.

Report No. 98-063, Defense Logistics Agency Product Quality Deficiency Program, February 5, 1998.

We initiated the audit in response to a request from the Director, Defense Logistics Agency (DLA). We determined whether defective products were reported by customers and, if reported, whether they were promptly investigated and corrected. We also reviewed progress in establishing and implementing the DoD-wide Deficiency Reporting System Program.

The DLA was correct in assuming there were ways to improve the product quality deficiency program. Deficiency reports were initiated when nonconforming materials were identified, and investigations into the causes of the deficiencies were promptly conducted. However, DLA product quality deficiency investigations did not always adequately identify the cause of the reported product deficiencies. As a result, the inventory control points missed opportunities to identify contractors with performance problems, and improve product quality. Also, the DLA Automated Best Value System for tracking contractor past performance did not fully reflect contractor quality problems. As a result, DLA increased its risk of procuring products from contractors with poor past performance. Management concurred.

Report No. 98-064, Commercial and Noncommercial Sole-Source Items Procured on Contract N000383-93-G-M111, February 6, 1998.

This was the first of a series of reports in response to Defense Hotline complaints that for sole-source commercial items (spare parts) DLA paid contractor catalog prices that were several hundred percent higher than the cost-based prices DLA previously paid for the items. The primary audit objective was to determine whether there was merit to the complaints.

The complaint was substantiated, although no laws were broken. The DLA paid modestly discounted catalog prices that were significantly higher than the cost-based prices DoD previously paid for the items. For CYs 1994 through 1996, DLA paid about $4.5 million (in 1997 constant dollars) or an average of about 280 percent more than fair and reasonable prices for the

$6.1 million of commercial items procured under this contract. The DLA contracting officers also did not effectively negotiate prices for other (noncommercial) sole-source items. Through cost analysis, we determined that DLA paid about $1 million (or more than 30 percent) above the fair and reasonable price.

In response to the audit, DLA awarded an indefinite-delivery corporate contract for 216 sole-source commercial items at prices DLA considered fair and reasonable. Estimated savings over a 6-year period are $83.8 million. The DLA is seeking a similar pricing arrangement for 1,567 other sole-source noncommercial items.

Report No. 98-025, Management and Administration of International Agreements in the Department of Defense, November 19, 1997.

This report was the second in a series addressing the management and administration of international agreements in DoD, based on observations and information available within the Office of the Secretary of Defense, the Joint Staff, the U.S. Pacific Command, and the U.S. Central Command. The overall audit objective was to evaluate whether the management and administration of international agreements between the U.S. and the countries in Southwest Asia and the Pacific Region support joint operations. We also evaluated whether the international agreements effectively met the requirements of U.S. Forces in support of U.S. national interests.

The DoD is not adequately overseeing the management and administration of its many thousand agreements with other countries. The DoD elements have not effectively inventoried, analyzed, and updated those agreements and planners lack sufficient information concerning them. Management concurred.

Report No. 98-023, Implementation of the DoD Joint Technical Architecture, November 18, 1997.

The objective was to assess progress in implementing information processing standards as a means of achieving systems interoperability. Specifically, we reviewed DoD guidance and plans for implementation of the Joint Technical Architecture (JTA).

The DoD did not have an integrated or coordinated approach to implementing JTA. As a result, DoD had little assurance that JTA would meet interoperability goals or DoD would efficiently use the over $10 billion invested annually in information technology.

Management concurred.

Report No. 98-006, DoD Family Housing Requirements Determination, October 8, 1997.

The House National Security Committee Report accompanying the National Defense Authorization Act for FY 1996, Report No. 104-131, June 1, 1995, questioned the different methodologies used by the Services for measuring available housing for military families in local housing markets surrounding military installations. Based on the Report, we performed a detailed comparison of the different methods used by each Service to evaluate available housing in local markets and an analysis of the appropriateness of a Department–wide standard for the housing market analysis.

The Services use different policies, processes and procedures to incorporate what they perceive as their particular needs into housing planning. Those practices vary significantly in cost and do not produce comparable results for determining the family housing requirements. As a result, OSD and Congress do not have sufficient assurance that current family housing construction budget submissions address the actual family housing requirements of the Services in a consistent and valid manner. Management concurred.

OCT 15 1998

MEMORANDUM FOR CORRESPONDENTS

The Office of Inspector General (OIG), Department of Defense (DoD), announced today that on October 13, 1998, Judge H. Dale Cook, U.S. District Court, Tulsa, OK, sentenced the following individuals for conspiracy to defraud the Federal Government: T. Robert Hughes, an attorney from Fort Collins, CO, to 24 months imprisonment, 3 years supervised probation, to pay $236,158 in restitution to the U.S. Army Corps of Engineers (USACOE) and a $50 special assessment; Stephen L. Schluneger, Scottsdale, AZ, to 12 months imprisonment, 3 years supervised release, to pay $10,000 restitution and a $50 special assessment.

Also indicted and convicted in the-case was Thomas S. Rhoades, Colorado Springs, CO. Rhoades died of natural causes on June 21, 1998. ARCO Properties, Limited, and ARCO Business Services, two business trusts controlled by Hughes, were also convicted during the trial in February 1998. ARCO Properties was placed on 3 years probation and ordered to pay restitution of $236,115.03 and a special assessment of $200. The jury convicted ARCO Business Services during the same trial but found the entity had quit the conspiracy. Judge Cook dismissed the count based on a motion by the defense.

Rhoades and Schluneger were personal sureties on a USACOE contract to sandblast and paint the gates of the locks and dams on the Arkansas River in Oklahoma. When the contractor defaulted, Rhoades and Schluneger signed a takeover agreement to complete the work. They, along with Hughes, an attorney and trustee of ARCO Business Services and ARCO Properties, devised a scheme to defraud the Government. After the contractor defaulted, there was $1,642,739.81 remaining on the contract. As sureties, Rhoades and Schluneger were limited to costs and expenses by the takeover agreement. They found a subcontractor, Skyline Painting (Skyline), who agreed to complete the work for $1.2 million. Rhoades and Schluneger never informed the USACOE about the subcontract agreement. As progress payments were made by the USACOE to Rhoades and Schluneger, payments were made to Skyline. However, Skyline was required to pay the ARCO entities 29 percent of the gross as a finder's fee and for engineering consulting services, which were bogus charges. The ARCO entities kept a share of each payment, then paid a kickback to Rhoades and Schluneger. By the time Skyline was forced to discontinue work on the project, due to losses as a result of floods, Rhoades, Schluneger and Hughes had stolen $236,000.

The investigation was conducted by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD). The prosecution was handled by Assistant U.S. Attorney Gordon Cecil, Tulsa, OK.

-END-

AUG 24 1998

MEMORANDUM FOR CORRESPONDENTS

The office of Inspector General (OIG), Department of Defense (DoD), announced today that on August 20, 1998, Charter Hospital Orlando South (Charter Hospital), Kissimmee, FL, reached an agreement with the Department of Justice (DoJ) to pay $4.7 million to settle a civil complaint. Two former employees of Charter Hospital filed the complaint on November 6, 1994

An investigation, found that Charter Hospital improperly admitted and retained patients for psychiatric treatment who were actually suffering from dementia, organic brain disorders and symptoms of Alzheimer's Disease. The investigation determined that Charter Hospital personnel knew such treatment was not medically necessary for patients with those conditions. The patients included individuals covered by TRICARE, which is the DoD medical program that pays the medical bills of military retirees, dependents and other specified individuals who receive medical care from civilian doctors and facilities. The investigation further found that Charter Hospital personnel falsified patient medical records in order to receive Government reimbursement.

The investigation was conducted by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD). T. Reed Stephens, Trial Attorney, Civil Division, DoJ, handled the prosecution.

-End-

JUL 24 1998

MEMORANDUM FOR CORRESPONDENTS

The Office of Inspector General (OIG), Department of Defense (DoD), announced today that on July 24, 1998, Charles Cagegia was sentenced in U.S. District Court, Eastern District of New York, by Judge Arthur Spatt. Cagegia was sentenced to 21 months in prison, followed by 3 years supervised release, a fine of $9,000 and a $200 special assessment fee.

On January 29, 1998, a Federal grand jury returned a one-count indictment against Cagegia charging him with a conspiracy to defraud the Internal Revenue Service (IRS) by committing corporate income tax evasion. On April 21, 1998, a one-count criminal information was filed against Cagegia charging him with a separate conspiracy to defraud the IRS by committing corporate tax evasion. On April 24, 1998, Cagegia pled guilty to both the indictment and the information.

Cagegia operated various businesses, including messenger services operated under the names of We-Go Express and CKD Corporation and trucking companies under the names of Suffolk Distributing and Marietta Trucking. The indictment was the result of an ongoing investigation into Royce Aerospace Materials Corporation (Royce), Farmingdale, NY, a former DoD subcontractor that provided raw materials such as aluminum and titanium to prime DoD contractors. Between 1990 and 1996, Robert Berger, as president of Royce, conspired with Cagegia by devising a fictitious invoicing scheme that was used to generate cash out of Royce.

As part of the conspiracy, Cagegia provided the names of numerous fictitious companies to Berger. Checks were then written and issued from Royce to these fictitious companies and delivered back to Cagegia. Cagegia then cashed these checks through various methods, including bank accounts held under his various business names. The cash was then delivered back to Berger, less a fee kept by Cagegia, and was used to pay kickbacks to prime DoD contractors.

The criminal information charged that between 1989 and 1996, Cagegia’s various businesses received checks from customers for work performed. These checks were then deposited to the same bank accounts held by Cagegia that were used to cash Royce checks. Cagegia then withdrew this money by writing checks to fictitious individuals and/or to himself and cashing these checks through various “check cashers.” Cagegia failed to file corporate tax returns on the income he received from these various businesses.

This investigation was conducted jointly by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD) and the Internal Revenue Service. Prosecution was handled by Trial Attorneys Barry Jonas and David Bloch, Tax Division, Department of Justice.

-END-

APR 13 1998

MEMORANDUM FOR CORRESPONDENTS

The office of Inspector General (OIG), Department of Defense (DoD), announced today that on April 9, 1998, the Raytheon Company (Raytheon), entered into a civil settlement agreement with the Government in which Raytheon agreed to pay $2.7 million. The agreement settles allegations that Raytheon charged the Government for costs that Raytheon had incurred in marketing its products to foreign governments.

Since 1986, Raytheon's cost accounting procedures have provided for separate accounting treatment of foreign marketing costs and domestic marketing costs. These procedures, and the Cost Accounting Standards of the Federal Acquisition Regulations, require that Raytheon's foreign marketing costs be allocated to contracts between Raytheon and its foreign customers and that domestic marketing costs be allocated to Government contracts. The Government has asserted that most of the activities of the Raytheon international development function were foreign marketing activities and that Raytheon improperly classified the costs as "division administration" costs allocable to Government contracts, when they were not.

The investigation was conducted by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD), with audit assistance from the Defense Contract Audit Agency. The negotiation of the settlement agreement was handled by Assistant U.S. Attorney George B. Henderson, District of Massachusetts, Boston, MA.

-END-

NOV 20 1997

MEMORANDUM FOR CORRESPONDENTS

The office of Inspector General (OIG), Department of Defense (DoD), announced today that on November 19, 1997, the McDonnell Douglas Aerospace/Douglas Aircraft Company (DAC), Long Beach, CA, entered into a settlement agreement with the Government in which DAC agreed to pay $3.1 million to resolve a civil complaint filed in U.S. District Court, Central District of California, Los Angeles, CA. The settlement resolves issues relating to cost mischarging on the C-17 Military Transport Plane (MTP) program.

The suit alleged that DAC accepted defective, nonconforming tooling items from subcontractors for the C-17 MTP, in order to maintain the appearance of meeting production milestones and to obtain progress payments. It was also alleged that DAC reworked some of the defective tooling and billed the rework under its prime contract with the Government, thereby double-billing the Government for the same tool.

The DAC, without admitting liability, agreed that of the $3.1 million settlement they would pay a contract adjustment on the C-17,MTP program of $2 million in the form of an immediate payment to the Government. The remaining $1.1 million would settle the relator's attorney fees and costs.

The investigation was conducted by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD). Civil prosecution was handled by Attorney David Cohen, Commercial Litigation Division, U.S. Department of Justice.

-End-

OCT 7 1997

MEMORANDUM FOR CORRESPONDENTS

The Office of Inspector General (OIG), Department of Defense (DoD), announced today that on October 6, 1997, Andrew S. Shankman was sentenced by Judge Anthony A. Alaimo in U.S. District Court, Southern District of Georgia, Brunswick, GA, to 87 months incarceration, 3 years supervised release, 400 hours community service, while under supervised release, and a $6,300 special assessment fee.

Shankman was found guilty by a jury trial on June 27, 1997, of 125 counts of conspiracy, mail fraud, wire fraud, dispensation of controlled substances and money laundering. An investigation disclosed that Shankman and his company, Shankman/Davidson Psychiatric Management, Incorporated, employed unlicensed therapists to provide mental health services to beneficiaries of the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), Medicare and Medicaid, then billed the Government programs as if Shankman provided the services. The CHAMPUS (now called TRICARE) is the DoD program that pays the medical bills of military retirees, dependents and other specified individuals who receive medical care from civilian doctors and medical facilities. From 1992 through 1995, Shankman/Davidson received over $5.2 million from the Government programs.

The investigation was conducted by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD), the Federal Bureau of Investigation, the Internal Revenue Service, the Georgia Department of Medical Assistance and the Georgia Secretary of State Office. Prosecution was handled by Assistant U.S. Attorney Jeffrey J. Buerstatte, Southern District of Georgia, Savannah, GA.

-End-

SEP 22 1997

MEMORANDUM FOR CORRESPONDENTS

The office of Inspector General (OIG), Department of Defense (DoD), announced today that on September 19, 1997, Teasa Hutchins Jr., Temple Hills, MD, was sentenced by Judge Albert V. Bryan in U.S. District Court, Eastern District of Virginia, Alexandria, VA, to 21 months in prison, followed by 3 years supervised probation, ordered to pay $168,772 in restitution and a $100 special assessment fee. Sentencing was the result of a June 23, 1997, guilty plea by Hutchins to one count of embezzlement and theft of public money.

Hutchins was a civilian employee assigned as a military pay supervisor in the Finance and Accounting office, Military District of Washington, Fort Myer, VA. From December 1994 through April 1997, Hutchins misused his supervisory authority and his specialized knowledge of military pay and the operations of the Defense Finance and Accounting Service (DFAS) to embezzle funds. Hutchins was terminated from employment at DFAS following his guilty plea.

When he pled guilty, Hutchins admitted to defrauding the U.S. Government by embezzling approximately $168,772 and converting the monies for personal use. Hutchins admitted that he carried out his scheme by fabricating a Social Security Number and subsequently created a ghost account in the name of a fictitious military member, Carol M. Jones, Lieutenant Colonel, U.S. Army. Hutchins admitted he had falsified various documents, forged signatures, and input the false information into the DFAS military pay computer system in order to generate and control payments to the "LTC Jones" pay account. Hutchins then used the ghost pay account to cause the DFAS over a 28-month period to make a total of 57 electronic fund transfers (EFT) of "LTC Jones" pay and allowances to bank accounts owned by Hutchins and his girlfriend. To initially conceal his receipt of the money, Hutchins had the first three EFTs, totalling approximately $8,500, deposited into his girlfriend's checking account in exchange for cash kickbacks.

Hutchins had fled to Ohio to avoid prosecution. Before he was arrested, he had spent approximately $10,000 of the approximately $52,000 under his control that he had previously agreed to pay back to the Government. In part payment, Hutchins has thus far repaid the Government approximately $46,460 and has agreed to apply the proceeds of the sale of his real and personal property toward full restitution.

The investigation was conducted by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD), and the U.S. Army Criminal Investigation Command (USACIDC). Prosecution was handled by Assistant U.S. Attorney Daniel L. Bell II, Eastern District of Virginia, Alexandria, VA.

- End -

JUL 24 1997

MEMORANDUM FOR CORRESPONDENTS

The Office of the Inspector General (OIG), Department of Defense (DoD), announced today that on July 23, 1997, Leo Anthony Piatz, Jr., was sentenced in U.S. District Court, Western District of Wisconsin, Madison, WI, by Judge Barbara B. Crabb. Piatz was sentenced to 97 months confinement, 36 months of supervised probation and a $600 special assessment. Piatz was found guilty of 11 counts, to include, conspiracy, bribery and unlawful conversion of Government property. A decision on restitution will be made at a later date.

On March 11, 1997, Piatz was found guilty after evidence at trial established that he gave money and other items of value to various individuals, including civilian U.S. Army employees at Ft. McCoy, WI. In return, Piatz was allowed to remove military vehicles and heavy equipment from Ft. McCoy. The equipment illegally removed included TOW missile launchers, M548 cargo carriers, snow blowers, a Sheridan Tank, a bulldozer, a 20-ton crane and forklifts. Piatz, and others, sold, traded or provided as gifts, the property taken from Ft. McCoy.

This investigation was conducted jointly be the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD) and the Federal Bureau of Investigation. The prosecution was conducted by Assistant U.S. Attorney's Dan Bach and Rita Klemp, Madison, WI.

-End-

MAY 21 1997

MEMORANDUM FOR CORRESPONDENTS

The Office of Inspector General (OIG), Department of Defense (DoD), announced today that on May 20, 1997, United Technologies Corporation, Pratt & Whitney (P&W), Government Engine and Space Propulsion Division, West Palm Beach, FL, entered into a settlement agreement with the Government in which P&W agreed to pay $14.8 million to resolve a civil complaint filed by the Department of Justice (DoJ) in April 1995. The civil complaint charged that P&W violated the False Claims Act by preparing false purchase orders and by submitting false invoices under the Foreign Military Sales (FMS) Credit Program administered by the Defense Security Assistance Agency (DSAA). The program involved the FMS-funded Lavi Fighter Aircraft that had been under development by the Israeli Air Force (IAF).

An investigation disclosed that during the course of designing and developing the PW1120 turbojet engine, as part of the Lavi Program, officials of P&W entered into an agreement with Rami Dotan, a former IAF Brigadier General, to submit $10 million in false claims for projects not authorized or approved by either the Israeli government or the DSAA. On August 31, 1987, the Lavi Program was canceled and the contract was amended to have P&W supply, among other things, upgrade kits for the P&W F100 engines installed in the IAF F15 fleet. The investigation further disclosed that upon cancellation of the program, P&W officials agreed to set aside the $10 million to be used at the direction of Dotan and former IAF Lieutenant Colonel Nehemiah Oron. Between 1987 and 1990, over $2 million of the $10 million was paid to Yrretco, Incorporated (Yrretco), and Airtech, Incorporated (Airtech), two New Jersey based subcontractors that were owned by Yoram Ingbir, an Israeli subcontractor and associate of Dotan and Oron. The profits made by Yrretco and Airtech were diverted to accounts controlled by Ingbir in New York, Florida and Switzerland. As part of the settlement, P&W will repay those funds that remained on account with the corporation. Currently, Ingbir is under indictment in Israel for bribery.

The investigation was conducted by the Defense Criminal Investigative Service (the investigative arm of the OIG, DoD), with audit assistance provided by the Defense Contract Audit Agency. Litigation was handled by Trial Attorneys Shelley Slade, Mike Taxay and Benjamin Vernia, Commercial Litigation Branch, DoJ Civil Division, Washington, D.C.

-End-