WASTE, FRAUD AND ABUSE AT THE DEFENSE DEPARTMENT, VETERANS AFFAIRS, AND DEPARTMENT OF STATE

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

FEBRUARY 25, 1999

Serial No. 106–2

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

56–026 CC WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
JOHN T. DOOLITTLE, California
HELEN CHENOWETH, Idaho

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
GARY A. CONDIT, California
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
CARLA J. MARTIN, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

MARK E. SOUDER, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
DAVID M. MCINTOSH, Indiana
MARSHALL "MARK" SANFORD, South Carolina
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
HELEN CHENOWETH, Idaho

ROD R. BLAGOJEVICH, Illinois
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
GARY A. CONDIT, California
JOHN F. TIERNEY, Massachusetts
THOMAS H. ALLEN, Maine
EDOLPHUS TOWNS, New York
BERNARD SANDERS, Vermont (Independent)

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

LAWRENCE HALLORAN, *Staff Director and Counsel*
ROBERT NEWMAN, *Professional Staff Member*
JONATHAN WHARTON, *Clerk*
DAVID RAPALLO, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on February 25, 1999	1
Statement of:	
Hinton, Henry L., Jr., Assistant Comptroller General, National Security and International Affairs Division, U.S. General Accounting Office, accompanied by Steve Backhus, Director for Veterans' Affairs and Military Health Care Issues; Lisa G. Jacobson, Director for Defense Financial Audits; Ben Nelson, Director for International Relations and Trade; Eleanor Hill, Inspector General, U.S. Department of Defense, accompanied by Robert J. Lieberman, Assistant Inspector General; Richard J. Griffin, Inspector General, U.S. Department of Veterans Affairs, accompanied by Michael Sullivan, Assistant Inspector General; and Jacquelyn Williams-Bridgers, Inspector General, U.S. Department of State	3
Letters, statements, etc., submitted for the record by:	
Blagojevich, Hon. Rod R., a Representative in Congress from the State of Illinois, prepared statement of	80
Griffin, Richard J., Inspector General, U.S. Department of Veterans Affairs, prepared statement of	84
Hill, Eleanor, Inspector General, U.S. Department of Defense, prepared statement of	42
Hinton, Henry L., Jr., Assistant Comptroller General, National Security and International Affairs Division, U.S. General Accounting Office, prepared statement of	6
Williams-Bridgers, Jacquelyn, Inspector General, U.S. Department of State, prepared statement of	92

WASTE, FRAUD AND ABUSE AT THE DEFENSE DEPARTMENT, VETERANS AFFAIRS, AND DEPARTMENT OF STATE

THURSDAY, FEBRUARY 25, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:12 a.m., in room 2203, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Biggert, Blagojevich, and Tierney.

Staff present: Lawrence Halloran, counsel; J. Vincent Chase, chief investigator; Robert Newman, professional staff member; Jonathan Wharton, clerk; David Rapallo, minority counsel, and Ellen Rayner, minority chief clerk.

Mr. SHAYS. I am going to call the hearing to order, because I know you all have busy schedules and Members will be coming in and out. I welcome all of you here.

Two weeks ago in testimony before the full Government Reform Committee the Comptroller General, General David Walker, described programs posing a high risk of waste and abuse and "the serious challenges that must be confronted to achieve more efficient, effective and economical Federal operations, and to build greater public respect for and confidence in their Government."

To improve performance and accountability Governmentwide, he called for greater emphasis on program results, closer alignment of organizational structures to program missions and improved coordination of multi-agency or cross-cutting efforts. Today, we invite our oversight partners, the General Accounting Office, GAO, and the Inspector Generals [IGs], to help us answer the Comptroller General's call as we focus on high risk operation and program vulnerabilities at three crucial departments: Defense, State, and Veterans Affairs.

At the Department of Defense [DOD], weak financial controls allowed $1 billion in excess payments to contractors in a single year. Inventory systems cannot account for another $9 billion. Although GAO acknowledges some recent improvements, daunting obstacles confront the effort to bring DOD financial management and financial managers to the level required to support the Department's vastly complex and enormously costly mission.

At the Department of Veterans Affairs, both the GAO and IG note structure and operational issues affecting the quality of health care and chronic problems with the timeliness and integrity of data needed by VA managers to measure performance. At the State Department, GAO points to a number of complex challenges, most notably the need to enhance embassy security, upgrade crucial information and financial systems, and improve goals and measures under the Government Performance and Results Act.

Our oversight mission is to improve the effectiveness and efficiency of national defense, international relations, intelligence and veterans programs. We begin that effort today by asking the GAO and Inspector Generals to address broad but fundamental questions about the mission, management and performance of the departments within their purview, and ours as well. Next Thursday, witnesses from DOD, VA and State Department will address the same issue.

Let me at this time welcome our witnesses: Henry Hinton, Jr., Assistant Comptroller, National Security and Internal Affairs Division, U.S. General Accounting Office, accompanied by Steve Backhus, Director for Veterans Affairs and Military Health, Lisa Jacobson, Director for Defense Financial Management, and Ben Nelson, Director for Internal Relations and Trade.

Also we have Eleanor Hill, Inspector General, U.S. Department of Defense, accompanied by Robert J. Lieberman, Assistant Inspector General, U.S. Department of Defense. Then we have Richard Griffin, Inspector General, U.S. Department of Veterans Affairs, accompanied by Michael Sullivan, Assistant Inspector General, U.S. Department of Veterans Affairs. Finally, we have Jacquelyn Williams-Bridgers, Inspector General, U.S. Department of State.

I know we have a lot of you here. We could have had two separate panels. This is a general overview. It is really to acknowledge the fact that you all are the most important part of this process, and to begin some dialog. Some of what we are going to do is going to be a bit superficial, since we obviously are not going to have just one of you here talking in real depth about the issue. Obviously we are going to have you speak for more than 5 minutes, because even though there are a lot of you, we need to, and I know some are accompanying and not making statements, but it is important to put on the record some key points.

So we are going to be doing a little bit more listening today than asking. But I do need to, before we begin, to swear you in. I will also say to you that, you wonder, do I do the GAOs first, the Inspector Generals, we are all a family here, we are partners. Sometimes the Inspector General will go first and sometimes the GAO will go first and sometimes they will come separately and all that stuff.

Would all of you please rise, and raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. Thank you. We will note for the record that everyone responded in the affirmative. And we are going to go in the order that I called you. Mr. Hinton, you can begin, then we will go to Eleanor Hill and then to Richard Griffin, and then to Jacquelyn Williams-Bridgers.

STATEMENTS OF HENRY L. HINTON, JR., ASSISTANT COMPTROLLER GENERAL, NATIONAL SECURITY AND INTERNATIONAL AFFAIRS DIVISION, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY STEVE BACKHUS, DIRECTOR FOR VETERANS' AFFAIRS AND MILITARY HEALTH CARE ISSUES; LISA G. JACOBSON, DIRECTOR FOR DEFENSE FINANCIAL AUDITS; BEN NELSON, DIRECTOR FOR INTERNATIONAL RELATIONS AND TRADE; ELEANOR HILL, INSPECTOR GENERAL, U.S. DEPARTMENT OF DEFENSE, ACCOMPANIED BY ROBERT J. LIEBERMAN, ASSISTANT INSPECTOR GENERAL; RICHARD J. GRIFFIN, INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY MICHAEL SULLIVAN, ASSISTANT INSPECTOR GENERAL; AND JACQUELYN WILLIAMS-BRIDGERS, INSPECTOR GENERAL, U.S. DEPARTMENT OF STATE

Mr. HINTON. Thank you, Mr. Chairman. I am pleased to be here today to discuss major management challenges and program risks confronting the Departments of Defense, State and Veterans Affairs. As requested, my prepared statement focuses on one, the management challenges Defense, State and VA must address to improve the efficiency of their support operations, and two, whether these departments are meeting performance and accountability goals and measurements that are required under the Government Performance and Results Act of 1993.

With your permission, Mr. Chairman, I would like to have my statement entered into the record and I will summarize.

In summary, Mr. Chairman, four themes emerge from the performance and management challenges we have identified that can adversely affect the operational effectiveness of the departments if not addressed. First, Defense, State and VA are struggling like other Federal agencies to implement the basic results-oriented tenets of performance-based management.

I need to point out right at the start here, Mr. Chairman, that Defense is second to none in its combat effectiveness. But what we are really talking about here are business functions that I think offer a lot of room for improvements in economies and efficiencies of operations.

Too often we find that the Government's performance is limited by a failure to manage on the basis of a clear understanding of the results that agencies are to achieve and how performance will be gauged. This is true of Defense, State and VA. For example, our review of Defense's plans disclose many areas where improvements could be made. The principal shortcoming in Defense's plan centers on weaknesses; in one, establishing results-oriented performance goals with explicit strategies and timeframes for achieving them, and two, addressing what Defense has done or plans to do to resolve its performance management problems that you referred to in your opening statement.

Our review of State and VA's plans identified some strong points, but generally, they fell short of the expectations in the Government Performance and Results Act.

Second, Defense, State and VA depend on information technology to improve their performance and meet mission goals. The chal-

lenge is to ensure that modern information technology practices are consistently defined and properly implemented.

As we all know, resolving the year 2000 computing problem is the most pervasive, time-critical risk facing Government today. For an organization as large as Defense, with over 1.5 million computers, 28,000 systems, 10,000 networks, addressing the year 2000 problem is a formidable task and progress on the year 2000 program is slow.

State, too, has been slow. VA has made progress in addressing its year 2000 challenge, but it still has a number of associated issues to address. For example, VA faces significant information system challenges. It does not know the full extent of its challenges and could face widespread computer system failures at the turn of the century, if the systems cannot distinguish the year 2000 from the year 1900. Thus, veterans who are due to receive benefits and medical care could appear ineligible.

Third, Defense, State and VA must have reliable and timely performance in financial information to ensure adequate accountability, manageable results, and make timely and well-informed judgments. Widespread financial system weaknesses, problems with fundamental recordkeeping, incomplete documentation, and weak internal controls prevented the Government from adequately reporting a large portion of its assets, liabilities and costs.

For example, the material deficiencies in Defense's financial operations represent the single largest obstacle that must be effectively addressed to obtain an unqualified opinion on the entire Government's consolidated financial statements. State received, for the first time, an unqualified opinion on its 1997 statements, but needs to bring its systems into full compliance with Federal accounting and information management requirements.

State also must work on solving related material internal control weaknesses, if it is to adequately protect its assets and have timely, reliable data for cost-based decisionmaking, reporting and performance management.

Fourth, the leading performance-based organizations understand that effectively managing the organization's employees or human capital is essential to achieving results. Only when the right employees are on board and provided with the training, tools, structure, incentives and accountability to work effectively, is organizational success possible.

For example, Defense is a department that has experienced problems in finding and retaining staff with the technical training it needs. To achieve the wide ranging reforms necessary to address its longstanding financial management deficiencies, Defense must upgrade the skills of its financial personnel. Defense's vast financial operations include a cadre of about 32,000 financial management personnel. A survey we completed of over 1,400 key Defense financial managers—individuals often serving in comptroller, deputy comptroller and/or budget officer positions—showed that over half of those folks received no financial training in fiscal years 1995 and 1996.

To summarize, Mr. Chairman, GAO is committed to help the Congress and Federal agencies better serve the American people and prepare for the demands of the 21st century. We have identi-

fied, as my statement points out, the critical challenges facing Defense, State and VA. These challenges, again, if not addressed, can adversely affect the operational effectiveness of these departments.

We stand ready, Mr. Chairman, when we get through with the witnesses, to address your questions.

[The prepared statement of Mr. Hinton follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives

For Release
Expected at
10:00 a.m., EST
Thursday,
February 25, 1999

MAJOR MANAGEMENT CHALLENGES AND PROGRAM RISKS

Departments of Defense, State, and Veterans Affairs

Statement by Henry L. Hinton, Jr., Assistant Comptroller General, National Security and International Affairs Division

GAO/T-NSIAD/HEHS-99-84

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss major management challenges and program risks confronting the Departments of Defense (DOD), State, and Veterans Affairs (VA). Our testimony is derived from a special series of reports we recently issued on this subject entitled Performance and Accountability Series: Major Management Challenges and Program Risks. The series contains separate reports on 20 agencies—one on each of the cabinet departments and on most major independent agencies as well as the U.S. Postal Service. As a companion volume to this series, we have also issued an update to those government operations and programs that our work has identified as "high risk" because of their greater vulnerabilities to waste, fraud, abuse, and mismanagement.

As requested, our testimony today will focus on (1) the management challenges DOD, State, and VA must address to improve the efficiency of their support functions and (2) whether these departments are meeting performance and accountability goals and measurements that are required under the Government Performance and Results Act of 1993.

RESULTS IN BRIEF

For each of the three agencies—DOD, State, and VA—we have identified and reported management challenges that have hampered the efficiency of their support functions in carrying out their missions. To their credit, each of the agencies has implemented a number of initiatives to improve their operations, but more remains to be done. These challenges, many of which have been long-standing in scope, also underscore the critical role that the principles of performance-based management, as embraced in the Results Act, can play in successfully providing the products, services, and results that taxpayers expect.

For many years, we have reported significant problems at DOD that cut across many of its program areas. These problems can be categorized into systemic management

challenges, which deal with issues such as financial management, information management, weapon systems acquisition, and contract management; and program management challenges, which deal with issues related to infrastructure, inventory management, and personnel. DOD has implemented a number of Departmentwide reform initiatives that are intended to improve some of its processes along with key business practices. Despite DOD's military successes, many of DOD's programs and operations are still vulnerable to fraud, waste, abuse, and mismanagement, and need improvement. Overcoming these challenges requires DOD to address the underlying causes, such as cultural barriers and service parochialism, that limit opportunities for change. To address these problems, DOD must have an effective overall strategic plan for the agency and all levels of the organization that includes goals, performance measures, and time frames for completing corrective actions. The Results Act provides the framework for resolving high risk and other problems and for providing greater accountability in DOD's programs and operations. However, DOD has not fully embraced the underlying principles in the Results Act.

In our past and ongoing work at State, we have identified a number of performance and management challenges State faces in carrying out its mission, such as providing enhanced overseas security, upgrading its information systems, strengthening financial accounting and controls, enhancing controls over the issuance of visas, integrating other foreign affairs agencies' functions into the Department, and improving its strategic and performance planning, State is making progress in addressing these issues. For example, State is now devoting substantial resources to developing a strategy to enhance its information management capacity and security as well as its financial management systems. State has also completed strategic and annual performance plans under the Results Act. However, these plans had their strong points but often fell short on meeting Results Act requirements. For example, State's strategic plan addressed neither the potential impact of the consolidation of the foreign affairs agencies on its systems nor the potential for other agencies to have functions duplicative of State's. State's performance plan revealed similar deficiencies.

For many years, we have reported significant management problems at VA. These problems include obsolete infrastructure, poor monitoring of the effects of health service delivery changes on patient outcomes, inadequate data, and ineffective management of non-health-care benefits and management information systems. VA has made progress in developing a framework for managing and evaluating changes in health care service delivery, as required by the Results Act; however, much more needs to be done to achieve Results Act requirements. For example, VA must continue to set results-oriented goals for compensating disabled veterans and develop effective strategies for improving disability claims processing and vocational rehabilitation. VA must also improve its management information to help it ensure that veterans have equitable access to care across the country, that it maintains its capacity to serve special populations, and that it can meet enrolled veterans' demand for care.

CHALLENGES FACING THE DEPARTMENT OF DEFENSE

Managing and overseeing an estimated $1 trillion in assets and annual budget of over $250 billion, or about one-half of the government's discretionary funding, is an enormous task. As the United States begins the new millennium as the world's sole superpower, it continues to lead the world with superior military forces. The effectiveness of U.S. forces is well evidenced by experiences in the Persian Gulf and Bosnia. Also, the Department of Defense (DOD) has implemented a number of Departmentwide reform initiatives that are expected to improve its financial management, information management, and defense weapon systems acquisition processes and other key business practices. However, DOD still faces challenges with many of its key performance and management processes. A number of these challenges have been included on our high risk list for many years (see App. I). Successfully addressing these challenges can yield fiscal dividends that the Department could use to meet priorities such as readiness and modernization needs. The challenges DOD faces can be grouped into two categories: (1) systemic problems with management processes related to plans, finances, information, acquisition, and contracts and (2) specific problems related to infrastructure, inventory, and personnel programs. Summaries of the challenges that need to be addressed follow.

Systemic Management Challenges

Serious Financial Management Weaknesses Persist

DOD continues to struggle to overcome the many problems brought about by decades of neglect and to fully institute sound financial management practices. These problems range from being unable to properly account for billions of dollars in assets to being unable to produce reliable and timely information needed to make sound resource decisions. The most recent audits of DOD's financial statements—for fiscal year 1997—resulted in the identification of serious deficiencies across the full spectrum of DOD's recordkeeping and controls systems. For example:

- DOD has not properly accounted for and reported billions of dollars of property, equipment, inventory, and supplies. Recorded information on the number and location of several military equipment items—such as F-4 engines and service craft—was not reliable, on-hand quantities of inventories differed by 23 percent from inventory records at selected major storage locations, and over $9 billion in known military operating materials and supplies were not reported.

- DOD has not estimated and reported on material environmental and disposal liabilities. While DOD reported nearly $40 billion in estimated environmental cleanup and disposal liabilities for fiscal year 1997, its reports excluded costs associated with military weapon systems or training ranges—these undisclosed liabilities are likely to be an additional tens of billions of dollars.

To achieve the wide-ranging reforms necessary to address its long-standing financial management deficiencies, we have made numerous recommendations to DOD regarding its need to upgrade the skills of its financial personnel and successfully overcome serious design flaws in its financial systems. DOD has many well-intentioned planned and ongoing financial management reform and improvement efforts, such as an action plan to identify short-term initiatives to address DOD's financial reporting deficiencies.

However, until DOD deals with these two key issues, resolution of its financial management problems is unlikely.

Given the seriousness and long-standing nature of these weaknesses in DOD's financial management operations, we are continuing to monitor this area as part of our high-risk program. Taken together, the material deficiencies in DOD's financial operations represent the single largest obstacle that must be effectively addressed to obtain an unqualified opinion on the entire U.S. government's consolidated financial statements. These weaknesses must be effectively addressed if DOD is to put into place the disciplined financial practices needed to produce credible financial information not only for financial statements but also for support of operational and budgetary decisionmaking and maintaining effective accountability over DOD's vast resources.

Information Management and Technology Issues Pose Major Concerns

Information management and technology issues are key DOD management challenges. We are continuing to designate DOD's information technology project management efforts as high risk. A primary short-term concern centers on the implementation of the Year 2000 conversions of date-sensitive information on DOD's computer systems. In February 1997, we designated the Year 2000 problems as a governmentwide high-risk area. Another area of concern is information security for computer systems. Malicious attacks on these systems are an increasing threat to our nation's security.

For an organization as large as DOD—with over 1.5 million computers, 28,000 systems, and 10,000 networks—addressing the Year 2000 problem is a formidable task and progress on the Year 2000 program is slow. In fact, the Office of Management and Budget, in its November 15, 1998, report on federal agencies' progress on Year 2000 conversion, has placed DOD on its "Tier 1" list—those agencies "where there is insufficient evidence of adequate progress." DOD has an enormous effort underway to remediate its mission-critical systems and ensure that its key operational missions will

continue to function after the century date change. However, that effort is at risk. We have issued 10 reports and the DOD IG and audit agencies have issued 130 reports that continue to question the Department's management of its Year 2000 program. For example:

- The Department lacks reliable, timely information on program status.
- Component reports on systems compliance are often inaccurate.
- Contingency plans (developed in the event of system failure) are frequently not executable.
- Inconsistent guidance has led to false starts and uncoordinated efforts.

Another area of major concern is information security. Providing security over DOD's vast array of networked computers is a major challenge. DOD's computer systems are particularly susceptible to attack through connections on the Internet, which Defense uses to enhance communication and information sharing. The Defense Information Systems Agency estimated that attacks numbered in the hundreds of thousands per year and were successful 65 percent of the time and that the number of attacks was doubling each year.

Reports to DOD have included numerous recommendations related to specific control weaknesses as well as the need to establish a defined systems architecture and a comprehensive program for improved information security management. Based on our recommendations and legislative requirements DOD is taking a variety of steps to (1) develop a plan for evaluating, in an operational environment, Year 2000 compliance, and (2) establish the Departmentwide Information Assurance Program to improve and better coordinate the information security-related activities of the military services and other DOD components. A sustained effort will be needed to ensure that these efforts are successful.

Weapon Systems Acquisition Problems Persist

Effectively managing the weapon systems acquisition process continues to be a concern for DOD. Although DOD has increased its procurement budget, it consistently pays more and takes longer than planned to develop systems that do not perform as anticipated. DOD spends about $85 billion annually to research, develop, and acquire weapon systems. Although DOD has many acquisition reform initiatives in process, pervasive problems persist regarding

- Questionable requirements and solutions that are not the most cost-effective available. For example, DOD could have met its strategic airlift requirements and achieved a significant life cycle cost savings by buying fewer C-17s than planned.

- Unrealistic cost, schedule, and performance estimates. For example, in restructuring the F-22 program, it is doubtful that the Air Force can offset the $13-billion projected increase in production costs because many of the cost-cutting initiatives it identified were not well defined.

- Questionable program affordability. DOD tends to overestimate funding that would be available in the future, and underestimate program costs, resulting in the advent of more programs than could be executed as planned. For example, in analyzing the 1998 Future Years Defense Program, we found that funding for infrastructure activities was projected to increase, while procurement funding was projected to be lower than anticipated.

- The use of high-risk acquisition strategies. Acquisition strategies such as the acquisition of weapons based on optimistic assumptions about the maturity and availability of enabling technologies were being based on the need to meet the threat and to reduce acquisition costs. For example, DOD's approval of the Joint Surveillance Target Attack Radar System's full-rate production was premature and

risky because the system's operational effectiveness and suitability for combat were not yet demonstrated and plans to address deficiencies and reduce program costs were not completed.

Acquisition reforms under way by DOD have a sound basis and have the potential for improving the outcomes of weapons systems. Acquisition reforms and commercial practices can help produce better outcomes on DOD acquisitions if they help a program succeed in its environment.

Improved Processes and Controls Key To Reducing Contract Risk

DOD spends over $100 billion a year contracting for goods and services. Since 1995, we have reported DOD contract management as a high-risk area. Over the last few years, DOD has made several broad-based changes to its acquisition and contracting processes to improve DOD-contractor relationships and rules. DOD has given attention to acquisition reform initiatives, but we continue to identify risks in DOD's contracting activity, including areas such as erroneous, fraudulent, and improper payments to contractors; payment of higher prices for commercial spare parts than necessary; and the award and administration of DOD health care contracts.

The need for DOD to achieve effective control over its payment process remains an imperative. DOD receives about a billion dollars a year in checks from defense contractors. While some of these are the results of contract changes that result in reduced prices, others represent errors by DOD's payment center. DOD is considering the use of private contractors, through a process known as recovery auditing, to identify overpayments. In addition to erroneous payments, weak systems and internal controls can leave DOD vulnerable to fraud and improper payments. Our September 1998 report discussed two cases of fraud that resulted from a weak internal control environment.[1] In

[1] Financial Management: Improvement Needed in Air Force Vendor Payments Systems and Controls (GAO/AIMD-98-274, Sept. 28, 1998).

one instance, the lack of segregation of duties and other control weaknesses provided Defense Finance and Accounting Service employees a level of access to the vendor payment system that allowed them to enter contract and payment information and remittance addresses needed to create payment vouchers. No one individual should control all key aspects of a transaction or event without appropriate compensating controls.

In recent years, DOD has significantly changed the way it acquires goods and services by removing what were considered barriers to efficient and effective use of the commercial marketplace. A major focus of these changes is the adoption of commercial buying practices. We and the DOD IG have found that DOD needs to strengthen the quality of its price analyses. For example, the IG found that DOD had not formulated good procurement and management strategies for commercial parts in the acquisition reform environment. As a result, DOD was paying higher prices for commercial spare parts than necessary.

DOD's implementation of health care management programs, particularly the TRICARE Program, further illustrates DOD's difficulty in managing contracts. TRICARE was established during a period of military downsizing and budget concerns to contain costs and maintain access to and the quality of health care for DOD's 8.2 million beneficiaries. However, TRICARE's implementation, entailing the award of seven competitively bid, 5-year contracts, has been fraught with problems. All seven contracts, totaling about $15 billion, were protested. As a result, DOD and the competitors incurred added costs, and the program was significantly delayed. Three of the protests were sustained, resulting in further delays.

While DOD is taking steps to improve its payment process and controls, it will likely take an extended period of time to get its payment problems under control. Similarly, DOD is taking steps to simplify its procurement approach for health care contracts. Whether DOD can successfully develop and launch the new method, and whether what it designs

will reduce the current volume of contract changes or control health care costs remains to be seen.

Program Management Challenges

Defense Infrastructure Can Be Better Streamlined

Although DOD has substantially downsized its force structure over the past 7 to 10 years, it has not reduced operations and support costs commensurately because the services are reluctant to consolidate activities that span service lines and reduce capacity as necessary. DOD has found that infrastructure reductions are difficult and painful because achieving significant cost savings requires up-front investments, the closure of installations, and the elimination of military and civilian jobs. Further, DOD's ability to reduce infrastructure has been affected by service parochialism, a cultural resistance to change, and congressional and public concern about the effects and impartiality of decisions. For fiscal year 1998, DOD estimated that about $147 billion, or 58 percent of its budget, would still be needed for infrastructure requirements, which included installation support, training, medical care, logistics, force management, acquisition infrastructure, and personnel.

The Secretary of Defense's November 1997 Defense Reform Initiative Report emphasizes the need to reduce excess Cold War infrastructure to free up resources for force modernization. Initiatives included privatizing military housing and utility systems, emphasizing demolition of excess buildings, and consolidating and regionalizing many defense support agencies. The Secretary noted that DOD continued to be weighed down by facilities that are too extensive for its needs, more expensive to maintain than it can afford, and detrimental to the efficiency and effectiveness of the nation's armed forces. Likewise, he noted that DOD must do a better job of managing facility assets on its remaining bases. The Defense reform initiatives are steps in the right direction but collectively they do not provide a comprehensive long-range plan for facilities infrastructure. We have cited the need for such a plan but have noted that DOD's past

plans were not focused on long-term comprehensive strategies for facilities revitalization, replacement, and maintenance and were not tied to measurable goals to be accomplished over specified time frames or linked to funding. The Results Act underscores the need for improved planning for facilities infrastructure. Improved infrastructure planning can help agency components and programs to develop outcome-oriented goals and performance measures that are linked to and support agencywide goals.

In February 1997, we identified defense infrastructure as a high-risk area, and it remains on our high-risk list. We have identified numerous areas in which infrastructure activities can be eliminated, streamlined or reengineered to be made more efficient in the following areas: acquisition infrastructure, central logistics, installation support, central training, force management, and medical facilities and services.

Inventory Management Problems Persist in DOD

DOD's inventory management practices continue to be ineffective and inefficient. As a result, DOD spends more than necessary to procure inventory, yet items are not available when needed. In 1990, we identified DOD's management of secondary inventories (spare and repair parts, clothing, medical supplies, and other items to support the operating forces) as a high-risk area because levels of inventory were too high and management systems and procedures were ineffective.

DOD has had inventory management problems for decades. Some examples of DOD's problems follow:

- Adequate inventory oversight has yet to be achieved. In 1995, we reported that DOD's strategic plans for logistics called for improving asset visibility in such areas as in-transit assets, retail level stocks, and automated systems. DOD will not completely implement its current plan until 2004.

- DOD has not taken sufficient steps to ensure the accuracy of inventory requirements to preclude the acquisition of unneeded items. For example, the Navy could have eliminated about $13 million of planned program requirements for 68 of 200 items we reviewed because the requirements were also included in the reorder-level requirement.

Recently, the Congress enacted legislation requiring the Defense Logistics Agency and the services to develop and submit schedules for implementing best commercial practices in the acquisition and distribution of inventory items. DOD recognizes potential opportunities in adopting best practices. DOD seeks to reengineer its support activities and business practices by incorporating many business practices that the private sector companies have used to become leaner, more agile, and highly successful. Since 1991, we have issued 11 reports that identify significant opportunities for DOD to test and adopt, where feasible, best inventory management practices used in the private sector to improve logistics operations and lower costs.

Military Personnel Issues Need Attention

DOD's personnel programs to recruit, train, and retain a high-quality active-duty enlisted workforce have not received the management attention needed to ensure their successful operation. The military services recruit tens of thousands of new enlistees each year who fail to complete their contracts.

Our body of work in this area indicates that DOD faces an especially significant challenge in retaining the hundreds of thousands of new recruits it enlists each year. While each new enlistee signs a contract ranging from 2 to 6 years, most first-term contracts are for 4 years. Despite this contractual obligation, we found that between fiscal year 1982 and 1993, 31.7 percent of all enlistees did not complete their first terms of service. First-term attrition is costly: DOD estimates that the services' recruiting and training investment in each enlistee during the first term is an average of $35,532. For fiscal year 1993 we calculated that the services spent $1.3 billion on the 72,670 enlistees

who entered the services in fiscal year 1993 and departed prematurely. Enlistees were separated because of inadequate screening prior to enlistment; ineffective service procedures for selecting the best candidates for recruiting duty; and enlistee misconduct, medical conditions, performance problems, drug use, pregnancy and parenthood.

We have made a number of recommendations to which DOD is now responding. It has formed a joint service working group and agreed to prepare a report by October 1999 documenting service initiatives to reduce attrition. Examining the roles of all persons involved in recruiting and retaining enlistees is in keeping with the intent of the Results Act, which requires agencies to clearly define their missions, to set goals, and to link activities and resources to those goals. Recruiting and retaining well-qualified military personnel are among the goals included in DOD's strategic plan required under the Act.

Addressing the Challenges in DOD

To address the management and performance problems we have cited, DOD has taken actions in the high risk and other areas and has made progress in improving some of them. DOD has had some success in addressing its inventory management problems, is working to reform its weapon systems acquisition process, has recognized the need for infrastructure reductions, and has identified initiatives to reduce attrition of military personnel. For example, in May 1997, the Secretary of Defense issued the Report of the Quadrennial Defense Review, which examines America's defense needs from 1997 to 2015, including issuing a blueprint for a strategy-based, balanced, and affordable defense program. In addition, DOD's latest efforts to reform operations and processes are contained in the Secretary's DRI Report, in which DOD proposed to revolutionize its business and support operations by identifying and adopting best business practices from the private sector.

Despite DOD's military successes, many of its programs and operations are still vulnerable to fraud, waste, and abuse, and mismanagement, and need improvement. To meet these challenges DOD must address their underlying causes, such as cultural

barriers and service parochialisms. DOD must have an effective overall strategic plan that includes goals, performance measures, and time frames for completing corrective actions. In our view, the Results Act provides the framework for resolving high risk and other problems and for providing greater accountability in DOD's programs and operations.

DOD, however, has not fully embraced the underlying principles in the Results Act. The Secretary of Defense has stated that the May 1997 Quadrennial Defense Review will serve as DOD's overall strategic planning document and is intended to fulfill the requirements of the Results Act. Our review of DOD's strategic plan and its February 1998 performance plan disclosed many areas where improvements could be made. The principal shortcomings in DOD's plan center on weaknesses in (1) establishing results-oriented performance goals with explicit strategies and time frames for achieving them and (2) addressing what DOD has done or plans to do to resolve its persistent management problems. In our opinion, DOD needs to work closely with the Congress now to develop performance goals and measures. Addressing these areas would provide congressional decisionmakers and DOD the information necessary to ensure that DOD's plans are well thought out for resolving ongoing problems, achieving its goals and objectives, and becoming more results oriented, as expected by the Results Act.

CHALLENGES FACING THE DEPARTMENT OF STATE

As the lead agency for the conduct of foreign affairs, State has enormous responsibilities as it works to shape a more secure, prosperous, and democratic world for the benefit of the American people. A substantial amount of State's nearly $2.7 billion annual budget for the administration of foreign affairs is spent on what could be called "business" functions that support its broad mission. The Department has a worldwide network of operations to maintain its headquarters and more than 250 overseas posts, as well as about 35 other U.S. agencies that operate overseas. State provides security for thousands of U.S. personnel and facilities abroad. In addition, State operates a network of communications facilities around the globe that are critical to its foreign affairs mission.

In carrying out its important mission, State faces a number of significant management challenges that, if not met, could affect its ability to function effectively in the 21st century. These challenges are not simple: they cover a wide spectrum of State operations and responsibilities around the world. Key among these challenges are issues State faces in enhancing overseas security, improving its information and financial management systems, integrating other foreign affairs agencies' functions into the Department, enhancing the controls over the issuance of visas, and improving its strategic and performance planning.

Enhancing the Management of Security Programs
for Overseas Personnel and Property

The need to adequately protect employees and their families overseas may very well be the single most important management issue currently facing the State Department. The acts of terrorism in Kenya and Tanzania claimed more than 260 lives and injured thousands in August 1998. Worldwide, several embassies found themselves either shut down or unable to provide normal services because of threatening situations. The monetary requirements for undertaking security enhancements will be significant, as will the management and technological challenges. State received $1.45 billion in emergency funding to rebuild the embassies in Kenya and Tanzania, relocate other embassies, and improve security for other facilities serving U.S. personnel worldwide. State reports that it has completed security surveys of over 200 posts and formulated six internal working groups to direct and track program implementation. One initiative will require the accounting system to accumulate spending data on areas such as equipment acquisition and construction.

State is also assessing its longer-term security enhancement needs, and estimates that several billion dollars may be needed for additional embassy construction. A key issue facing State is whether it will have the capacity to implement a major security construction program. In the early 1990s, we reported that State encountered several

management problems in using the $1.47 billion in funds that were applied to the diplomatic security construction program during fiscal years 1986-1995. These management problems were related to inadequate staffing, poor program planning, difficulties in site acquisition, changes in security requirements, and inadequate contractor performance. All of these directly contributed to significant delays and cost increases in the majority of State's construction projects. For example, inadequate coordination within State in determining building requirements contributed to millions of dollars in cost increases in a project in Pretoria, South Africa. A lack of agreement within State on potential building sites delayed projects in Bogota, Colombia, and Tunis, Tunisia for several years and substantially increased costs. State has since undertaken a number of efforts to improve construction programs. Nevertheless, the scope of the problems encountered indicated that State had systemic weaknesses in its program management.

In view of State's prior experiences and difficulties in implementing the security construction program, several questions and issues need to be addressed as part of today's efforts to formulate strategies for enhancing security.

- What would be the total costs to bring overseas posts into compliance with current security standards?

- What actions would State need to take to ensure it has the management capability to implement a large-scale construction program?

- Are there adequate control mechanisms to ensure efficient and effective use of emergency funds and any subsequent funding for overseas security?

One issue that should be considered in addressing future security requirements is the sheer number of U.S. employees overseas. The security burden is directly associated with the size of the overseas work force. In our work on overseas staffing issues in the mid-1990s, we noted that the U.S. government (excluding military operational commands)

employed a total of nearly 38,000 personnel overseas--split evenly between U.S. direct hire employees and foreign national employees. An important trend has been the increase in the number of overseas U.S. direct hires by the non-foreign-affairs agencies. A broad examination of how the U.S. government carries out its overseas role and related missions may now be needed in view of the increased security threats. State needs to take the lead in working with other agencies operating overseas to examine their overseas staffing requirements and explore alternatives to reducing the number of U.S. employees overseas.

Improving Information and Financial Management Systems

State's information resource management infrastructure has historically been inadequate to support the Department's core foreign policy and administrative functions. We have reported that State relied on outdated and unsecured information and financial management systems that are vulnerable to Year 2000 problems and security breaches. State estimated in 1997 that it would need $2.7 billion over 5 years to achieve a modernized global infrastructure. However, this estimate was not prepared through the rigorous analytical process called for in federal guidance designed to control costs and improve efficiency. State has since taken steps to improve its information security and adopted an improved approach to addressing its Year 2000 problems. It has also begun to incorporate a comprehensive capital planning and investment process into its information technology investments. However, State needs to ensure that it remediates on a timely basis its mission-critical systems. The Office of Management and Budget has designated State as a Tier 1 agency in its assessment of agencies' Year 2000 progress, that is, State demonstrated insufficient evidence of progress in dealing with this problem.

In the financial management area, State received, for the first time, an unqualified opinion on its fiscal year 1997 financial statements. This achievement provides State with a foundation from which it can move toward being able to more routinely produce the timely and reliable financial information that is critical to making sound decisions that promote effective and efficient use of federal funds. To reach this goal, State needs to

continue to bring its systems into full compliance with federal accounting and information management requirements. State also must work on solving related material internal control weaknesses if it is to adequately protect its assets and have timely, reliable data for cost-based decision-making, reporting, and performance management.

Effectively Reorganizing Foreign Affairs Agencies

The long-planned reorganization of the government's foreign affairs agencies is under way. In April 1997, the White House announced a plan to put matters of international arms control, U.S. Information Agency's (USIA) public diplomacy, and other functions within a "reinvented" State Department. In October 1998, the Congress authorized the reorganization, which abolished the USIA and the Arms Control and Disarmament Agency (ACDA) and consolidated and integrated those functions into State. The reorganization is intended to reinvigorate the foreign affairs functions of the United States within the State Department. About 3,000 employees of ACDA and USIA will be integrated into State. Potential areas identified for integration among the three agencies include legal affairs, congressional liaison, press and public affairs, and management. Central management functions that are to be integrated include IRM, overseas facilities and operations, logistics, diplomatic security, financial management, and human resources. In December 1998, State submitted a report to the Congress describing its reorganization strategy.

State has indicated that during the transition, costs would likely increase because of the need to implement system conversions and transfers; in the longer term, overall staffing and costs may decrease. State faces several challenges in achieving the objectives of this reorganization. One major challenge is the technological difficulty of uniting the agencies, including integrating separate electronic mail and computer systems. Overall issues include whether the reorganization will actually produce identifiable efficiencies and improved performance in foreign affairs programming. As our prior work has indicated, many of the areas targeted for management consolidation need substantial reform.

Effectively Managing the Visa Process

The Immigration and Naturalization Service (INS) estimated that as of October 1996, 5 million illegal aliens were residing in the United States. While not the primary source of illegal immigration, visa fraud is a significant matter of concern. State's consular officers at overseas posts are responsible for providing expeditious visa processing for qualified applicants. At the same time, they must prevent the entry of those who are a danger to U.S. security interests or are likely to remain in the United States illegally. In fiscal year 1997, over 7 million aliens applied for nonimmigrant visas, and 640,000 foreigners immigrated to the United States. Visa processing is a particular problem for some overseas locations where volume and/or security concerns are high.

State has introduced new technologies, equipment, and controls designed to improve visa processing and reduce the incidence of fraud. State notes that progress has been made in several areas, including installation of machine-readable visa systems at all visa-issuing posts, online connectivity to Washington, D.C., data bases, and implementation of a first phase of a State-INS data-share program. Many improvements were made possible through State's temporary authority to retain fees charged foreigners applying for nonimmigrant visas. Those fees generated millions of dollars, enabling the Department of State to invest in border security technology and to pay the salaries of nearly 2,000 employees.

State will need to remain vigilant in a number of areas to further reduce the vulnerability of the visa system to fraud and abuse. These issues include (1) critical staffing gaps in overseas consular positions; (2) limitations in consular automated systems; (3) restrictions in the exchange of intelligence information with INS and other law enforcement agencies; and (4) weaknesses in the integrity of immigrant and nonimmigrant documentation, including the computerized systems used to produce them. The Department must also continue its efforts to encourage consular sections to implement best practices designed to streamline and rationalize the visa workload.

Potential best practices include using travel agents for initial processing, establishing appointment systems to control workload, and allowing the payment of visa fees at a bank or other financial institution. In view of the increased international terrorist threats, continued attention to State's progress in addressing these issues will be needed.

Strengthening Strategic and Performance Planning at State

State needs to strengthen its strategic and performance planning as part of its overall efforts to improve management. In its first strategic plan for foreign affairs, State formulated 16 foreign policy goals that cover a wide spectrum of U.S. national interests--national security, economic prosperity, American citizens and U.S. borders, law enforcement, democracy, humanitarian response, and global issues. Our review of that plan and the Department's annual performance plan for 1999 indicated that State's plans had their strong points but often fell short of meeting the requirements of the Results Act.

One area of concern was that State's strategic plan addressed neither the potential impact of the consolidation of the foreign affairs agencies on its systems nor the potential for other agencies to have functions duplicative of State's. We have found that State's functional bureaus share responsibility with multiple U.S. agencies on various overlapping issues, including trade and export policy and international security functions. The strategic plan also did not address the serious deficiencies in State's financial accounting and information systems, noting only in general terms that several years will be required to develop performance measures and related data bases to provide sufficient information on the achievement of goals.

Our review of State's performance plan revealed similar deficiencies but also some encouraging points as well. For example, State's performance plan generally provided clear and reasonable strategies and goals in the areas of improving U.S. citizens' services and border security, and promoting democracy. In contrast, State's plan did not present a clear picture of its methods to meet strategic and performance goals in the areas of furthering economic prosperity, preventing international crime, and enhancing

humanitarian assistance. Overall, the performance plan did not clearly indicate the Department's intended performance and was vague about how State will coordinate with other agencies. Further, State's performance plan did not provide sufficient confidence that the Department's performance information will be credible. It did not address how the known deficiencies in State's financial and accounting and information systems will affect performance measurement. In response to our work, State is attempting to improve its planning by developing clearer and more objective performance measures linked to performance goals and identifying partnerships with other agencies or governments to address crosscutting issues.

State's initiatives have also received top-level management support in recent months as evidenced by the appointment of a permanent Chief Information Officer (CIO), and a deputy CIO for architecture and planning, the creation of a Deputy CIO position for the Year 2000 issue, and the assignment of information system security issues to the Deputy CIO for Operations.

CHALLENGES FACING THE DEPARTMENT OF VETERANS AFFAIRS

The Department of Veterans Affairs (VA) is responsible for administering benefits and services that affect the lives of more than 25 million veterans and approximately 44 million members of their families. Through its budget--approximately $43 billion in fiscal year 1999--VA provides an array of health care benefits; non-health-care benefits, such as compensation and pension; and other supporting programs. Over 200,000 VA employees deliver these services from more than 1,000 facilities.

As required by the Results Act, VA submitted a strategic plan for fiscal years 1998 to 2003. In this plan, VA developed strategic goals covering all its major programs and included objectives, strategies, and performance goals to support its strategic goals. VA has made significant progress in developing a framework for managing and evaluating changes in service delivery. However, there are several management challenges VA

must overcome to meet its strategic goals of efficiently and effectively delivering services to veterans and their families. These challenges include:

- an infrastructure that does not meet current and future needs,
- inability to ensure that veterans have access to needed health care services,
- lack of outcome measures to assess the effects of managed care initiatives,
- ineffective management of non-health-care benefits programs, and
- ineffective management of information systems.

VA Health Care Infrastructure Does Not Meet Current and Future Needs

Because of their age and recent changes in the way VA delivers health care, many of VA's facilities are no longer adequate for the way VA delivers health care services today and plans to deliver services in the future. For example, most VA facilities were constructed as hospitals with an array of bed sections, treatment rooms, surgical suites, and other accommodations and equipment for treating an inpatient population and are often poorly suited for delivering care to an ambulatory population on an outpatient basis. Although changing care practices and efficiency initiatives, such as emphasizing outpatient care and facility integration, have allowed VA to eliminate approximately half of its 52,000 acute-care hospital beds since 1994, excess capacity remains. Furthermore, the veteran population is declining: VA projects that the number of veterans in the country will drop about 21 percent from 1997 to 2010. We have reported that if past efficiency trends and demographic projections are realized, VA will need only about 10,000 of its current 26,000 acute-care beds to meet veterans' health care needs in 2010. VA will likely need to close some facilities, but it also must plan for the needs of the increasingly older veteran population. As the nation's World War II and Korean War veteran populations age, their health care needs are shifting from acute hospital care to nursing home and other long-term care services. For example, the number of veterans aged 85 and older is projected to increase to about 1.3 million in 2010, a fourfold increase from 1995.

The continued need for some VA facilities may be affected by the expanded authority to contract for health care services that the Congress provided VA in 1996. Under this authority, VA can contract with public or private providers, who can provide care at lower cost or care that VA does not offer in a particular geographic location. To the extent that VA uses this authority, it may create additional excess capacity in existing facilities.

Integrating various clinical and support operations across some of its facilities is an important tool VA is using to meet current and future needs. Integrations are also intended to enhance the efficiency and effectiveness of VA's health care delivery system by reducing unnecessary duplication of services. We have reported that the 23 facility integrations involving 48 health care facilities that have been completed or are under way will produce millions of dollars in savings that can be used to enhance veterans' health care. However, VA could do more. We have reported that consolidating services from four to three locations in the Chicago area could save $6 million to $27 million in future renovation costs. Although VA has recently developed a guidebook for planners to use in developing, implementing, and evaluating potential facility integrations, VA needs to apply this framework and evaluate its effectiveness in saving resources for both the short and the long term.

VA's restructuring efforts, particularly integrating administrative and clinical services across two or more medical centers, are complicated by affiliation agreements that VA facilities have with medical schools. Since VA's medical education program began in 1946, 130 VA medical centers have affiliated with 105 medical schools to provide training opportunities for medical students and residents. Transforming VA's health care delivery system from an inpatient to an outpatient focus, increasing reliance on primary care, and integrating services in fewer hospitals are all causing VA and medical schools to rethink their affiliation arrangements.

Restructuring efforts will also affect VA's support of the nation's medical needs during national emergencies. Since 1982, VA has served as the primary medical system backup to DOD. VA also works with the Federal Emergency Management Agency and the National Disaster Medical System during national emergencies. The integration of facilities' administrative functions, the consolidation of medical services in fewer VA locations, and VA's reduced reliance on providing specialized care may alter the way VA is able to support DOD and the federal emergency and disaster systems. However, VA has not specified how it will maintain its emergency backup functions in light of restructuring.

VA Is Unable To Ensure That Veterans
Have Access To Needed Health Care Services

Because VA lacks accurate, reliable, and consistent information on how resources are being allocated, it cannot ensure that veterans who have similar economic status and eligibility priority have similar access to care regardless of the region of the country in which they live, as required by Congress. In fiscal year 1997, VA introduced a new resource allocation system to begin to correct historical inequities in allocating resources, with the intent of improving the equity of veterans' access to care. Instead of allocating resources directly to medical centers on the basis of their budget for the previous year, VA now allocates funds to its 22 Veterans Integrated Service Networks (VISNs) based on the number of veterans each VISN has served. VISNs, in turn, allocate resources to the facilities in their geographic area. We have reported that while the new method has indeed improved the equity of resource distribution among VISNs, VA does not know if it is making progress in providing similar services to similarly situated veterans. VA's strategic plan does not include a goal for achieving equitable access, nor does VA monitor the extent to which equitable access is being achieved among or within VISNs.

Furthermore, VA has not been able to provide the necessary data to assure that it maintains its level of certain high-cost, specialized services, as required by the Congress. We have reported that much more information and analyses are needed to support VA's

conclusion that it is maintaining its national capacity to treat special disability groups, including the four the Congress identified -- spinal cord dysfunction, blindness, amputation, and mental illness -- in the face of the many initiatives to become a more efficient provider of care.

VA has not developed information to help ensure that it meets the likely increased demand for care generated by its new process for enrolling veterans in its health care system. As a result, VA's success in enrolling veterans may jeopardize the availability of care for some veterans. As part of its 1996 eligibility reform legislation, the Congress required VA to develop a priority-based enrollment system to allow VA to better manage access while operating within its budgetary limits. VA has determined that in fiscal year 1999 it will enroll all priorities and categories of veterans and serve each veteran who enrolls. Because enrolled veterans are eligible for all needed hospital and medical care from VA regardless of their priority category, access to care for higher-priority veterans may be jeopardized as medical centers provide care to all enrollees, including high income veterans without service-connected conditions.

VA Lacks Outcome Measures To Assess the Effects of Managed Care Initiatives

Responsibility for monitoring quality assurance shifted several times in the last few years among headquarters and VISN offices, and VA's Inspector General and veterans' service organizations raised concerns that VA had weakened its quality assurance efforts with some of these shifts. In response, in fiscal year 1998, VA realigned the Office of Performance and Quality to report directly to the Under Secretary for Health. The realignment has the potential to improve VA's quality assurance efforts because this office is situated to more readily identify emerging challenges across the health care system, implement and oversee local and national corrective actions when needed, and help create the single standard of care required by accrediting agencies.

VA has made little progress in developing, implementing, and evaluating results-oriented outcome measures to assess the health status of veterans. Instead, VA's efforts to determine how well it delivers health care have relied primarily on process-oriented performance measures. For example, in its performance plan, VA identifies performance measures such as the number of beds in use, the number of patients served, and the number of patients receiving certain diagnostic tests. Although these measures can provide useful information on progress toward meeting managed care goals, they provide little information on the specific impact of changes on the health status of veterans.

Moreover, VA has generally not performed the program evaluations necessary to determine whether its performance measures are the most appropriate or sensitive measures for assessing responses to treatment and changes in health outcomes. The need for such measures is critical, given the multitude of changes in delivering care that VA has introduced over the last few years. Indeed, the need is exacerbated by the flexibility VISNs and medical centers have in choosing how they deliver care in VA's decentralized management structure. VA recognizes that it needs to ensure that the changes made to improve its efficiency and effectiveness do not unintentionally compromise the health status of veterans. VA is not alone in its need to design, implement, and evaluate health outcome measures. Other public and private providers have recognized the necessity--and the difficulty--of creating such criteria and instruments.

VA's challenges in assessing outcomes are further complicated by poor data. We and others have reported numerous concerns with VA's outcome data. These concerns, which are similar to those with VA's access data, include inconsistent, incompatible, and inaccurate databases; changes in data definitions over time; and lack of timely and useful reporting of information to medical center, VISN, and national program managers.

VA Faces Major Challenges In Managing
Non-Health-Care Benefits Programs

The non-health-care benefits which VA provides include disability payments, compensation, pension, housing credit assistance, and vocational rehabilitation assistance programs. We have reported that VA's current disability rating schedule does not reflect the economic loss experienced by veterans today and may not be equitably distributing disability compensation funds. In the late 1960s, VA conducted a study of the 1945 version of its disability rating schedule which concluded that at least some disability ratings in the schedule did not accurately reflect the average impairment in earning capacity among disabled veterans and needed to be adjusted. While VA has done little to ensure that the schedule's assessments of the economic loss associated with service-connected conditions are accurate, successful implementation of the revised rating scale would likely require congressional action.

In addition, a 1996 Congressional Budget Office report, found that VA was paying about 230,000 veterans about $1.1 billion in disability compensation payments annually for diseases or injuries neither caused nor aggravated by military service. VA regulations provide that a disease or injury resulting in disability is considered service-connected if it was incurred during a veteran's military tour of duty or, if incurred before the veteran entered service, was aggravated by service. No causal connection is required between the circumstances of the disability and official military duty. As a result, veterans can receive compensation for diseases related to heredity or life-style, such as heart disease and diabetes, rather than military service, thus calling into question the fairness of VA's treatment of veterans who were disabled because of their service.

In another area of concern, the National Academy of Public Administration reported, in 1997, that the timeliness and quality of adjudication decisions and slow appellate decisions continued to be a major challenge in VA's compensation and pension program. VA reported in fiscal year 1997 that it took an average of 133 days to complete the processing of a veteran's original disability compensation claim. While this is

substantially faster than the average of 213 days required in fiscal year 1994, VA's goal is to reduce the average to 53 days in fiscal year 2002. In September 1998, VA's OIG reported on its audit of three key compensation and pension claims processing performance measures. The OIG found that the performance measures lacked integrity because the compensation and pension program's automated information system was vulnerable both to reporting errors and to manipulation of data by regional offices to show better performance than was actually achieved.

Other areas of concern are VA's Housing Credit Assistance and Vocational Rehabilitation programs. VA's Annual Accountability Report, Fiscal Year 1997, described several deficiencies that contributed to VA's receiving a qualified opinion. Among the areas of concern was the level of control and accountability over the direct loan and loan sale activities. The auditors were unable to conclude that the $3 billion loans receivable account balance was accurate because of inadequate controls and incomplete records. In addition, the auditors identified a number of errors, including inaccurate recording of loan sales transactions and improper accounting for loan guarantees.

VA's vocational rehabilitation program continues to place few disabled veterans in jobs. Our 1996 review of records of about 74,000 applicants for vocational rehabilitation between October 1991 and September 1995, who were classified by VA as eligible for assistance, showed that only 8 percent had completed the vocational rehabilitation process by finding a suitable job and holding it for at least 60 days. VA is implementing a number of initiatives to address its compensation and pension claims processing and vocational rehabilitation performance weaknesses, including establishing performance measures for processing times and unit costs, initiating quality assurance efforts, and reassessing its business process reengineering.

VA Needs To Manage Its Information Systems More Effectively

VA has made progress in addressing its Year 2000 challenges but still has a number of associated issues to address. For example, VA faces significant information systems

challenges. It does not know the full extent of its Year 2000 challenges and could face widespread computer system failures at the turn of the century if its systems cannot adequately distinguish the year 2000 from the year 1900. Thus, veterans who are due to receive benefits and medical care could appear ineligible.

In addition, VA has not established effective controls to prevent individuals, both internal and external, from gaining unauthorized access to VA systems. VA's access control weaknesses are compounded by ineffective procedures for monitoring and overseeing systems designed to call attention to unusual or suspicious access activities. VA also does not have a comprehensive computer security planning and management program. If these control weaknesses are not corrected, VA operations, such as financial management, health care delivery, benefit payments, life insurance services, and home mortgage loan guarantees--and the assets associated with these operations--are at risk of misuse and disruption.

Furthermore, VA has not yet institutionalized a disciplined process for selecting, controlling, and evaluating information technology investments, as required by the Clinger-Cohen Act. Information technology accounted for approximately $1 billion of VA's fiscal year 1999 budget request of $43 billion. At the time of the budget request, VA decisionmakers did not have current and complete information, such as cost, benefit, schedule, risk, and performance data at the project level, which is essential to making sound investment decisions. In addition, VA's process for controlling and evaluating its investment portfolio has deficiencies in in-process and post-implementation reviews. Consequently, VA does not know whether it is making the right investments, how to control these investments effectively, or whether these investments have provided mission-related benefits in excess of their costs. VA has concurred with most of the recommendations we have made to address information systems management issues, and has taken actions to implement many of them.

SUMMARY

To address the management and performance problems we have cited, DOD, State, and VA have taken actions in the high risk and other areas and have made progress improving some of them. For example, DOD has had some success in addressing inventory management problems, is working to reform its weapon systems acquisition process, and has recognized the need for infrastructure reductions. Although past and current efforts have resulted in progress in improving their operations, long-standing problems still exist. To address these problems, these agencies must have an effective overall strategic plan and performance plans that, among other things, include goals, performance measures, and time frames for completing the corrective actions. The Results Act provides the framework for resolving high risk and other programs and for providing greater accountability in agencies' programs and operations. In our opinion, agencies such as DOD, State, and VA need to work closely with the Congress now to develop performance goals and measures. Addressing these areas would provide congressional decisionmakers and individual agencies the information necessary to ensure that plans are well thought out for resolving ongoing problems, achieving its goals and objectives, and becoming more results oriented, as expected by the Results Act.

Mr. Chairman, this concludes our statement. We would be happy to answer any questions you or the members of the Subcommittee may have.

DEPARTMENT OF DEFENSE HIGH-RISK DESIGNATIONS

High-Risk Area	Year Designated as High Risk
Inventory Management	1990
Weapon Systems Acquisition	1990
Contract Management	1992
Systems Development and Modernization Efforts	1995
Financial Management	1995
Infrastructure Management	1997

Mr. SHAYS. Thank you, Mr. Hinton.

It is really appropriate, I think, to have the GAO go first, since you were covering all three, as a nice introduction. At this time, Eleanor Hill.

Excuse me, Ms. Hill, I really should acknowledge that we have a Member here from Massachusetts, John Tierney, and it is wonderful to have him on the committee. It is nice to have him here. I am going to take advantage of just doing some bookkeeping, if I could, given that we have a Member on both sides of the aisle. I would ask unanimous consent that all members of the subcommittee be permitted to place any opening statement in the record and that the record remain open for 3 days for that purpose.

Without objection, so ordered.

And I also ask further unanimous consent that all witnesses be permitted to include their written statement in the record. Before giving you the floor, I would just ask the gentleman if he has any comments.

Mr. TIERNEY. Actually, I do not. I am here prepared to listen and learn.

Mr. SHAYS. OK, thank you.

Ms. HILL. Thank you. I am going to briefly summarize my statement. As you pointed out, Mr. Chairman, we will have the full statement in the record.

Mr. SHAYS. It is amazing, this is the first time we do not have a clock, and all of you are going to be punctual. [Laughter.]

Ms. HILL. We are trying.

I am pleased to have this opportunity to discuss the Department of Defense's vulnerabilities to waste, fraud and abuse, as well as opportunities for continuing the momentum developed over the past few years toward management reform and improvement.

There are 10 areas where we in the IG's office believe further management improvement is particularly important, based on recent audit and investigative results. 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 those top 10 high risk areas. In each of those areas, there are numerous problems that are inter-related, complex, and involve a wide range of organizations. Many specific problems are relatively long-standing. Others have emerged only recently.

Briefly, the 10 problem areas are as follows. No. 1, and this is something Mr. Hinton has already alluded to, 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 DOD statements for fiscal year 1998. The inability of DOD's systems to produce reliable annual financial statements means that DOD managers and commanders lack much of the timely, accurate and useful financial information that they need for program decisionmaking on a day-to-day basis.

The second area we have concerns about is weapons system acquisition. Increasing the weapons procurement share of the budget is a high priority DOD budget goal. There are compelling technological and financial reasons to accelerate the acquisition cycle and to cut per unit costs, especially overhead costs. It is by no means certain, however, 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.

The third area involves 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 ships and missiles. DOD administers over $800 billion in open contracts and plans to award $135 billion of new contracts in the current fiscal year. The sheer volume and great variety of DOD contracting activity makes this a high risk area.

While the Department has made progress in initiating acquisition reform initiatives, 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.

The fourth area is health care. The Defense health program serves 8.2 million eligible beneficiaries through a combination of DOD in-house and outsourced care. Total DOD health care costs are nearly $16 billion annually. The Defense health programs cost containment challenges are exacerbated by the continued lack of good cost information and significant levels of fraud, particularly by some private sector providers. We currently have about 500 open criminal investigations on health care fraud.

I should point out that traditionally, the biggest priority area in our office in criminal investigations, was procurement fraud which started back in the early to mid-1980's, the emphasis on that. In recent years, while the largest category of our cases are in procurement fraud, the No. 2 priority, involving a significant amount of our work is in the health care area. So this, in recent years has become a bigger and bigger problem for the Department. More of our resources are now devoted to health care fraud.

The fifth area is supply inventory management. The Department had reduced wholesale supply stocks by nearly a third and is pursuing a number of logistics reform initiatives.

However, spare parts shortages are being reported more frequently by operational units. Audits continue to show that war reserves are overstocked in some locations, but short of critical items in others. Fraud and inappropriate disposal practices remain particular problems in the disposal area, where we have almost 70 open criminal investigations.

The sixth problem area is the year 2000 conversion. The Department of Defense depends heavily, as Mr. Hinton has mentioned, on automated information processing by about 28,000 systems, 2,274 of which are considered mission critical. DOD faces a $2.5 billion cost and a monumental management challenge because of the scale of the year 2000 conversion problem, a belated start in seriously

addressing it and the legacy of past inattention to good information technology and management practices.

As of January 1999, approximately 77 percent of mission critical systems have been certified as Y2K compliant. We believe that the number and severity of the remaining Y2K issues will not be readily apparent until at least June 1999, when more testing results become available.

The seventh area we have designated as other information technology issues, aside from the Y2K problem. As indicated in 21 recent audit reports, the Department faces major problems related to the acquisition of computer systems, and the security of both old and new systems. Automated system development projects have tended to overrun budgets, slip schedules, evade data standardization and inter-operability requirements and shortchange use needs.

Audits continue to show lax security measures and inadequate focus by program managers on the threat to information systems, 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.

The eighth area is other infrastructure issues. 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. Difficulty in collecting reliable cost information with which to make outsourcing or restructuring decisions is a major infrastructure management problem. There are continued problems in determining facility requirements, especially for housing, where estimates of the cost of modernizing DOD facilities run as high as $30 billion.

No. 9, readiness. We have 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. Units have indicated weaknesses related to chemical and biological defense preparedness and communications capability.

Last, we have designated as area No. 10, turbulence from change. For most of the past decade, all functional areas within the Department of Defense have been engaged in fundamental reform and process re-engineering efforts at the same time. Conflicting priorities, downsizing, outsourcing, dependence on new and unproven systems or processes, de-emphasis on management controls and oversight, reorganization, sustained requirements growth, despite resource constraints, and the continued unexpectedly intensive need for frequent U.S. 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.

In sum, as the largest and most complex government agency in the world, the Department of Defense 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. Department managers have agreed with about 96 per-

cent of our audit recommendations, and have completed action on over 5,200 audit recommendations over the past 5 years, realizing estimated monetary benefits of $18.6 billion. We will continue to do our best to highlight the Department's high risk areas, both in our audit and investigative work, and in the semi-annual reports from my office to the Congress.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Hill follows:]

Hold for Release
Until Delivery
Expected 10:00 a.m.
February 25, 1999

Statement of

Eleanor Hill

Inspector General

Department of Defense

Before the

Subcommittee on National Security, Veterans Affairs,

and International Relations

Committee on Government Reform

U.S. House of Representatives

on

Department of Defense Vulnerabilities to Waste,

Fraud and Abuse

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-

Mr. SHAYS. Thank you. Ms. Hill.

Richard Griffin, who is the Inspector General, U.S. Department of Veterans Affairs.

We've been joined by the ranking member of this committee, really a partner in this whole process, Mr. Blagojevich. I welcome you here. I do not know if you'd just like to make a statement for the record.

Mr. BLAGOJEVICH. Thank you very much, Mr. Chairman. I will be very brief. Let me first of all say good morning to our distinguished witnesses on the panel, and just say, this is the subcommittee's first hearing of the new Congress. It is also my first hearing as a ranking member. If I could say a couple of things, No. 1, I want to extend my special appreciation to our very able chairman, Mr. Shays, and say how much I am looking forward to working with you over the next 2 years.

And second—what do I do next? This is my first hearing as ranking member.

I have a statement for the record. In the interest of time and brevity, I will just allow the rest of it to be entered into the record, then allow the witnesses to testify. Thank you.

[The prepared statement of Hon. Rod R. Blagojevich follows:]

Opening Statement of Rep. Rod Blagojevich

Hearing on Vulnerabilities to Waste, Fraud and Abuse: Inspectors General and GAO Views on the Departments of Defense, State, and Veterans Affairs

February 25, 1999

Thank you, Chairman Shays, and good morning to our distinguished witnesses on both panels.

As the subcommittee's first hearing of the new Congress, and my first hearing as a Ranking Member, I want to extend my special appreciation to our very able chairman, Chris Shays, and say how much I am looking forward to working with you over the next two years.

Your record of substantive achievement in Congress and your commitment to working closely with members on both sides of the aisle are well known. I know all of us on the minority side are anxious to work with you to make our government more efficient and more responsive to the needs of the American people.

In the last decade, we've seen dramatic changes in our government's approach to foreign affairs. The end of the cold war, increased threats of terrorism, and a more intensive focus on peace efforts worldwide have all significantly altered the landscape of international relations. This, in turn, has led the United States to reevaluate its strategic goals -- and forced us to reevaluate the means by which we will achieve them.

In this changing climate, existing systems may lose their effectiveness. Our purpose, as I see it, is to continuously evaluate their effectiveness and to consider adjustments when appropriate -- and to root out waste and mismanagement.

Let me just diverge for a second and point out that I am also a member of the Armed Services Committee. There is a growing recognition in that committee and throughout Congress that our country faces a problem of declining readiness and personnel retention within the military.

As we address this problem and search for the additional funding that is needed, the work of this subcommittee in tackling waste, fraud, and abuse within the Department of Defense and other Federal agencies becomes even more critical.

This morning, we plan to examine the major performance and management challenges facing the Departments of Defense, Veterans Affairs, and State. I want to first welcome the representatives of the General Accounting Office. Your diligence is evident in both the reports from the "Performance and Accountability Series" and the "High Risk Series," as well as many other reports on particular issues.

I would also like to welcome the inspectors general from each of these departments. I would like to commend you at the outset for your dedication to streamlining our government and helping us along the way to more efficient and effective systems. I look forward hearing your views -- from the inside -- about the major management challenges facing each of your agencies.

I understand there are areas of agreement between GAO and the IG's about major concerns in each of the agencies. For example, the security of our embassies in light of last year's bombings is an area we all agree deserves the highest scrutiny. Financial management issues at DOD continue to present serious cause for concern. And Veterans Affairs' conversion to managed care principles presents both drawbacks and opportunities for our Nation's veterans.

I recognize that, in many cases, there are extremely dedicated and knowledgeable people working tirelessly to develop and implement programs to address these concerns. I don't want to detract from these efforts. In fact, I hope we will learn more about them next week when we have our second hearing on this issue and hear representatives from your agencies respond to your testimony here today. But I appreciate your honest appraisal of how the agencies are doing now -- sort of a "snapshot" at this point in time.

Finally, I would like to say a word about our goals here today. The substance of this hearing is about management "challenges." Cynics might say the word "challenges" is just Washington's way of saying "problems" or "failures." But our purpose in this subcommittee cannot be this cynical. We must not limit ourselves only to identifying shortfalls and reciting in retrospect what agencies have done wrong.

Fortunately, I don't think any of us intends to do that. Instead, it is my hope that we can work with the agencies to determine the most effective solutions to the problems before us. We must search out practices that are successful so we can duplicate them elsewhere, and we must reward creativity, flexibility, and ingenuity.

So, again, I look forward to hearing from our witnesses and to working with you, Mr. Chairman, in partnership toward our common goals.

Thank you very much.

Mr. SHAYS. Thank you very much. I didn't read the third page of my statement, and I would just like to read this paragraph, now that you are here, and just say, as we proceed to narrow our focus further in the weeks and months ahead, I want our oversight to be constructive and I want it to be bipartisan. I view our work as a zero-sum proposition, with the benefits of increased efficiency and reduced waste accusing to existing underfunded priorities like force readiness at DOD, health care quality at the VA, and embassy security enhancements, for example.

It really is a joy to have you as the ranking member, and I know that we will work well together. I know we will be working with our colleagues at GAO and the Inspectors General. I know that they know what the ranking member wants from you all, as if we were asking it for the committee. DOD is responsible to both sides of the aisle, as you always have been.

Thank you. I am sorry for that slight interruption.

Mr. GRIFFIN. Mr. Chairman and members of the subcommittee, I am pleased to be here today to discuss major performance and management challenges facing the Department of Veterans Affairs and the Department's progress in meeting performance and accountability measurements and goals under the Government Performance and Results Act. I will also highlight contributions of the Office of Inspector General in combating waste, fraud and abuse in VA programs and administrative activities.

Last November, I responded at length to Chairman Burton's request for the Office of Inspector General's views on the 10 most serious management problems facing the Department. These issues appear in an abbreviated form in my full statement which is being submitted for the record for this hearing. While most of these challenges are long term in nature, I am pleased to report that the Department has made great strides in addressing the Y2K issue and expects to complete the implementation of all applications into production next month.

I will briefly highlight recent activities of my office that focus on some of the other top 10 issues. Monitoring the quality of health care is a top priority for my organization. This year, I directed that my Office of Audit, Office of Health Care Inspections and Office of Investigations initiate a Combined Assessment Program to conduct recurring reviews of VA medical centers. These collaborative assessments of medical center operations will focus on key indicators or "pulse points" if you will, to provide medical centers and veterans integrated service network management with timely feedback on the status of local operations and program effectiveness.

In the area of workers' compensation, a collaborative pilot project, involving OIG investigators and VHA, was initiated to identify VA employees who were fraudulently receiving workers' compensation benefits. Indictments were obtained against 14 individuals, all were convicted. Fines and restitution exceeded $550,000, and savings to VA resulting from this pilot project amounted to $4.4 million.

In 1998, we audited the workers' compensation program at the request of the Department and concluded the program was not effectively managed, and that by returning current claimants to work who were no longer disabled, VA could reduce future payments by

$247 million. To help ensure the integrity of VA's workers' compensation program, we are developing a protocol package for VA managers for enhanced case management and fraud detection.

In the area of improper payments, we recently conducted an audit to determine if the disability benefit payments to incarcerated veterans were appropriately adjusted as required by Public Law 96–385. We reviewed a sample of veterans incarcerated in State and Federal prisons, and found that 72 percent of the cases were not adjusted as required. We estimated that nationwide, about 13,700 incarcerated veterans have been or will be overpaid by $100 million.

Additionally, overpayments to newly incarcerated veterans totaling approximately $70 million will occur over the next 4 years if VA does not establish appropriate controls.

Prior reviews of the implementation of GPRA in VA showed that while VA had made progress implementing strategic plans, the Department required additional efforts to achieve the ultimate goal of using performance measurement as a tool for improving the efficiency, effectiveness and economy of VA operations. We recommended establishing more specific and quantifiable performance measurements and holding managers accountable for the development and implementation of the Department's strategic plan.

During fiscal year 1998, the Office of Inspector General made significant contributions to the economy, efficiency and effectiveness of the Department's programs and operations. Audits, investigations and other reviews identified over $734 million in monetary benefits, including $31 million in recoveries. These monetary results constituted a return on investment of $21 for every dollar expended on OIG operations.

Additionally, our oversight of Departmental operations identified opportunities to improve benefit services and the quality of health care provided to VA patients. Finally, our criminal investigations and special inquiries resulted in 111 criminal convictions and 223 administrative sanctions involving patient homicide and assault, drug diversion, theft of Government property, bribery, kickbacks and benefits fraud.

This concludes my oral statement. I will be pleased to respond to any questions the Members may have.

[The prepared statement of Mr. Griffin follows:]

STATEMENT OF
THE HONORABLE RICHARD J. GRIFFIN

INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS

BEFORE
THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS, AND INTERNATIONAL RELATIONS

HEARING ON VULNERABILITIES TO WASTE, FRAUD, AND ABUSE

FEBRUARY 25, 1999

Mr. Chairman and Members of the Subcommittee,

I am pleased to be here today to discuss major performance and management challenges facing the Department of Veterans Affairs (VA) and the Department's progress in meeting performance and accountability measurements and goals under the Government Performance and Results Act. I will also highlight the contributions of the Office of Inspector General in combating waste, fraud, and abuse in VA programs and administrative activities.

The OIG is firmly committed to improving VA program operations and being of service to VA management officials. To that end, we have implemented a strategic planning process designed to identify the essential issues facing VA and to focus available resources on high-risk areas. The views and priorities of OIG stakeholders and clients, including the Secretary, administration and staff offices, Veterans Service Organizations, and the Congress, are thoroughly considered in determining the focus of OIG operations.

Last November I responded to Chairman Burton's request for the Office of Inspector General views on the 10 most serious management problems facing the Department. The following issues were identified:

- Challenges faced in allocating resources among the networks of VA medical centers.
- Prevention, management, and collection of debt owed VA.
- Untimely processing of veterans claims, appeals, and medical examinations associated with claims for benefits.
- Security of data in automated systems and physical security of systems and facilities.

- Reducing the high cost of workers compensation and preventing program fraud and abuse.
- Inaccurate or inappropriate benefit payments.
- Eliminating deficiencies in VA financial systems and achieving unqualified audit opinions on VA Consolidated Financial Statements.
- Ensuring that high quality health care is uniformly provided throughout the VA health care system.
- Ensuring VA operating systems and equipment are tested and modified to meet federal deadlines for Year 2000 compliance.
- Ensuring agency compliance with the Government Performance and Results Act and the accuracy of management information and reporting data.

I will highlight recent efforts conducted by my office that address some of these issues.

Quality of Health Care

Monitoring the quality of health care is a top priority for my organization. This year I directed that my Office of Audit, Office of Health Care Inspections, and Office of Investigations initiate a Combined Assessment Program (CAP) – to conduct recurring reviews of VA medical centers. These collaborative assessments of Medical Center operations will focus on key indicators or "Pulse Points," to provide medical center and Veterans Integrated Service Network management with timely feedback on the status of local operations and program effectiveness.

Workers Compensation Fraud

The 1916 Federal Employees' Compensation Act (FECA) authorizes benefits for disability or death resulting from an injury sustained in the performance of duty. The U.S. Department of Labor (DOL) administers the FECA program for federal agencies. The benefit payments have two components – compensation payments and payment of the cost of medical treatment for the disability. DOL reports that payments total about $1.8 billion annually - approximately $140 million annually for VA.

A collaborative effort involving OIG investigators and the Veterans Health Administration was initiated to identify VA employees who were fraudulently receiving workers' compensation benefits and private health providers who may be aiding and abetting the frauds. Investigations conducted under this effort disclosed evidence that 14 workers compensation claimants made false statements to the Government when they certified they were incapacitated from working due to on-the-job injuries. Indictments were obtained against these individuals and all were convicted. Fines and restitution exceeded $550,000 and savings to VA resulting from removing these individuals from the compensation rolls, is estimated at $4.4 million.

In 1998, we audited the workers compensation program at the request of the Department and concluded the program was not effectively managed and that by returning current claimants to work who are no longer disabled VA could reduce future payments by $247

million. (The DOL calculates savings based on the age of the recipient at the time of removal up to age 70, the life expectancy of these individuals.) Although the majority of inappropriate payments are due to poor case management, the audit also identified 26 additional potential fraud cases that were referred to our Office of Investigations. Based on the audit results, we estimated over 500 fraudulent VA workers compensation cases were being paid about $9 million annually. Similar conditions were reported in a 1993 OIG report.

To help ensure the integrity of VA's workers compensation program, we are developing a protocol package for VA mangers for enhanced case management and fraud detection.

Improper Payments to Federal and State Prisoners

In July 1986, our office reported that veterans who were imprisoned in state and federal penitentiaries were improperly receiving disability compensation benefits or needs based pensions. This occurred because controls were not adequate to ensure benefits were terminated or reduced upon incarceration, as required by Public Law 96-385. Department managers agreed to implement certain measures to identify incarcerated veterans and reduce or terminate benefits as appropriate.

We conducted a follow-up evaluation to determine if disability benefit payments to incarcerated veterans were appropriately adjusted, and other procedures agreed to in 1986 had been taken. We found that Department officials did not implement the agreed to control procedures and improper payments to prisoners continued.

We reviewed a sample of veterans incarcerated in state and federal prisons and found that 72 percent of the cases were not adjusted as required. We estimate that nationwide, about 13,700 incarcerated veterans have been, or will be overpaid by about $100 million. Additionally, overpayments to newly incarcerated veterans totaling about $70 million will occur over the next 4 years. if VBA does not establish appropriate controls.

Employee Embezzlement from the Benefits Program

OIG personnel and managers from VBA are currently reviewing management controls concerning veterans benefits payments. This review was requested by VBA in response to two recent OIG criminal investigations. In the first case, a regional office employee created a computer file in the name of a fictitious veteran, and paid benefits directly into an account opened by the employee under the fictitious name. The employee subsequently left VA for unrelated reasons. However, the fraudulent payments continued for several years until they came to light when the former employee was arrested on drug related charges. The loss to VA totaled over $624,000.

In another case, a supervisor at a regional benefits office established a computer record in the name of her boyfriend who is a veteran and created a series of fraudulent disability ratings and award actions, which eventually caused $614,000 to be deposited into their joint account.

Embezzlement by Veteran's Guardians

Perhaps some of most tragic exploitations occur when fiduciaries embezzle from the incompetent veterans whose funds they have been entrusted to protect. In one recent case, a fiduciary pleaded guilty to the misappropriation of $200,000 from six veterans. In another recent case, an attorney pleaded guilty to having stolen $113,000 from the account of a disabled veteran. We give investigations of this type the highest priority.

Government Performance and Results Act (GPRA) Implementation and Validity of Program Results Data

Prior reviews of the implementation of GPRA in VA showed that while VA had made progress implementing strategic plans, the department required additional effort to achieve the ultimate goal of using performance measurement as a tool for improving the efficiency, effectiveness, and economy of VA operations. For example, Departmental strategic plans either did not include program or performance measures, or incorporated measures which were not sufficiently specific and quantifiable to measure whether goals and objectives were achieved.

We recommended establishing: (1) more specific and quantifiable performance measurements to assess whether goals and objectives were achieved, and (2) management responsibility and accountability for the development and implementation of the strategic plan.

In 1998, we initiated a multi-stage audit to examine the integrity of the data used for GPRA reports. The first of the audits assessed the accuracy of three Veterans Benefits Administration (VBA) GPRA performance measures: (1) average days to complete original disability compensation claims; (2) average days to complete original disability pension claims; and (3) average days to complete reopened compensation claims. We found that reported processing timeliness was inaccurate. For example, more than 30 percent of the records reviewed in each of the three categories were inaccurate. Data from the automated systems used in developing GPRA reports indicated average processing times for all three samples were shorter than the actual processing times. We are working with the Department to establish procedures that will result in more accurate reporting. Our ongoing assessment to validate the accuracy and reliability of VA performance measures includes five VHA and one National Cemetery Administration performance measures.

OIG Accomplishments

During Fiscal Year 1998 the Office of Inspector General (OIG) made significant contributions to the economy, efficiency, and effectiveness of Department programs and operations. Audits, investigations, and other reviews identified over $734 million in monetary benefits - including $31 million in recoveries. These monetary results constitute a return on investment of $21 for every dollar expended on OIG operations. Additionally, our oversight of departmental operations identified opportunities to improve benefit

services and the quality of healthcare provided VA patients. Finally, our criminal investigations and special inquiries resulted in 111 criminal convictions and 223 administrative sanctions, involving patient homicide and assault; drug diversion; theft of Government property; bribery; kickbacks; and benefits fraud.

This concludes my formal statement, I will be pleased to respond to any questions you may have.

Mr. SHAYS. Thank you, Mr. Griffin.

We will now go to Jacquelyn Williams-Bridgers.

Ms. WILLIAMS-BRIDGERS. Mr. Chairman, members of the subcommittee, thank you for the opportunity to testify before you today on the major management challenges facing the Department of State.

The Office of Inspector has identified several significant challenges facing the agencies that we oversee, including the need to strengthen border security, consolidate the foreign affairs agencies, correct weaknesses in financial management and improve management and maintenance of real property overseas. I discuss each of these in more detail in the statement which I appreciate being submitted into the record.

I would like to focus my short statement on the Department's progress in addressing security vulnerabilities, especially overseas, the Y2K compliance and implementation of GPRA. No greater challenge exists for the Department today than that of providing safety and security for our people, our facilities and our information. The scope and gravity of this challenge was brought into clear focus by the attacks on our embassies in Africa late last year.

The Department faces an immediate need to address physical security vulnerabilities and to enhance emergency planning at our overseas posts. For several years, my office has reported that the Department faced the challenge of managing and funding the security of personnel, data and our buildings. The devastation caused by the terrorist strikes on our embassies in Nairobi and Dar Es Salaam fundamentally changed the approach to security at our missions.

The Department now assesses the vulnerability of mission buildings, the actual buildings, to terrorist attack, coming across national borders, in addition to the threat levels emanating from the cities in which our embassies are located. My office has made corresponding changes in our oversight to security.

The State Department Office of Inspector General provides the only regularized security oversight of all U.S. Government nonmilitary facilities overseas. I have recently taken a number of steps to significantly enhance the security oversight component of OIG.

First, we have expanded our security oversight by including experienced security officers on our routine post-management inspection teams. The security officer's attention focuses on physical security and the emergency preparedness of personnel at the post in times of crisis. This year, we plan to complete inspections of 31 posts.

In addition, we will complete security audits of our card access control programs at our missions, protective details, handling of classified information and overseas telecommunications security.

Second, we will provide oversight of the $1.4 billion in emergency security funds recently appropriated to the Department. A large portion of the emergency supplemental funds will go to procuring goods and services and construction of new facilities. Our office plans to perform pre-award contract audits to ensure that costs are reasonable.

We will also evaluate the adequacy of physical and technical security being built into our new buildings in Nairobi and Dar Es Sa-

laam. In addition, we will examine the security for construction personnel, onsite construction and logistics for transporting and installing items to be used in controlled access areas.

We also are pressing the Department for improvements in emergency preparedness. As a result of our recent audit in emergency evacuations, the Department reinstated its crisis management exercise program, which trains emergency action committees at posts on how to manage crises more effectively.

The Department also faces challenges in information systems security. Our own work has pointed to deficiencies in the Department's mainframe and communications systems security, including incomplete and unreliable security administration, inadequate training of information systems security officers, and the lack of controls over who accesses our information systems. GAO, as was mentioned earlier, reiterated our findings on the need for improved management of information security.

Another critical challenge facing the foreign affairs agencies is our vulnerability to the Y2K problem. Despite the Department's steady progress to prepare systems for the year 2000 date change, we are concerned that the Department's Y2K certification process is proceeding much too slowly. Failure to meet the Y2K challenge could create havoc in our community, including disruption of messaging systems, impediments to embassy operations, such as visa and passport processing, and failures in the administrative functions, such as payroll and personnel processing in the year 2000.

Embassies and consulates rely on their respective host country government's infrastructures to provide essential day to day services, such as water, power, and telecommunications. In some countries, these services could be disrupted if critical infrastructure components and control systems are not made Y2K compliant. Many Americans living, traveling, working overseas will certainly seek the services from our embassies should there be massive, sustained outages in a country.

My office has been actively engaged in Y2K efforts in three major areas. First, we helped the Department establish a process to certify Y2K compliance of its mission critical systems. We helped them write the guidelines that the bureaus now use to document that every necessary step has been taken to ensure that their most critical business processes will continue after January 1. In addition, we are reviewing the adequacy of the documentation they provide.

Clearly, for the certification process to work, the Department must speed up its processes to ensure that there is sufficient time to make any changes if they should be necessary before December 31st.

The second area of our focus in Y2K is in reviewing the Department and USIA efforts overseas to prepare for the millennium change. We have conducted assessments in 25 posts in 20 countries within the past 6 months to determine if our embassies are prepared. Early on, we found very little contingency planning in the event of failure of basic infrastructure services. The Department is aware of this problem and has sent a contingency planning tool kit, if you will, to all embassies.

Finally, because our U.S. embassies and Americans abroad might be vulnerable to Y2K failures, we are assessing the Y2K readiness of host countries where the U.S. Government maintains a presence.

In conclusion, I would like to make some observations on the Department's planning process, and its progress in implementing GPRA. As you know, the Results Act requires Federal agencies to set measurable goals for program performance and to annually report on their results in achieving those goals. Over the past 3 years, strategic planning efforts as required by GPRA have prompted notable improvements in the Department's planning process.

For example, at posts overseas, there is increased focus on and discussion by U.S. Government entities at posts about their collective sense of U.S. policy goals in a country. Also, there is a much improved collective assessment of all U.S. Government resources available at each post to be dedicated toward specific U.S. foreign policy goals. Prior to the GPRA mandate, our chief submissions could not readily identify the total U.S. Government resource commitment to U.S. foreign policy goals in a country.

The challenge that exists for the Department and its partners in the foreign affairs community is to define the goals stated in mission, bureau and Department plans in measurable terms and in terms of outcome. For example, what does the U.S. Government hope to achieve within countries and within regions?

Also, the Department needs to establish a credible system that will reallocate resources across geographic boundaries as changes in priorities and resource requirements are dictated by strategic decisionmaking.

This concludes my statement, Mr. Chairman. I would be happy to answer any questions that you or members of the subcommittee may have.

[The prepared statement of Ms. Williams-Bridgers follows:]

STATEMENT OF
JACQUELYN L. WILLIAMS-BRIDGERS
INSPECTOR GENERAL OF THE
U.S. DEPARTMENT OF STATE,
ARMS CONTROL AND DISARMAMENT AGENCY, AND THE
UNITED STATES INFORMATION AGENCY, INCLUDING
INTERNATIONAL BROADCASTING

FOR THE

COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND
INTERNATIONAL RELATIONS
U.S. HOUSE OF REPRESENTATIVES

FEBRUARY 25, 1999

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to testify before your subcommittee on the major management challenges facing the Department of State. As my office also oversees the United States Information Agency (USIA), including international broadcasting, and the Arms Control and Disarmament Agency (ACDA), my testimony will incorporate some management challenges that apply to all three agencies.

Summary

My office has identified several significant challenges facing the agencies that we oversee. Foremost among these is the safety and protection of our people, facilities, and information. The scope and gravity of this challenge was brought into clear focus by the attacks on U.S. embassies in Africa last year. The Department is faced with the immediate need to address physical security vulnerabilities and enhance emergency planning at our overseas posts. Longer-term challenges include major embassy renovations to improve security, new embassy construction, and the maintenance of security equipment.

Another critical challenge facing the foreign affairs agencies is their vulnerability to the Y2K problem. Generally, the Department is making steady progress toward preparing computer systems for the Year 2000 date change, and estimates that 55 of 59 mission-critical systems will be implemented by the Office of Management and Budget's (OMB's) March 31, 1999 deadline.

Despite this progress, we are concerned that the Department's Y2K certification process, which is designed to provide documented independent assurance that all possible

steps have been taken to prevent Y2K-related failures, is proceeding too slowly. Thus far, only two mission-critical systems have been certified by the Department's Y2K Certification Panel. Failure to meet the Y2K challenge could create havoc in the foreign affairs community, including disruption of messaging systems, impediments to embassy operations such as visa and passport processing, and failures in administrative functions such as payroll and personnel processing in the Year 2000.

I would also like to share with you some of our observations of the Department's planning process and implementation of the Government Performance and Results Act (Results Act). Although strategic planning efforts as required by the Results Act have prompted some improvements in the Departments planning process, more measurable goals and outcomes are needed.

Other major challenges faced by the Department include the need to strengthen border security, consolidate the foreign affairs agencies, correct weaknesses in financial management and improve real property management and maintenance. Before I provide additional details on these challenges, I would like to give you a sense of OIG's mission and responsibilities, as well as provide a brief overview of our strategic plan.

OIG Operations

OIG Organizational Structure

The mandate of my office is to improve the economy, effectiveness, and efficiency of the Department of State (the Department), ACDA, USIA, and the Broadcasting Board of Governors and to detect and prevent waste, fraud, and mismanagement. Toward this end, OIG consists of four operational offices that carry out inspections, audits, and investigations.

Office of Audits. OIG's office of Audits consists of seven divisions, each with a specific area of focus: Consular and International Programs, Information Management, Financial Management, Property Management and Procurement, International Broadcasting, Human Resources, and Contracts and Grants. Audits conducted by these divisions assess management and financial operations and the economy or efficiency with which an entity is managed. Examples of reviews the Office of Audits is currently conducting include the Department's Consular Fraud Program, Year 2000 (Y2K) remediation efforts, implementation of the International Cooperative Administrative Support Services (ICASS) system, management of overseas property, and financial statement preparation.

Office of Inspections. OIG is required by law to routinely inspect the activities of overseas posts and domestic bureaus. These inspections are conducted to provide overseas missions and domestic bureaus information about the effectiveness of their performance and the quality of their management and operations through an assessment of three primary areas: policy implementation, resource management,

and management controls. In FY 1998, the office inspected posts in 32 locations, including Russia, China, Thailand, and several African countries.

Office of Security and Intelligence Oversight. Through audits and inspections, the Office of Security and Intelligence Oversight evaluates the ability of overseas posts to respond to threats from terrorism, mobs, or other physical intrusion, intelligence penetrations, and crime through audits and inspections. The office also evaluates whether the Department's security and intelligence programs and activities are being carried out with the most effective use of resources and in accordance with the law. Our security oversight inspection program supports the Secretary of State's statutory responsibility for the security of all nonmilitary U.S. personnel, property, and information abroad.

In an effort to add greater rigor to OIG's intelligence oversight responsibilities, I created an Intelligence Oversight Division within the Office of Security and Intelligence Oversight. The division reviews foreign policy aspects of programs and functions involving components of the intelligence community and identifies key areas of concern in the review of intelligence oversight and coordination by chiefs of mission.

Office of Investigations. The Office of Investigations performs investigations of criminal, civil, and administrative misconduct related to organizational programs and operations. Additionally, the office manages a Hotline for employees who wish to disclose potential fraud, waste, and mismanagement. The office also focuses on fraud prevention by increasing employee awareness and understanding of the standards of conduct and accountability and by reducing areas of vulnerability and opportunities for misconduct. We publish "Standards of Conduct," a guide to ethical conduct, which is issued to each employee in the Department, USIA, and ACDA. My office also issues fraud alert bulletins and management implication reports when our work identifies systemic weaknesses that have agency-wide or bureau-wide implications.

Followup and Resolution

Once an OIG report is issued, Department bureaus or posts with responsibility for implementing the report's recommendations have 45 days in which to respond. The responses are reviewed by OIG to determine whether they meet the intent of the recommendation. In the event that the bureau or post does not accept the recommendation as written, OIG can either accept the suggested alternative, if any, or refer the decision to the next management level for reconsideration. If an impasse is reached in resolving a recommendation, it is referred for decision to the Under Secretary for Management or, ultimately, to the Secretary of State or agency director.

The OIG semiannual report to the Congress identifies audit significant recommendations unresolved or outstanding during the 6-month review period. In addition, the Secretary or agency Director is required to report to the Congress twice each year on any recommendations for which resolution has not been achieved within a year. Our most recent semiannual report shows outstanding OIG recommendations in areas identified as management challenges, including maintenance and repair of buildings overseas, financial system acquisition and development, mainframe systems security, and management of secure communications.

OIG Strategic Plan

The Secretary of State has established seven broad national interests and strategic goals for international affairs in the following areas: National Security, Economic Prosperity, Enhanced Services to American Citizens overseas and Controlling U.S. Borders, Law Enforcement, Democracy, Humanitarian Response, and Global Issues. The Secretary's National Interests provide the framework within which the OIG conducts its integrated program of audits, inspections, and interdisciplinary reviews to evaluate progress toward achieving the Secretary's objectives.

OIG's strategic plan establishes the OIG-wide goals that guide the work we will undertake into the 21st century. OIG strives to be proactive in addressing foreign affairs agencies' efforts to effectively implement U.S. foreign policy; clearly link resources to policy objectives; and maintain efficient, effective, and secure operations and infrastructures. We are committed to protecting the Secretary of State's ability to pursue the foreign policy objectives of the United States free from the impediments of waste, fraud, and mismanagement.

I would like to turn now to a more detailed discussion of the major management challenges facing the Department in the context of OIG strategic objectives.

Improved Implementation of Foreign Policy

The successful development and implementation of U.S. foreign policy depends on many factors. These include a clear understanding of foreign policy goals, coordination among the various agencies and entities with foreign policy interests, and clear and consistent lines of communication between the President, the Secretary of State, and the internal components of the Department.

Strengthening Border Security

Over the past few years, the Department has maintained a strong emphasis on the need to improve border security, however, the passport process and the immigrant and nonimmigrant visa processes remain material weaknesses. Improvements needed to address these weaknesses include additional management positions to support consular automated systems, expanded intelligence information sharing among U.S. Government

agencies, and the installation of modernized machine-readable visa systems worldwide. In terms of consular staffing, our own work has shown that the Department will face severe shortages of experienced midlevel managers for the next several years. We have also pointed out the need for more senior, experienced consular officers at posts with high fraud levels.

The Department has mounted a major effort to counter visa fraud, including initiatives such as the machine-readable visa program, worldwide advisories to overseas posts on detecting fraudulent documents, and programs to detect terrorists. The Department also continues to refine its consular lookout systems to identify names with different spellings or those that may be translated into multiple spellings. This will better enable the Department to identify individuals who should not receive visas. OIG is currently reviewing the Department's consular fraud prevention efforts to evaluate several aspects of the program, including the adequacy of the Department's guidance and training in fraud prevention and the coordination of antifraud efforts.

Our work in this area has facilitated several improvements in the Department's consular operations. For example, our recommendations helped ensure that the modernized version of the machine-readable visa system has the capability to electronically transmit relevant data on visa issuances to the Interagency Border Inspection Service for transmission to ports of entry. Also, our work encouraged the Department to establish a proactive program to identify individuals ineligible for a nonimmigrant visa in its computer system, such as drug traffickers, alien smugglers, and organized crime members. Additionally, an OIG recommendation contributed to the Department's ensuring that consular officers overseas have access to information on individuals from high-risk countries listed on the Department's CD ROM.

OIG also recently reviewed the U.S. border crossing card replacement program for eligible citizens of Mexico. The laser visa is more tamperproof than previous documents. However, many problems reduce the effectiveness of the program, such as the lack of laser visa processing equipment at consular posts in Mexico, an inadequate criminal database against which to check applicants, delays in production, and continued issuance of nonbiometric 10-year visas. Because the Department is not solely responsible for implementing this program with other agencies, a multi-agency effort will be needed to address many of these issues. The problems identified jeopardize the timely implementation of the program and compromise its enhanced border security protection.

Better Alignment of Fiscal and Human Resources with U.S. Foreign Policy Priorities

The Results Act requires Federal agencies to set goals for program performance and to measure results with the goal to improve the efficiency and effectiveness of Federal programs. Specifically, the law requires that each agency submit to Congress and OMB a 5-year strategic plan for program activities. The plan is to contain goals and

objectives, and how they will be achieved. Each agency is also required to submit an annual performance plan with measurable goals and indicators that link to the strategic plan.

Over the past three years, strategic planning efforts as required by the Results Act have prompted notable improvements in the Departments planning process. For example, at posts overseas there is increased focus and discussion on the U.S. Government's overall goals in each country. Also, there is an improved collective assessment of all U.S. Government resources available at each post to achieve specific mission goals.

The challenge that exists for the Department and its partners in the foreign affairs community is to define goals stated in mission, bureau, and Department plans in more measurable terms, and in terms of outcomes--what the U.S. hopes to achieve--rather than broad policy statements. In addition, the Department needs to establish a credible system that will allocate resources across geographic boundaries.

The upcoming merger of foreign affairs agencies will provide an opportunity to realign foreign affairs resources with policy priorities. Effective integration of the foreign affairs agencies will depend, in large part, on the success of merging diverse personnel systems, adapting varied and diverse information systems, and melding complex financial systems.

Linking Resources to Foreign Policy Priorities

In response to changing foreign policy priorities, and the need to demonstrate positive outcomes, the Department developed a strategic plan containing 16 international affairs strategic goals and 3 diplomatic readiness goals. The Department then asked each post and bureau to submit a plan and budget linked with the Department's strategic goals. At the request of the Department, OIG has been active in reviewing the mission and bureau planning process.

Mission Performance Plans are the principal vehicle for documenting and reaching interagency consensus on country-level goals and strategies. The Mission Program Plans, in turn, serve as building blocks for the Bureau Performance Plans, and ultimately, the Department's budget submission to OMB. However, OIG found that the process used during FY 1998 to develop Mission Performance Plans was poorly timed, and the guidance sent to the Bureaus and posts was unclear. The unclear guidance resulted in some incomplete or incorrect plans, and performance indicators that did not necessarily link with the indicators, baselines and targets included in the Department's overall performance plan. Further, the software intended to link budgets with goals and objectives, the Resource Allocation and Budget Integration Tool proved cumbersome, ineffective and difficult to deploy, and the Department is currently developing a new system to replace it. These problems resulted in corresponding weaknesses in the Bureau Performance Plans.

To date, the Department has been unsuccessful in implementing Results Act requirements for performance plans. The Department's FY 1999 Performance Plan, which was developed from the Bureau Performance Plans, did not comply with the Results Act, and both Congress and the Department identified several deficiencies with the plan. For example, the plan lacked baselines and performance targets, omitted management initiatives, contained goals that were broadly stated and extended beyond the Department's span of control, and provided little information on the resources required to achieve specific performance goals.

Although the draft of the combined FY 1999-2000 performance plan still does not comply with the Results Act, it is an improvement over the previous plan. For instance, the Department decided to focus its initial attention on the management bureaus, and as a result, the plan contains a comprehensive set of performance goals, baselines, and targets for the Department's diplomatic readiness goals. However, the sections in the plan on the 16 strategic goals are incomplete, providing only one illustrative goal paper under each strategic goal. For example, under the strategic goal on regional security, the Department provides a performance goal, indicators, baselines, and targets only for its efforts in Northern Ireland.

OIG will continue to assess the Department's progress in implementing the GPRA, and will take steps to verify and validate selected performance data. In addition, our audits will include reviews of the performance measures related to the areas reviewed. For example, our review of Foreign Trade Barriers will determine whether the Department's FY 1999 performance goals, indicators, and information sources accurately reflect its progress in opening foreign markets in the telecommunications industry.

The International Cooperative Administrative Support Services (ICASS) system was initiated in 1996 in response to a congressional mandate to implement a system that allocates to each department and agency the full cost of its presence abroad. Additionally, ICASS was intended to provide posts more control of administrative services through local empowerment, equity, transparency, local selection of service providers, and the establishment of customer service standards. The goal was to obtain quality services at the lowest cost. OIG initiated a review of the ICASS program to assess posts' progress in selecting the most cost-effective service providers.

Our work to date has generally shown that posts have not yet used ICASS to seek out more cost-effective service providers. There are a number of reasons for this: the process for selecting alternate providers is unclear, post ICASS councils lack training and expertise in selecting alternate service providers, and the Department and ICASS Councils lack the authority to mandate that other agencies participate in what may be the most cost-effective solution for the U.S. Government through economies of scale.

At some posts, a few agencies have opted out of ICASS services. While those agencies have reported reducing their operating costs from what ICASS charges, the total U.S. Government costs may be higher since costs were redistributed among the agencies

that did not opt out and ICASS staffing levels remained the same. We also found that some posts have not fully implemented ICASS, and ICASS information is not being used within Department headquarters elements to seek out more cost-effective alternatives.

Consolidating Foreign Affairs Agencies

The Omnibus Consolidated Appropriations and Emergency Supplemental Appropriations Act for FY 1999 mandated the consolidation of the Department of State, the Arms Control and Disarmament Agency, and the United States Information Agency into one foreign affairs agency.

OIG is addressing consolidation issues on a number of fronts. In a review conducted prior to the legislation merging the foreign affairs agencies, OIG recommended the consolidation of the security function in USIA and the Department. We determined that USIA's Office of Security could be merged with the Department's Bureau of Diplomatic Security resulting in more streamlined security activities. We identified about $500,000 in funds that could be put to better use, including up to 10 positions that could be used for other purposes in the security area. USIA's security staff will be formally integrated in October 1999 into the Department's Bureau of Diplomatic Security pursuant to the recent omnibus appropriations legislation.

The merger of the foreign affairs agencies also raises several challenges in the area of personnel management. Numerous policies and practices that differ between the Department and USIA such as assignment procedures, language training, tenuring regulations, and Senior Service competition rules will have to be reconciled. The Department has stated its intention to offer increased opportunities for retraining and upgrading employee skills and to work with USIA staff to integrate public diplomacy into the curriculum at the Foreign Service Institute.

Overseas tours of duty are another example where personnel policies differ between agencies. The Department's current policy of two- and three-year tours for staff at virtually all overseas posts differs from other government agencies, including USIA, where the tour is four years. A recent OIG review found that longer tours would reduce costs, and increase employee productivity. Costs could be reduced because longer tours would reduce the number of times employees move--the average cost of a move was over $18,000 in fiscal year 1996. Also, because of the considerable time necessary to become oriented to a new post, and the time at the end of the tour to bid for and transfer to the next post, longer tours would increase the time employees were fully productive in their current position.

Several studies by the Department and other groups have also recommended lengthening tours to improve effectiveness and achieve cost savings. However, in January 1999, Department officials announced that they would apply the Department's tour length policy when the foreign affairs agencies are consolidated, rather than adopt

longer tours. In our view, this is a missed opportunity for the Department to increase the effectiveness of overseas personnel while also achieving cost savings.

The consolidation of foreign affairs agencies also presents a challenge to incorporate the best use of technology by USIA into the Department. The Department faces the challenge of effectively merging its decentralized information resources management organization with USIA's highly centralized system -- at a time when both agencies are working to resolve Y2K problems in their respective systems. In addition, connecting USIA systems to Department systems must take into account necessary security considerations.

The pending merger of USIA and the Department has raised the issue of whether USIA's Y2K certification efforts meet the stringent standards set by the Department. USIA's current certification process is of concern for two reasons. First, it lacks independent verification of Y2K compliance because the same contractor is tasked with both remediation and validation. Second, USIA's certification guidelines do not contain the level of detail and specificity used by the Department. When USIA merges with the Department in October 1999, USIA functions and the systems that support those functions will become the Department's responsibility. As such, we believe it would be prudent for the Department to assure itself that USIA's systems are evaluated for Y2K compliance on the same basis as Department systems.

Financial management challenges are also associated with the consolidation of foreign affairs agencies. This includes integrating USIA and ACDA into the Department's Central Financial Management System, which is being upgraded. The preparation of accurate and timely agencywide financial statements which include data from each agency will be necessary. Complicating the process is the fact that neither ACDA nor USIA is currently required to prepare audited financial statements under the Government Management Reform Act.

The consolidation of the Department and ACDA is planned to occur during FY 1999; therefore, ACDA will be included in the Department's FY 1999 financial statements. Because ACDA is a fairly small agency in relationship to the Department, no significant problems are expected from the consolidation of the financial information. The consolidation of financial information with USIA is more significant and complicated. The Department and USIA plan to consolidate on October 1, 1999, which means the consolidated information would be reflected in the FY 2000 financial statement. However, to facilitate the preparation of the consolidated statements, as well as provide a proper accounting of assets to be transferred to Broadcasting Board of Governors, USIA should, at a minimum, prepare an audited statement of its financial position for FY 1999.

More Effective, Efficient, and Secure Operations and Infrastructures

The ability of the State Department, ACDA, and USIA to advance the foreign policy interests of the United States and their respective missions depends upon the quality of agency operations and infrastructure. Readiness to promote national interests and represent the United States to the world requires high-performance organizations with efficient and effective supporting systems.

As demonstrated by the terrorist attacks on U.S. embassies in Nairobi and Dar es Salaam, perhaps no greater challenge exists for the Department than providing adequate security to protect our people, facilities, and information. In response to the bombings, the Department is aggressively addressing physical security vulnerabilities and enhancing emergency planning at our overseas posts. I have also taken a number of steps to significantly enhance the security oversight operations of my office.

The foreign affairs agencies also face challenges in other areas related to operations and infrastructures. Generally, the Department is moving ahead on preparing computer systems for the Year 2000 date change, and expects to have the majority of its mission-critical systems implemented by the OMB deadline of March 31, 1999. Despite this progress, we are concerned that the Department's Y2K certification process is proceeding too slowly.

In the area of financial management, the Department's financial and accounting systems are inadequate, and there are significant concerns with the security of financial systems on the Department's mainframe computer systems. In property management, the Department has yet to establish a baseline of maintenance and repair requirements and costs for overseas property.

Addressing Security Vulnerabilities

The bombings of U.S. embassies in Nairobi and Dar es Salaam underscored the vulnerability of some of our posts and changed the approach to security at our missions for both the Department and OIG. Prior to the bombings in Africa, the Department generally allocated security resources to overseas posts based on the threat category of the city in which the diplomatic facility was located. The Department gathered threat information from a variety of sources and published a classified "Composite Threat List." Threats fell into four categories: political violence, human intelligence, technical intelligence, and crime. Threat levels in each of these categories ranged from critical to low. Embassies with a "critical threat" rating were generally allocated more funds for security enhancements than those embassies with "low threat" ratings. The bombings of our embassies, however, have caused the Department to realize that allocating resources based solely on the use of the Composite Threat List is inadequate. In addition to the threat rating, the Department now factors in the vulnerability of all posts to terrorist attacks. Under this new approach, all posts should meet a high level of protection against acts of terrorism and political violence.

In response to the attacks on our embassies last year, the Department conducted an extensive review of mission security around the world and identified eight facilities so vulnerable that the missions will be moved into safer, more secure facilities as quickly as possible. In Nairobi, the mission is moving into interim office buildings that will provide a degree of security until new office buildings can be constructed and occupied. In Dar es Salaam, such a move has already taken place. Construction of new embassies in these countries is scheduled to be complete by 2003. The Department also plans to undertake significant renovations to address serious vulnerabilities at other locations. For example, the Department plans to enlarge the setback at one post at a cost of $21 million.

To enhance emergency response, the Department plans to spend $118 million on handheld radios. This will serve to upgrade the entire emergency radio program and send new radios to every overseas post for use during an emergency. The Department is also planning to purchase satellite telephones so that posts and emergency response teams can depend on reliable communication during and after an emergency.

Staffing shortages in security have been addressed by the recent supplemental appropriation, and the Department is engaged in an aggressive recruitment program for both security officers and security engineers to increase its workforce. However, the training period in the Department before new security officers gain the expertise to perform successfully overseas has historically taken up to 6 years. The new officers will be going overseas with only 2 or 3 years of experience. To examine the adequacy of the Department's support of these new officers, we plan to review the Bureau of Diplomatic Security's overseas operations management in the coming year.

I have taken a number of steps to significantly enhance the security oversight operations of my office. First, we have expanded our security oversight inspections to include low and medium threat posts. Also, routine post management inspections now include an experienced security officer who focuses on physical security and emergency preparedness, and prepares a classified security annex to the inspection report. This year we plan to complete 16 security inspections, and to have our security officers accompany routine inspection teams to 15 additional posts. We also will complete security audits of the card access control program, protective details, the protection of classified information, and overseas telephone security.

Second, our new Security Enhancements Oversight Division will provide oversight of the $1.4 billion in emergency security funds, and future funding received by the Department, to enhance overseas security. OIG will evaluate physical and technical security being built into the new office buildings in Nairobi and Dar es Salaam. In addition, OIG will examine security for construction personnel, on-site construction, logistics for items used in the controlled access areas, and contract management. This Spring, an inspection team will evaluate the security at the interim office building in Dar es Salaam and the temporary office building in Nairobi.

Because a large portion of the emergency supplemental funds will go toward procuring goods and services and the construction of new facilities, OIG plans to provide audit assistance to ensure that contract costs are reasonable. OIG may audit selected contractors prior to award and at contract completion, and provide technical support to Department contracting officers in reviewing contractor proposed costs.

OIG already provides oversight of the embassy construction project in Moscow, Russia. The Moscow Oversight Team, established in 1994, provides oversight to the Moscow chancery construction project. The team was formed in response to the costly security mistakes that characterized previous construction efforts of Embassy Moscow. Rather than waiting to identify problems after the construction is complete, we have undertaken this ongoing oversight effort in order to flag potential vulnerabilities so that they can be addressed promptly. With this approach we are contributing our expertise to facilitate project completion on time, within budget, and in a secure manner.

Another important oversight project for OIG will be the China 2000 initiative, which is scheduled to enter the design phase in FY 1999. The Department will have to respond to several formidable challenges in order to construct secure compounds. Construction security oversight is critical to ensuring that the China 2000 project adequately addresses security needs, and that security systems, once designed, will function as intended.

Followup on Security Recommendations

For several years, my office has reported that the Department faced significant challenges in managing and funding security and made numerous recommendations to address specific vulnerabilities at our missions worldwide. The Department has generally corrected deficiencies identified by OIG where they have had resources available to do so. Of the 588 security recommendations made in FY 1997, the Department agreed to correct approximately 90 percent of the deficiencies and completed action on about 50 percent within one year after they were identified.

However, many of the recommendations still outstanding are significant, and require major capital investments to implement. Examples include relocating missions to safer facilities, building safe havens, or improving walls that surround the facility. Despite the recent emergency appropriation, the Department continues to face funding shortfalls. Security equipment will also need long-term funding. An OIG audit of the maintenance and repair of security equipment found that, despite the fact that much of the Department's equipment, purchased in the mid-1980's, was reaching the end of its useful life or was obsolete, the Department had not budgeted for new equipment.

OIG's audit of overseas card access systems found similar problems with equipment maintenance. The Department lacked a uniform program for the installation, repair, and maintenance of the card access system equipment. In addition, the equipment was never certified for use and, in some cases, was locally procured and maintained. We

have serious reservations as to whether the card access control systems can effectively control access and protect sensitive information. Our security inspections have repeatedly demonstrated that security at "lock-and-leave" posts without 24-hour cleared U.S. Marine Guard protection is often inadequate to protect classified material.

Emergency Preparedness

As a result of our audit on emergency evacuation, the Department reinstated its crisis management exercise program, which trains emergency action committees at posts on how to manage crises more effectively. The ability of posts to respond to emergencies, such as natural disasters or terrorist attacks, is greatly enhanced by the Department's crisis management exercises and emergency drills. However, our security inspections consistently report that posts are not conducting the required drills needed to prepare for likely attacks. In addition, we recently reported to the Bureau of Diplomatic Security on specific steps it should take to enhance procedures for vehicle bomb drills and coordinate with the Accountability Review Board, which addressed this in its report. In this respect, security inspection teams recommend regular practice of "duck and cover" drills along with specific recommendations for immediately alerting staff to vehicle bomb attacks.

Strengthening Information Security

The Department faces significant challenges in information systems security. Our work has pointed out deficiencies in the Department's mainframe and communication systems security, including incomplete and unreliable security administration, inadequate training, and lack of access control. Similar problems have been identified in specialized telephone switching and card access computer systems. In many cases, the Department is modernizing systems without a parallel effort to improve information security. A May 1998 General Accounting Office audit report reiterated our findings on the need for improved management of information security.

The Department also does not have sufficient backup capability at major data-processing facilities for use in an emergency; an issue raised by several OIG audits since 1989. The Department is in the process of developing a mainframe contingency program to provide an alternate processing site in the event of an existing system failure. OIG has stated that those backup sites and systems currently in place will not be effective until issues including planning, coordination, training and resources are resolved. In addition, once established, the contingency plans will need to be tested to ensure they work as planned.

Open OIG recommendations in the area of information security call for the Department to establish a security program for the mainframe system to address risks identified by OIG and to ensure that responsible officials are identified and kept informed about the systems security. We have also recommended that the Department require personnel who hold positions with access to bulk quantities of sensitive information to

undergo a special counterintelligence screening process prior to each assignment. This last issue will be the subject of an OIG audit scheduled to begin next month.

Achieving Y2K Compliance

Another critical challenge facing the foreign affairs agencies is their vulnerability to the Y2K problem. Generally, the Department is making steady progress toward ensuring that it is ready for the Year 2000 date change. As of February 8, 1999, the Department reported that 36 of 59 mission-critical systems had been fully implemented, and it expects to have 55 mission-critical systems implemented by the March 31, 1999, OMB deadline. Despite this progress, we are concerned that the Department's Y2K certification process, which is designed to provide documented independent assurance that all possible steps have been taken to prevent Y2K-related failures, is proceeding too slowly. Thus far, only two mission-critical systems have been certified by the Department's Y2K Certification Panel.

Failure to meet this challenge could create havoc in the foreign affairs community, including disruption of messaging systems, impediments to embassy operations such as visa and passport processing, and failures in administrative functions such as payroll and personnel processing in the Year 2000. The Department's presence at more than 260 locations worldwide increases the Department's challenge to continue functioning effectively in the Year 2000. Embassies and consulates rely on their respective host countries' infrastructures to provide essential, day-to-day services such as power, water, telecommunications, and emergency services. In some countries these services could be disrupted if critical infrastructure components and control systems are not made Y2K compliant.

My office has been actively engaged in Y2K efforts in three major areas. First, we assisted the Department in its efforts to develop certification guidelines identifying what steps the Department must take to determine whether systems are Y2K compliant, and identified documentation needed to certify computer systems as "Year 2000 ready." OIG is also evaluating the adequacy of certification packages prepared by bureaus for mission-critical systems. Second, we are reviewing Department and USIA efforts overseas to prepare adequately for the millennium change. This effort includes monitoring efforts of our overseas posts to raise global awareness of the Year 2000 problem, ensuring that U.S. embassy and consulate system vulnerabilities are properly addressed, and reviewing post contingency plans. Finally, because U.S. embassies and Americans living and working abroad might be vulnerable to Y2K-related infrastructure failures, we are assessing the Y2K readiness of host countries where the U.S. Government maintains a presence.

Our work with the Department has resulted in several improvements. A clearer definition of what constitutes "Y2K compliant" resulted in more accurate reporting to the Office of Management and Budget on the status of the Department's Y2K effort. OIG findings also resulted in greater focus on Departmentwide project management tracking;

discovery of seven new applications, which were added to the Department's system-tracking database; and development of a new rating system that tracks and evaluates system interfaces.

OIG has conducted site assessments in 25 cities in 20 countries as part of an aggressive effort to review embassy preparedness and collect and analyze information on host country Y2K efforts. Early on, OIG found little contingency planning at posts in the event of a failure of basic infrastructure services on January 1, 2000. The Department is aware of this problem, and is sending a Contingency Planning Toolkit to all embassies and consulates to assist them in developing their respective plans.

In our effort to assess the readiness of host countries to address Y2K-related problems, OIG has met with representatives from foreign governments, key infrastructure sectors, and private industry in each country we visited. We have provided information summaries on each of these countries to the Department, USIA, the President's Council on the Year 2000 Conversion, congressional committees, and other foreign affairs organizations.

OIG has initiated a series of USIA Worldnet Interactive broadcasts throughout Latin America and Canada. In coordination with the Organization of American States and USIA, these interactive programs have been broadcast live throughout this hemisphere and worldwide via the internet to explore problems, strategies and solutions in the areas of timely contingency planning, energy and financial institutions readiness, and auditing techniques to promote Y2K compliance.

Correcting Weaknesses in Financial Management

Financial management continues to be another major challenge facing the foreign affairs agencies. The Department accounts for more than $5 billion in annual appropriations and over $16.7 billion in assets. The Department has made significant improvements in financial management since the Chief Financial Officer's Act was passed in 1990. OIG has focused on the Department's financial management through our audits and annual review of the Department's progress to improve material weaknesses in conjunction with the preparation of the Federal Manager's Financial Integrity Act (FMFIA) report. Over the past few years, the Department has complied with OIG recommendations in areas such as disbursing, cashiering, travel advances, and accounts receivable, which significantly improved these areas and led to these weaknesses being removed from the FMFIA report.

However, a number of significant concerns still exist, some of which have been outstanding for a number of years. Although OIG's audit of the Department's 1997 agencywide financial statements showed that the Department's statements were free of material misstatements, the report brought to management's attention significant concerns with the security of the Department's domestic main frame computer.

OIG's audit of the Department's 1997 agencywide financial statements also raised concerns about the inadequacy of the Department's financial and accounting systems, which is both an internal control weakness and an issue of noncompliance with several laws and regulations, including the Federal Financial Management Improvement Act (FFMIA). The FFMIA requires that agencies report whether the Department's financial management systems substantially comply with the Federal financial management system requirements, applicable accounting standards, and the United States Standard General Ledger at the transaction level. Based on our review, OIG found that the Department does not substantially comply with one aspect of the FFMIA, that is the Federal financial management system requirements. The Department has reported its financial systems as a high-risk area and a material nonconformance for more than 15 years in its annual FMFIA report.

OIG has urged the Department to focus attention on its financial systems and to develop benchmark performance indicators to measure the improvements to these systems. In response to our recommendations, the Department is planning to study the level of compliance with the FFMIA and to prepare a remediation plan as required by that Act. The Department also has efforts underway to improve these systems, including upgrading its Central Financial Management System and developing standard financial capabilities for overseas posts.

Issues regarding timeliness of the financial statements and data, internal controls over major processes, and presentation of data for new requirements have yet to be resolved. OIG's last two audits of the financial statements identified the inadequacy of internal controls over the management of unliquidated obligations. Although we have recommended that the Department focus on this area, our preliminary audit work on the Department's 1998 financial statements shows that these weaknesses persist.

In addition, we have recommended that the Department ensure that adequate resources are devoted to financial statement preparation, especially during the preparation of the FY 1998 financial statements due to the increased reporting requirements. Based on our preliminary work, however, we have found that the Department is still unable to provide certain financial documentation by the agreed upon deadlines.

Grants management is another area of financial management weakness in USIA, and needs to be carefully considered in the consolidation with the Department. USIA annually awards about 500 domestic grants and cooperative agreements totaling approximately $240 million, about 1500 overseas grants totaling about $20 million, and numerous transfers to bilateral commissions and foundations totaling $120 million. OIG's audits have identified unauthorized, unallowable, and unsupported costs, internal control weaknesses, or noncompliance with applicable regulations associated with these awards. For example, OIG identified about $1 million in surplus funds at the Fulbright commission in India. USIA fully implemented our recommendation to offset the commission's 1998 allocation resulting in a one-time cost savings. Screening and monitoring of the recipients of these funds will become more critical because under

revised Office of Management and Budget guidelines, the majority of USIA's grantees will no longer be required to have annual financial audits.

Overall, Federal assistance funds in the form of grants, cooperative agreements, transfers, or loans from the Department, USIA, and ACDA total over $1 billion annually. For example, the Department's migration and refugee assistance programs alone amounted to $650 million in FY 1998. The Department is currently considering alternatives to managing grant activities once consolidation occurs.

Improving Real Property Management and Maintenance

Currently the Department reports holding 12,000 properties with an estimated historical cost of about $4 billion. OIG has identified problems in the Department's acquisition and disposition decisions for real property, including funding decisions. These findings contributed to legislation requiring the establishment of a Real Property Advisory Board to act as the arbitrator of disposal or retention of oversized, underutilized, and high-value properties. OIG has completed a review of the activities of the Board, and found that disputed properties are appropriately chosen for the Board's review and recommendations of the Board are based on sufficient information.

At the request of the Under Secretary for Management, OIG is working with the Department to assist in identifying excess, underutilized, and obsolete government-owned and long-term leased real properties worldwide. OIG has conducted limited reviews of real property in the course of its ongoing audits and inspections at overseas posts. Since March 1998, OIG has provided the Department with reviews on 48 posts, and is in the process of completing reviews on another 24 posts. The reviews can be used by the Department to manage the acquisition and disposition of overseas real property assets.

To date, OIG reviews have identified 5 properties as excess and 81 properties underutilized. An example of the latter included a nearly 1-acre unpaved site near the chancery building in Paris used to provide parking for official vehicles and free parking to some embassy employees. According to post officials, there were plans to construct an office building on the site in the mid-1980's, but those plans had been rejected. The Department has no plans to develop this site, and has stated that sale of the property would raise security and operational concerns. OIG reviews also identified 6 properties as obsolete. For example, OIG has identified two obsolete properties at Embassy Harare, requiring immediate Department attention for disposal action.

OIG reviews also noted 29 properties that the Department had previously identified for future development or disposal when local economic conditions become favorable. Examples include properties in Bangkok, Seoul, and Kathmandu.

The Department and overseas posts have recently addressed many real property maintenance and repair issues, in part, due to the work of the OIG. In 1993, OIG recommended that the Department establish a system to identify and monitor the

worldwide maintenance and repair requirements and establish an initial baseline for outstanding maintenance and repair requirements. In response to the recommendation, the Department has established a system to identify and monitor requirements, but has not analyzed the information contained in that system to establish a baseline of maintenance and repair requirements and costs. Future OIG work will evaluate the Department's systems to identify, prioritize, and perform maintenance and repair.

* * *

In conclusion, Mr. Chairman, I have outlined what my office believes are the major management challenges facing the foreign affairs agencies we oversee. While we have focused much of our work in these areas, there are no quick fixes. Indeed, several of these issues have been the subject of repeated OIG recommendations. Overcoming these challenges will require careful and long-term management attention. In some areas, such as addressing security vulnerabilities, additional resources will be required.

I look forward to working with members of this subcommittee in the coming year on many of these issues. I would be pleased to answer any questions you may have.

Mr. SHAYS. Thank you very much.

I am going to recognize Mr. Tierney from Massachusetts first. But I am going to make a request of all of you for the question I am going to ask, and I wanted to give you some time to think about it. I want each of you—and I would like, when I say each of you, not just those of you who have testified, but all of you at this table—to give me your top two priorities, if you were the chairman or ranking member of this committee, as to what you would look at if you were on this committee.

Mr. Lieberman, I am going to be asking you to do the same thing, and Ms. Hill, and I know you have the kind of relationship that you may come up with two different answers. That is all right. Because it will be more helpful that way. I hope we have that independence. So I am going to ask each of you here, and you will not tell me right this second, because Mr. Tierney will be asking you some questions, then we will go to the ranking member. Then we will go back and forth.

I thank you for all of your testimony.

Mr. TIERNEY. I thank you. I would almost rather hear that answer first than ask questions.

Mr. SHAYS. We have to give them time to think of it.

Mr. TIERNEY. Ms. Hill, you indicated in your testimony that some estimated monetary benefits of the number of audits that were done in compliance was about $18.6 billion. Can we anticipate savings in that ball park as we go forward, if we continue the processing of auditing and cooperation?

Ms. HILL. You cannot guarantee that you will have the same amount of savings. But I can say that we have consistently come up with high savings figures not only in terms of audits, but also in terms of our recoveries from civil and criminal cases. Recovery figures have been consistently high. I would echo what Mr. Griffin said about VA. Historically, at the OIG's office in Defense, there has been a substantial return on costs. In other words, the cost of operating the Inspector General's office is far outweighed by the dollar we are able to return to the Department.

Mr. TIERNEY. Thank you. You also testified that there were barriers, in your remarks on that. Would you expand on that a little bit, what effect does that have on this?

Ms. HILL. I think there are a couple of things to consider. One thing that strikes me about the Department is that it is simply huge to start with. It is a massive task for anybody to manage the Department. And that is compounded by the fact that within the Department, because it is so huge, you have the services and you have all sorts of other, I call them fiefdoms, out there, whether they are agencies or commands or services.

Historically, it has been a stovepiped organization. Everybody has had a separate chain of command. So it is very difficult to break down that historical culture, if you will, and try and integrate the Department and get, not only the services, but all the different parts and the components of the civilian side of the Department to focus on these common problems. It is very, very difficult.

An example is in the financial management area, where the Department has had to combine systems, financial systems and accounting systems, that historically were developed among the serv-

ices. They have tried to bring those together. One of the big problems now is to get good financial information into DOD's finance and accounting systems, which need to be vastly improved to get clean audit opinions. Part of the problem is that the information that comes into those systems comes from all sorts of what we call "feeder systems" throughout the Department that are run by separate entities. So you have to get them integrated with the finance and accounting systems to try to get a smooth transition and accurate information.

So, it is still very fragmented, there are a lot of walls, and barriers and there is a lot of parochialism. One of the biggest challenges is simply to get so many different organizations or different components to work together on common problems.

Mr. TIERNEY. Mr. Hinton, did you want to make a remark on that?

Mr. HINTON. We have the same concerns that Ms. Hill does across this whole area, where you have the individual components that are very difficult to cut across. That is one of the cultural issues that we see within the Department in trying to move to achieve efficiency across all the issues I think we have been talking about, particularly Ms. Hill and myself, as it relates to the business activities, whether it be financial management, logistics, or acquisitions. We have that phenomenon that is out there, and we have to find ways to find more jointness across those business activities to get the efficiencies that we need.

Mr. TIERNEY. Let's talk about that for a second. When we look at recommendations from the different branches to those of the F–22, the FA–18, the joint strike fighter or whatever, those recommendations to build simultaneously all of those, moving in the direction, are those likely to be affected by this kind of parochialism and culture?

Mr. HINTON. I think that is an ultimate issue for the Congress and the administration, because it is one of affordability. As we look at all the priority needs for the Department, we have to ask ourselves the question that Congress has to ask, where do we have the highest priority needs, do we need three separate tactical aircraft programs working at one time. That is a judgment that has to be made in part up here.

Our work has looked at the individual systems to try to keep the facts and analyses up here around the individual systems on cost, schedule and where they are against performance for the individual systems. But the ultimate question is going to be, can we afford all three, and will that meet the top needs that we have going into the next century?

Mr. TIERNEY. In view of the larger amounts we are now talking about in the national defense system on this, the missile defense system on that, are you of a mind that the Department of Defense is being overly optimistic with regard to the maturity of this particular system?

Mr. HINTON. I think that what we have seen over our work has been mixed across the various programs, whether they are aircraft, national missile defense and those things. A lot of this evolves around technology, where are we and how ready are we to launch programs. Do we have the knowledge that the technology will

work? Where we have seen some of the concerns that we've had in the past was, we would move too quick to launch programs, hence you come up with a lot of the concerns that we've raised in the acquisition programs that we've exceeded costs, it has taken longer to produce the systems, and we did not get what we started out to get for those systems to do. That was because of technology, unit costs rose as we did not have all those answers at the beginning.

National missile defense, I think that is a tremendous challenge. The counsel that we would offer is that we need to move slowly to make sure that we have a good system that works. I think that is part of the debate that has to occur as DOD comes up for its funding to support the programs for that.

Mr. TIERNEY. Ms. Hill, do you have a comment on that?

Ms. HILL. We have not looked specifically at that proposal. But I would share what Mr. Hinton just said, that historically there have been problems in starting out down the road to get something, and then we find out it has either slipped the schedule, or it is not what we really wanted in the first place. Those sorts of things happen repeatedly.

I would think if they are going to embark on something like that, it needs to be done very carefully. Hopefully all the lessons learned from the past mistakes, will be considered.

Mr. TIERNEY. Thank you.

Mr. SHAYS. Mr. Blagojevich, you have the floor.

Mr. BLAGOJEVICH. Thank you.

Mr. Hinton, I would like to talk a little bit about the discrepancy between the administration's request of $3 billion over 5 years to bring the U.S. embassies into compliance with security standards and a group headed by Admiral Crowe, which recommends the spending of $14 billion over 10 years to meet those security needs. I am hopeful, first of all, that you saw the reports, and second, rather than tell us who you think is right, could you give us your assessment with regard to the financial and management processes used by the two groups, Admiral Crowe's group and the administration, to determine these estimates?

Mr. HINTON. Congressman, we have not looked specifically behind the estimates on these programs. I think as Ms. Bridgers mentioned in her statement, and I kind of reinforced across the three agencies here, our concern at the Federal level has been over whether or not the systems give you good data in terms of the cost of the programs. That is one issue I think that is very important as we think through the cost of these programs. That is a key issue we really have to define, what are the requirements and what are the true costs.

I would also echo something that Ms. Bridgers raised, too, is a challenge in this area and that is knowing what the Government's full presence is overseas. Not just State, but look at the other agencies over the years where there has been growth in the overseas deployment of their resources. So you have to factor that into the total picture and determine your requirements. Then you have to come up with good methodology to assess the cost.

Then I think the true challenge that is out there, and it goes back to some work that we have done in the early 1990's, where we had issues around the capacity to carry out and actually do the

programs that we set up for enhancing the security of our overseas missions and folks that we had deployed overseas. We found issues of not having adequate resources, both on the human side, questions around contract management issues, site selection issues, and a host of those programmatic issues that have to be carefully looked at as we advance into this area.

Mr. BLAGOJEVICH. Mr. Hinton, some of those deficiencies, can you give us an illustration of what you are talking about?

Mr. HINTON. Well, I think that you have to look at the data behind cost estimates. And you have to look at the assumptions and see whether or not we agree with the assumptions upon which the estimates are made. That is going to be very key to the members of this committee and also the appropriations committees, as we decide the amount of money to go forward to support the estimates. I think that remains to be seen in terms of the total costs.

We have the varying estimates out there, and I think we have to look carefully at them, and we have to ask ourselves the capacity question. Do we have a good program to launch, do we have the right people, do we have the right designs, do we have the right location for the security issues that Jackie brought up to you. I think they are the fundamental types of questions we need to ask.

Mr. BLAGOJEVICH. OK. Ms. Williams-Bridgers, are you familiar with the report by Admiral Crowe and the administration's position?

Ms. WILLIAMS-BRIDGERS. Yes, I am generally familiar with the findings.

Mr. BLAGOJEVICH. Could you just kind of free flow and tell us what you think?

Ms. WILLIAMS-BRIDGERS. I would be glad to. I would like to make three points about Admiral Crowe's report. First, I would like to say he provided invaluable information to the community. Some of the recommendations, in fact, reiterated some of the same types of recommendations OIG had made about the need for emergency preparedness, the need for duck and cover drills. When you hear the indications of a bomb going off, do not go to the windows and look out and see what is happening. Find some place to hide under and prevent the glass from injuring your body, which so often occurred in the two attacks last August.

Three points about the Crowe report. One is the $1.4 billion that he estimated for annualized costs of embassy security. It is just an estimate. It was based on his review, the panel's review of what happened in Africa. The $1.4 billion may not be enough. Because Africa is not representative of all the types of threats in security vulnerabilities that we have throughout the world, first point.

A couple of years ago, OIG looked at what is the security posture of DS given its current levels, then-current levels of funding. What we found was that security resources for diplomatic security had declined by 12 percent between 1991 and 1996. They were providing minimal levels of safety to personnel overseas, minimal levels of security to our buildings overseas, at that point in time.

So I think we need to look behind the $1.4 billion. We did not look at all the methodology used to come up with that estimate.

No. 2, we must go beyond the Crowe report. As I mentioned, the Crowe report looked at Africa, looked at what happened in Africa

as any accountability review board should do. But what it did not take into account as adequately as we think should be taken into account is the trans-national threat. In Africa what happened was, we had embassies where we never suspected there would be a terrorist strike. Because those were low terrorist posts.

The threat came across the borders, from places that we least suspected. So we have to take that into account now, and we are taking that into account now, with the revised methodology, to analyze the integrity of our buildings to sustain any attack, regardless of where that attack comes from.

A third point, some of our posts will never be secure, given where they are now. Are we going to move London? Are we going to move Paris? Can we afford to relocate to places to provide adequate setback? It would be tantamount to buying a Manhattan city block, the investment that we would have to make.

Another point I would like to make, though, about the cost estimates of the Department, one of the things we are most concerned about in the representation of the budget is that there is no allowance for recurring costs, the maintenance, the operating, the life cycle costs associated with equipment that the Department intends to procure. The costs that we see as represented in the budget are for procurement only. So we have to look long term, what is the investment going to be.

Mr. BLAGOJEVICH. Thank you.

Mr. SHAYS. What I'd like to do is, Mr. Backhus, I will start with you. Basically you have the VA responsibilities. What would be the first two priorities?

Mr. BACKHUS. May I have a third as it relates to the DOD?

Mr. SHAYS. You may have a third. Let me just say, the purpose for this is that this committee has the resource of 11 members on the majority side and 2 on the minority, but they also have other responsibilities as well. So our resources are limited, and we want to really make sure we are spending them well.

And I also will say, you may give us a very important issue, all of you, to look at. But we may determine that another committee is going to be doing that extensively. But yes, you may have three.

Mr. BACKHUS. Obviously, limiting issues to two probably puts this in the realm of those that are the most difficult to deal with. Understand that.

The two issues I would really concentrate on working on in VA are first, as far as the health care side of VA goes, the infrastructure of that system. If you were going to build a health care system today, it would not look like the current VA health care delivery system. They are not structures that are built to provide health care in the next century. They were built to provide health care a long, long time ago.

The future for health care is not in that kind of a delivery system. Consequently, they have hundreds of facilities that are not well suited for that mission. Roughly, we are talking about approximately 25 percent of the health care budget is consumed by the cost of keeping those buildings maintained.

If there was a way to potentially close hospitals and open more ambulatory kinds of health care facilities that can do outpatient surgeries on a more efficient basis, that could be located closer to

veterans, I think care would improve, access would improve and costs would probably be less.

Mr. SHAYS. An excellent suggestion. I am going to suggest that that is going to be Mr. Blagojevich's suggestion, to have a VA BRAC.

Mr. BACKHUS. Good luck.

Mr. TIERNEY. How does that play into your community based outpatient clinic? Is that the alternative?

Mr. BACKHUS. That is the step in the right direction, that is correct. And it is great to open up those community based outpatient clinics. But there is a limit to how many there are going to be that they can open, given that VA is burdened and saddled with this huge infrastructure that they have to continue to fund and maintain.

So if that money from those huge over-built, inefficient facilities could be transferred into these community based outpatient clinics, you have a much more efficient and effective health care delivery.

Mr. SHAYS. Kind of like a base closing bill, though. But it is very significant. What is No. 2?

Mr. BACKHUS. Switching over now to the benefits side, the VA pays some $20 billion a year in compensation to veterans with disabilities. They have struggled for years to do and adjudicate claims in a timely fashion. In fact, there was an article in the paper the day before yesterday about this, and their re-engineering attempts to reduce that backlog and the timeframe; they have just been unsuccessful.

So we are talking about a need to really re-engineer and to restructure this whole benefits area to be more responsive to the veterans. In some cases, appeals to the initial adjudication take 2 years to resolve. So we have veterans who are waiting upwards of 3 years for a determination as to whether their claim will be approved.

Mr. SHAYS. One thing this committee could do would be to look at how long it takes claims to be resolved and decide how that process could be sped up.

Mr. BACKHUS. Yes, I think we are really talking about a technology infusion here that is going to be needed. This is a paper-intensive kind of activity.

Mr. SHAYS. You asked for three.

Mr. BACKHUS. I did, because I also have responsibility for evaluating the military health care system.

Mr. SHAYS. That is wonderful that you are connected to the two. That is the advantage GAO has.

Mr. BACKHUS. There is an opportunity here, I think, for a lot more jointness between the DOD and the VA. I heard these folks talk about the stovepiping that occurs within the Department of Defense. Well, there has also been historically a lack of cooperation and collaboration between the VA and the military health care systems.

They do a lot of things alike, health care is health care in many respects. They have facilities that they could share considerably more. There is purchasing they could share considerably more. There are personnel that they could share significantly more. And it goes on and on and on.

I have to say there is progress that has been made over the years to get the two departments to work together more collaboratively. It is, however, probably just a pittance of what the potential really is though.

Mr. SHAYS. One of the advantages GAO has is that you can cross different departments. I know Inspector Generals speak with one another and so on, and there is coordination. But you can do it more directly. But the committee can do the same thing.

In my former life as chairman of the Human Resources Subcommittee in Government Reform, we oversaw all of HHS and VA. So we brought in one of the employees we had then, and we thought to ask her to do just particularly your third recommendation. How we can coordinate the two? I can see coordinating and having some impact with No. 2 as well—the benefits side.

Mr. BACKHUS. Is that Marcia? Yes, we have been working with her.

Mr. SHAYS. Did she put this idea in your bonnet? Because this is—I was going to change her responsibilities, now I am going to say, OK, we are going to go back to plan A.

That is very helpful, thank you. I think, Ms. Williams-Bridgers, if we could come to you, if you would give me your suggestions. You are not accompanied at the desk by anyone formally introduced. So you get to jump right in. What would they be?

Ms. WILLIAMS-BRIDGERS. I would have two. One is security. Security of the U.S. Government's——

Mr. SHAYS. I am sorry, I meant VA. I apologize. We are going to start with you, Mr. Sullivan.

Mr. SULLIVAN. Thank you. With Steve here, as often comes about in these situations, Mr. Backhus over at GAO, we are very consistent in our view of the VA.

Mr. SHAYS. I like consistency.

Mr. SULLIVAN. VA, just in their purpose for being part of the Government, is to serve the veteran. Service is their No. 1 priority. And he picked the absolute two things that the VA is here for.

Mr. SHAYS. Would you just pick your two issues, though?

Mr. SULLIVAN. The two issues are, one, to provide good quality health care to the veterans, first the disabled vets and then the other veterans who may not be disabled on a space available basis. Steve is right on target, it is the structure of those facilities, the movement from inpatient to outpatient needs to be looked at, and how VA can move construction money and any of their operating moneys to do so, to allow these large, vacant structures that have been built over the years to be converted to outpatient clinics. And then the further establishment of these CBOCs, these community based outpatient clinics.

The second issue, of course, is the benefit aspects. The VA provides compensation, pension and education benefits to all veterans. Our concern over the years has been the timeliness in which claims are processed, as well as when one does try to speed up those claims, what are the vulnerabilities to fraud and misuse of that money if you go too far in those system changes, by eliminating some of the controls established, did we look at that.

So the two areas are very consistent with Mr. Backhus.

Mr. SHAYS. I know we are talking about third rail issues in some cases, but what we are dealing with is honesty before the committee. We may decide that there are only so many real heavy lifting issues. But it is really important to establish what you think are the crucial issues. It is really very interesting. I am fascinated with this.

Mr. Griffin.

Mr. GRIFFIN. The No. 1 issue in the eyes of my senior management team, which came out of a retreat that we had, is quality of care in the VA. Notwithstanding the fact that Mr. Backhus put that on the table, that is our No. 1 priority. That is why we created this new combined assessment program, to get out to VA facilities, to satisfy ourselves that the right quality controls are in place, that the right level of service exists, waiting times are not excessive, that the right medical professionals are in place at that facility.

All of these things are issues that when Dr. Kaiser came into VA and started this movement, which parallels the movement in the private sector of moving from inpatient care to primary care, that creates a whole host of issues. Previously maybe your staff is loaded up with specialists as opposed to physicians that are primary care physicians.

In addition to caring for patients, VA has a number of veterans under their stewardship in nursing homes. There are a lot of post-traumatic stress syndrome vets who are in long term care facilities. What they are trying to do to address that is, if we have excess capacity, which clearly exists in some of the 173 originally constructed hospitals, they are trying to convert some of that capacity into long term care facilities. That requires budget money.

In the past 3 or 4 years, they have opened over 500 outpatient clinics. That requires budget money also. So it is a balancing act as to, where you cut your losses on that excess space? Is it most prudent from a business standpoint to convert that space for long term care, or do you pour the money into the outpatient clinics?

Their perspective has been that health care is not about buildings, it is about access to medical professionals, which is why they have moved in the direction of outpatient clinics. But it takes a long time to turn that aircraft carrier around, to get things up and running in an efficient——

Mr. SHAYS. And your second issue?

Mr. GRIFFIN. The second issue is a combination of things. The Department got a qualified opinion this year on their financial statements. I think stewardship over this $43 billion or $44 billion in a broad is the issue. If you do not have systems in place to address some of these items that I raised in my opening remarks, like workers compensation, incarcerated veterans, where you cannot show where those tax dollars that you were given are being spent, then that is a major problem. I think that is an umbrella issue which speaks to a lot of the shortcomings that are outlined in the financial statement audit.

Mr. SHAYS. I am happy to jump back to my cause, but I would like to finish, we've done State. Mr. Hinton, we left you out a little bit on State. We've done VA. I am sorry. Now what I would like to do is State. Mr. Nelson.

Mr. NELSON. With respect to the State Department, I think there will not be much disagreement that the primary challenge to the Department is enhancing security over U.S. buildings and staff overseas. The caution, however, is that as the Department receives funds to deal with this issue that oversight must be vigilant. It is important to have a clear game plan for how those funds will be spent.

In the past, programs have been affected by lack of agreement on design, construction problems, locations that changed from time to time, resulting in increased costs. I believe for the last major building program in the mid 1980's, very few of the projects actually came in on time and at cost. So I believe that is a critical area for the committee to focus on, as it is very important to have a strong, capable overseas presence to carry out our foreign policy objectives, but to have those people be as safe and secure as possible. I think that would rate No. 1.

I will be surprised if my colleagues here were to disagree on that. That is a possibility, but I will be surprised.

The second area is the area of strategic planning and performance. I think the Department will not be able to address some of the sub-issues or challenges absent some greater statement of what the critical missions are and how the funds will be applied to these missions are adequately funded, and there is a clear sense of where the Department is trying to go. Their performance plans have been good in some respects, but they have not been clear on performance goals or on performance measures.

Now, I know we are limited to two. But I think in order for the Department to address the second one, it has to deal with two other items that are included in the statement.

Mr. SHAYS. A and B?

Mr. NELSON. Yes, A and B. You need better information in order to make decisions about what it is you are going to do or not do, because you need to understand what things really cost. In the past, the Department has not had a good handle on what things cost. We have had some difficulty when trying to make recommendations for the adoption of best practices, because of limited, very limited financial information.

The other challenge facing the Department is the consolidation of the Arms Control and Disarmament Agency and the USIA.

Mr. SHAYS. That is really three. In other words, the strategic planning and performance, what's its critical mission. One way they have to deal with is better information. Do you have anything else related to that, No. 2?

Mr. NELSON. Do you mean an example?

Mr. SHAYS. No. In other words, is there any other part to that? You said, you had two things. So this really is a third issue you want us to look at it?

Mr. NELSON. Yes, it is a third issue. And maybe I misspoke when I said A and B. But you cannot accomplish either goal without good financial information. With respect to the consolidation, you need good information to make good decisions about what functions and roles and missions you have to pursue.

Mr. SHAYS. Right, I've got you.

Mr. NELSON. So they are all tied together.

Mr. SHAYS. Ms. Williams-Bridgers.

Ms. WILLIAMS-BRIDGERS. I certainly agree with Ben Nelson on his assessment of security being the No. 1 area of focus, and the need of congressional oversight and attention, for a couple of additional reasons, though. One is State Department, while it serves as the platform for all U.S. Government entities overseas, it represents only 25 percent of our presence overseas. State Department, USIA and ACDA, sum total of those organizations is about 20,000 people, Americans.

Then we have, triple that number and you get the total U.S. Government effort, if you will, if you include FSNs, for whom we have some liability.

Mr. SHAYS. What are FSNs?

Ms. WILLIAMS-BRIDGERS. Foreign service national employees.

In Africa, we absorb the cost not only of the loss of life of Americans, but the loss of life of foreign service nationals as well. There was a financial liability associated with our employees there. And the foreign service nationals represent the largest part of our work force overseas.

I think also that the reason it is important for this committee to pay attention to security is that the Department cannot attend to security alone. It needs the help of the Congress. We talked about the costs of providing security facilities and secure networks for our information overseas. We are going to need the help of Congress, the commitment of resources, over a sustained period of time, in order to fully address those security needs.

While I agree with Mr. Nelson that strategic planning is extremely important, and the lack of good information, financial systems, information systems, have been an impediment to good resource planning and goals, setting of goals, I think the more immediate problem is the failure of those information systems and financial systems to provide you the information after January 1, 2000. So in terms of a short term goal, I would say the Y2K problem is something that warrants this committee's attention. Not only because of Department of State's precarious position, although I think they are making progress. But Department of State is taking a lead in many ways in the rest of the world's attention to Y2K. From work that we have done with host country governments, we know that there are varying levels of attention being paid to the Y2K problem.

For the tens of millions of Americans that are traveling overseas, in Rome alone they are celebrating a jubilee, January 1, 2000 millions of Americans are expected to attend this jubilee. There is a lot of question of whether or not that country will be prepared on January 1. So I think the Y2K is more of a short term need that warrants this committee's attention.

Mr. SHAYS. Thank you very much.

We have a vote, and I think what we will do is end with Defense. Ms. Jacobson, you are in one area of the Defense area, but I still want you to give me your two, even if one goes beyond your area. And Mr. Hinton, I will ask you to comment on Defense.

Then we will ask the Inspector Generals, then come to you, Mr. Lieberman. I think that is what we will do—do we only have one vote? Sometimes we leave and we find out there is another vote,

and that we should keep going. Why don't we start with you, Ms. Jacobson, and we will make sure there is only one vote.

Ms. JACOBSON. Mine is financial management and you are all pretty aware of the issues in financial management at DOD. They are not denying them. There are serious difficulties, both in the stewardship of the assets, and in cost, and accumulating cost information and data.

Mr. SHAYS. When you all told me that in 1 year alone, vendors returned $1 billion of overpayment, I was shocked. And you all had probably quite frankly become desensitized to it. That is not a criticism. It just tells me the challenge. For me, I thought, wow. At one time, you all probably did, too.

Ms. WILLIAMS-BRIDGERS. When I first started, I did, too. When you first come out of the private sector, and $1 million is a big number, $1 billion kind of shocks you.

Mr. SHAYS. How much more is out there? All we need to do is find out if we have more than one vote. OK.

Ms. WILLIAMS-BRIDGERS. I think one of the most serious issues facing us, and challenges for GAO right now, in working with the Department to try to help them address their financial management problems, is getting them to view financial management in the broadest perspective.

We just issued a report on their biennial financial management plan. In that report, they eliminate from the discussion of financial management the budget side of the equation. That is a basic element of financial management. Until you look at financial management in a broad perspective, including how information is shared not only upwards to the financial systems, but also between financial program systems that need that information to control the assets and provide stewardship over the assets, and you do not have an adequate plan going forward to address the serious problems that we've seen with financial management.

Mr. SHAYS. We are going to go vote. The bottom line I am hearing you say is, we have to connect the budget to financial management, that is one issue we need to look at. Give me another one as well.

Ms. WILLIAMS-BRIDGERS. Connecting, providing the control element of the functional areas, feeding information to each other at the same time as the financial management systems as well. For example, when you acquire something, acquisition, provide that information to logistics, it is coming in, at the same time they provided it to accounting, pay for it. Then at the end of the day, accounting and logistics look and see if we got everything that we paid for. That is a basic element of the financial management control system that is totally lacking in DOD, and not planned for right now as far as we can tell.

Mr. SHAYS. Thank you very much.

We have been joined by Judy Biggert, and I do not know if Judy is going to be able to come back afterward. I want to welcome you to the committee. The purpose today is just to get a sense of where we are going to begin our travels here. Welcome.

Ms. BIGGERT. Thank you. Unfortunately, I will not be able to come back. But I have just been traveling in six countries in South America, Latin America. I have visited so many of the embassies

there, and the problems they are having, particularly those that are street levels, four sides exposed, and how concerned they are about the security there.

[Recess.]

Mr. SHAYS. Are we all done? You have given me your two points, and I will go to Mr. Hinton. We are taking Defense, first focus on Defense. I did not want you to use up all your good ideas on the other two.

Mr. HINTON. That is OK. My jurisdiction runs both to the international side, too. I will echo where they have been on that. I want to spend my time right now on Defense.

When I got your invitation to testify, I was really thinking how I would spread together all three departments in my statement. I want to come back to one of my key points right at the beginning, because I think it rises to Defense in a very important way. In the last page of my prepared statement, you will see a list of high risk areas which are about six or seven that we have had in DOD for many years.

Ms. Hill touched on those as she went through. Our work parallels each other. I think the issue I would have, Mr. Chairman, is GPRA implementation, to try to push the Department around to try and identify measures, goals, that will move forward trying to get some metrics out there that we can see progress going against these high risk areas.

Those high risk areas form the basis of the challenges that we have laid out in our reports here. I think that is very key, and as more knowledge becomes available, and the Department is starting to embrace that legislation more, I think you will see more measures, more metrics, and you will be in a position to look at the progress.

The other important part that comes on is that at some point, we tie the budget to some of these areas, so that we can see where the dollars are going and what we are getting for the execution and expenditure of those dollars against those goals and objectives. I think your committee is in a very good position to kind of watch that evolution of that and challenge the Department, are we getting where we want to go against these high risk areas?

I always think about these, I think that $1 that is not well spent in these areas is $1 less that we have to devote to readiness and modernization and those types of priority needs that the Department has been seeking additional moneys for.

My second one in DOD truly goes to the issue of financial management. The issues that Ms. Hill and I both talked about and Ms. Jacobson raised here really has at its heart the execution of the budget. Unless you have real good information, decisionmakers are not in a very good position to make informed judgments. That ties to the data itself and the systems we have in DOD. We are not in good shape. I would put that right there second to the first one that I mentioned.

Mr. SHAYS. Thank you very much.

Mr. Lieberman.

Mr. LIEBERMAN. I have a list of stuff written down on this paper, and I have been trying to find some innovative way to squeeze it all into two things.

Mr. SHAYS. I am all up for creativity.

Mr. LIEBERMAN. I think the No. 1 priority for the Department is military readiness. I believe that we cannot do too much oversight in terms of looking for readiness inhibitors. I think there are plenty of them out there.

Mr. SHAYS. I like the way you say that, readiness inhibitors.

Mr. LIEBERMAN. Questions arise such as, we spend $83 billion a year, approximately, on logistics. Yet we have the operating forces complaining, vehemently nowadays, about spare part shortages. How can this be? Are we really ready to deal with weapons of mass destruction, either in a war environment or in terms of counteracting terrorism, abroad or at home? There are others; it is certainly a long list. But I think, as a genre, that readiness is terribly important.

Mr. SHAYS. In regard to readiness, a good chunk was dealt with in your statement, Ms. Hill. You say accurate reporting of unit level readiness status remains a concern. In addition, audits have indicated weakness related to chemical and biological defense preparedness and communications capability. So did you inject that into her report?

Mr. LIEBERMAN. Yes. [Laughter.]

Mr. SHAYS. It caught my attention.

Mr. LIEBERMAN. I trust it is OK to let the secret out here.

Mr. SHAYS. When you say communications capability, can you elaborate a little more on that, Ms. Hill?

Ms. HILL. I think the one on communication, both of those are very critical areas. I was going to say that——

Mr. SHAYS. I am going to come back to you, Mr. Lieberman.

Ms. HILL. My first problem would also be readiness. My biggest concern is particularly in the chemical and biological area, where we have done a series of reports, some of which are classified. We cannot go into all the details here, but it is an area that I think is worth looking at.

Mr. SHAYS. Not all of the 12 are in regard to chemical and biological?

Ms. HILL. No.

Mr. SHAYS. The 12 are readiness overall?

Ms. HILL. The communications one, I believe, is the audit report on the frequency issue overseas, where we are using communications equipment where, and I am not a technical expert, and Bob can correct me if I am wrong, they are not using approved frequencies and not complying with all the requirements of the host nation. Therefore, the efficiency of the whole program or of the equipment is seriously in doubt.

Mr. SHAYS. Let me have you give me your second one, or if you wanted to elaborate more. I interrupted you.

Mr. LIEBERMAN. I think the second one relates to acquisition. Acquisition is the area of the Department where there is the most money. Last September, the Under Secretary of Defense for Acquisition and Technology made a statement, a public statement, in which he said the entire modernization program was in a death spiral due to underfunding. We are spending approximately $60 billion a year on weapons acquisition. So again, the question is, how can that be?

There are a lot of different facets to that. It leads you into the question of where do we go with acquisition reform. How have the reforms so far worked, and what kinds of further changes, if any, are necessary?

If I could impose and have a third?

Mr. SHAYS. Sure. For Defense, I think a third would be appropriate.

Mr. LIEBERMAN. Thank you. Information systems are really at the heart of everything that the Department does. All of our processes are completely automated. All of us, as managers, are dependent on information coming out of automated systems. There is a chronic lack of accurate day to day management information, as has been mentioned earlier. I think that pervades every single part of the Department's operation.

It leads you into areas like Y2K and security, as well as systems design. So how we can have 20 some thousand information systems and still have bad information, is my third question.

Mr. SHAYS. Does Mr. Horn tend to get into those issues as well into his committee, Ms. Jacobson? One of the things we have to decide is what we do in that regard.

Mr. HINTON. He is real key into the Y2K right now, but also in the broader picture around some of the information technology and systems development side.

Mr. SHAYS. Is it fair to say that GAO would tend to focus more on management because you tend to get into less—let me preface it by, I would think the Inspector Generals on occasion are going to get into some very specific programs, sometimes fairly narrow in focus, more micro. You can also get into macro issues as well. But it would seem to me that GAO would tend to get into more macro issues.

Mr. HINTON. Both. But largely on the macros. If we are going to have, if you could give Bob a third one, I would like to come back after Ms. Hill, because I have a couple at a broader national security level that go beyond Defense.

Mr. SHAYS. Great. I am going to ask Ms. Hill to give me her first two, then I am going to ask each of you to tell me the question you wish we had gotten into, the issue we wished, and each of you comment. And then I am going to let you get on your way, because this is just kind of a general introduction for me and the committee.

Ms. HILL. I preface it by saying that the problem with Defense, obviously, is there are so many important issues. Not only are there so many, but they are so interrelated. If you pick one issue, some other issue feeds right into it.

Mr. SHAYS. Fair enough.

Ms. HILL. But great minds must think alike, because Bob's list and mine are very similar here. My first would also be readiness, and particularly from what I have seen in our audits, it would be in the biological and chemical weapons area. Obviously, I would put readiness first, because to me, that involves the safety of our men and women in uniform. Although everything else, including financial management, is very important; readiness is a critical area with obviously a huge potential for disaster if it is not the way it should be.

Second, I would suggest the general area of acquisition procurement, because the amount of dollars that is at risk in that area is huge given the extent of the Department's activity. There is also a lot of reform going on in acquisition in the Department, some of which is very good and some of which we have supported, not only in the Department, but in the Congress, in the last few years.

There are some concerns that we have in that area. As the reform moves forward, there is a tendency to move more and more toward commercial practices. My own concern is that we are talking about the largest acquisition system in the world here, where a huge amount of taxpayers' dollars are at stake. We need to make very sure of what we are doing, before we implement commercial processes.

Not only understand what the practice is, but also that it makes sense in the Department of Defense, and that we do not just automatically implement something because its "commercial" before we have the evidence to support doing so.

Second, there is a lot of concern about going so "commercial" that we eliminate any of the traditional safeguards that we have had in the acquisition area, such as the False Claims Act, the Truth in Negotiations Act, cost accounting standards, and other internal controls. I am not saying those are sacrosanct, because certainly you can change things and moderate them where reasonable.

But I do not think we should throw everything out without looking at the risks there and making sure that whatever it is we put in place in the new system, it is done carefully and with evidence that it is going to work. So that would be my second area, and that of course feeds into every part of the Department in terms of acquisition and systems.

If I had a third, it would also be in the information area, but it would probably be more focused on information security. Everything we have seen and all the data and estimates suggest that there is a huge vulnerability in the Department as to the security of its information systems. Given the way the country and the world are going in the way of computers and information systems, I do not see that problem shrinking. I see that threat getting bigger.

The Department needs to be prepared to handle it again, because the potential for disaster there, if the worst happened, would be a terrible thing for the country and for the Department. That would be my third area, if I had a third area.

Mr. SHAYS. Mr. Hinton, I am going to ask you and I will ask John Tierney if he has any other questions before I go to that last quick question.

Mr. HINTON. I too would associate myself with the issues Mr. Lieberman and Ms. Hill had just brought up on readiness and the other. Our body of work is the same as theirs in terms of coordination.

There are a couple others I would like to bring up for you, Mr. Chairman, and one is broader than Defense. It is combating terrorism. It cuts across Government, it is a large effort. We have been heavily involved, largely with this committee, looking at that and identifying who the players were and combating the issue and working the issue, what the funding trail has been and trying to

assess the level of coordination amongst the Government team to combat terrorism and the effectiveness of our efforts as a Government to deal with the issues. That is one.

The second is, I think, the issue of human capital. As we look across all the issues, there are a lot of people working the issues within the agencies. Whether or not we have the right number, the right training, the right skills, good strategies as a Government to deal with these many important issues that you are hearing, I think, in itself, is a very key issue that we cannot lose sight of.

It is where we are today, because the public servants who work these issues, and I think we have to look at it from one, making sure we have a pipeline of people who are coming behind the ones who are working them now that have the skills and the tools as well as the focus for a lot of that. So I would add those two to the list we've already discussed.

Mr. SHAYS. Thank you very much.

Mr. Tierney.

Mr. TIERNEY. I only had one question, and I hope I am not repeating. Ms. Hill, I missed your first one.

Ms. HILL. It was readiness, particularly in the chemical and biological area.

Mr. TIERNEY. Do we have a real definition that is common right across the board of what people are talking about in each of the branches when they talk about readiness, or might they all be talking about different things and measuring it in different ways?

Ms. HILL. I do not know if there is an official definition. To me it is a common sense thing, and obviously——

Mr. TIERNEY. You would think so, except sometimes in listening to the different services, I wonder if we all have the same common sense. [Laughter.]

Ms. HILL. Certainly there is some standardization, since they look at readiness in terms of what they would be prepared to confront in a warfare situation. In that sense, I think they are pretty much on the same wave length. But I do not know if we could guarantee it is identical.

Bob, would you care to add to that?

Mr. LIEBERMAN. I think there is a tendency to miscategorize a lot of things as either related to readiness or not related to readiness. Many times that gets inconsistent.

Frankly, it is a real plus for someone's budget request to be able to say, we need this for readiness purposes. So it is more a case of everyone trying to jump on that bandwagon, rather than saying what they do is not related to readiness. I think we have had problems in ascertaining the ability of individual units to perform various kinds of missions.

That is not so much a definitional thing, as it is making it clear to people exactly what they are reporting and then being assured that what they are reporting is really accurate. There is still a lot of subjectivity in the process, which makes it difficult to accurately measure force capability.

Mr. SHAYS. Let me do this. If I could, we will end with this, and then I will just have a closing comment. Is there anything you wish we had asked you to talk about? Obviously there may have been a few, but any one particular thing you feel you would have liked

to have addressed? I am not looking for a long comment, but an explanation.

Mr. SULLIVAN. I have just one thing. Knowing the overall responsibility the subcommittee has over all three of these activities, I could see further discussions of why VA and DOD cannot work closer together. The portability of a veteran leaving the health care system of Defense and moving into the VA system, the use of common records as a serviceman leaves his service and moves into the VA, that sort of thing.

Mr. SHAYS. Great. Thank you.

Mr. GRIFFIN. I would say that in the area of workers compensation, which I identified as $140 million a year budget item for VA, and a $1.8 billion item Governmentwide.

Mr. SHAYS. Let me be clear. Why is that so large?

Mr. GRIFFIN. There are over 200,000 employees in the Department. Once someone gets placed on workers compensation——

Mr. SHAYS. These are the employees? What is the number again?

Mr. GRIFFIN. The dollar value for the chargeback, year of 1996, because you pay it in arrears, was $140 million, roughly. Governmentwide, it is $1.8 billion.

Those of us who are involved in investigating these things are handcuffed somewhat by some of the existing rules. One of those rules makes it very difficult to get access to income data. Part of the deal, when you go on workers compensation, is you sign a claim form wherein you say that you are unable to work or you are only able to work and earn a certain amount of income. There is not an easy way right now to do a data match with IRS records or Social Security records in order to determine whether or not an employee who is on workers compensation is in fact getting additional income on the side. This is something that we are going to be working through the system and seeking proposed legislation to fix.

Mr. SHAYS. I think we will also be encouraging the Civil Service Subcommittee to take a look at that in Government Reform. It is truly a very important issue. I got involved in the State. It is a big problem sometimes.

Ms. WILLIAMS-BRIDGERS. One area I think that was touched on briefly but I think warrants more attention is our overseas presence, the size of the U.S. Government's presence overseas. Our overseas presence has grown tremendously over the past several years, and it has come at tremendous cost. Security increases, and our vulnerability increases, with each American that establishes a presence overseas. I think there needs to be some general oversight over the reasons for increasing the numbers of Americans overseas, and whether we are in the right places for the right reason.

Mr. SHAYS. What I am surprised about is the number of what I call nontraditional State Department employees, like Commerce, Agriculture and so on. But you are talking about private citizens just being there?

Ms. WILLIAMS-BRIDGERS. No, I am talking about official U.S. Government presence.

Mr. SHAYS. OK, just like what I was mentioning?

Ms. WILLIAMS-BRIDGERS. Yes, Commerce, State, Justice, Transportation, Agriculture. The list goes on, 34 different U.S. Federal agencies.

Mr. SHAYS. I would like to say to the committee that I do believe that is something that would be logical for us to look at, and not all that difficult. How could we do it with our limited resources? That is something I think we can look at fairly easily. It is a fascinating issue.

Mr. LIEBERMAN. We mentioned human resources, and specifically, training people in financial management oriented jobs. I would agree wholeheartedly that that is an important thing to do. But I think the training in the acquisition area is even more critical. Also, the difficulty the Government has in retaining highly skilled information technology experts is a major problem that cuts across the whole Government.

So training tends to get short shrift. It sounds boring, but it really is critical, also.

Mr. SHAYS. Thank you.

Ms. HILL. The only one that I would mention fits into part of the acquisition process, namely the requirements process, the method by which the services, the components, whoever, set forth what their requirements are. The issue is the basis on what they're basing those requirements on, whether or not they are valid, whether the method they used to arrive at those requirements was a legitimate method, and how convincing the ultimate requirement is if you look at what is backing it up. We have certainly seen some problems in that area. And that is an important area, because it feeds right into the spending of dollars in the acquisition area.

Mr. HINTON. Two things, Mr. Chairman. One would be theft of inventory due to weak controls. I think it is probably broader than DOD, but particularly in DOD.

Mr. SHAYS. Do we see it in VA? Do we see it in State as much?

Ms. WILLIAMS-BRIDGERS. No. State Department, our largest assets are our real property. If you can walk off with the embassy—[laughter]——

Mr. HINTON. The second issue I would put is the incentives to effect change in behavior to address the many issues that are on the table here, particularly as they relate to the high risk programs in DOD.

Mr. SHAYS. Which programs?

Mr. HINTON. The high risk programs that are in DOD that we have identified cut across acquisition and information management and those things. I think also as it relates to the challenges that cuts across all the issues. There have to be incentives to motivate and to do things differently. You cannot operate the same way in the future that we have in the past.

Ms. JACOBSON. I guess I would just answer a question you asked earlier about other subcommittees' interests. You asked if Congressman Horn gets involved in financial management. He certainly does, and in the security area as well.

Financial management in DOD is a very broad issue. It does cut across national security and other areas of readiness and those kinds of issues as well. No one committee can cover all of those issues. I would be glad to work with you and your staff on identifying the specific aspects of financial management that might be of interest to the committee.

Mr. SHAYS. Something that we could get a handle on. I do not know if I would be chairman of the committee. One, be back here; two, be the chairman—would Republicans be in the majority or Democrats? But I kind of think we almost have to have a 4-year plan, and that is something I would talk to Rod about, so whoever is there, we could continue. There is just a lot to deal with.

Mr. BACKHUS. This next decade, the VA is going to be faced with the largest number of deaths of veterans it has ever had to confront. The peak years I think are projected to be 2007 and 2008, World War II veterans and Vietnam veterans, and Korean War veterans.

The question is, will they have the capacity through the National Cemetery Administration to meet that demand. There are efforts underway to try to involve States in contributing to constructing and maintaining cemeteries to meet this demand. But it is uncertain at this time whether they will be able to.

One last comment if I could make it, in terms of, if there was another question that you had asked. I have taken a quick look at the fiscal year 2000 performance plan for VA. I have seen where they are making a substantial amount of progress in terms of being responsive to the criticisms we have made in the past.

While we are not through reviewing it, we will be concentrating on it the next month, it appears that VA is really doing a lot more in the way of trying to identify more results-oriented measures to which to track their progress, and engaging folks like the IG's office in trying to improve the data reliability upon which they are going to report. If they can do those two things, then I think next year at this time, we might have a better report to give.

Mr. SHAYS. Mr. Tierney, do you have anything else?

Mr. TIERNEY. Nothing else, thank you, except to thank everybody very much.

Mr. SHAYS. We are going to close, and I will make a few observations. One, I truly found this very interesting. My motivation was primarily to get you here to make sure we develop a nice relationship. We have met privately, and one thing I would like to say on the record is, all of you do very important reports. We want to make sure that they do not just lie on the shelf and not get noticed.

You triggered, as you did in the beginning, Mr. Backhus, some ideas that I want to just comment on. One of them is for instance, for you to look at this issue of what will be there for our veterans and their families, primarily, obviously, in terms of cemetery space. That seems to be kind of this all encompassing forever kind of study. I think we could get a pretty good handle on it and make some suggestions and write a report that hopefully could be helpful to other committees, and then pursue it in legislation.

That can be done with not as much of our time, maybe some of yours. Then we could highlight it and make sure the public knew, and make sure our colleagues knew and move forward. Obviously, the one that becomes the most daunting would be this whole financial management.

I would ask, Ms. Jacobson, that maybe you can just get out some niches of that. I do know that we are going to focus in on terrorism in a big way and use more than one of our personnel for that from

our staff. That really cuts across two in particular, and to some measure the health care system of VA and DOD.

We are going to look at how we coordinate DOD and VA health care. It is a natural for us, because we have 4 years of experience in health care, so we come with a knowledge base. We are going to obviously look at the public safety issue of embassies—and that does get involved with the whole issue of terrorism.

All the suggestions that were made I think have tremendous merit. Some of them we will not look at, simply, we will not have the resources. I will conclude by saying that this truly is a partnership. Some of you all may be doing more of the work, we may do some really concentrated effort, we will pool our resources, and we will make sure the public knows about it and our colleagues know about it, and that we make some intelligent recommendations.

This has been helpful, very helpful. Thank you, and we will cause the hearing to adjourn, and we thank our recorder.

[Whereupon, at 12:19 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

○