VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Veterans Health Administration

Review of
Fraud Management for the
Non-VA Fee Care Program

June 08, 2010
10-00004-166

ACRONYMS AND ABBREVIATIONS

CBO	Chief Business Office
CMS	Centers for Medicare and Medicaid Services
FBCS	Fee Basis Claims System
TMA	TRICARE Management Activity
VAMC	VA Medical Center
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network

Report Highlights: Review of Fraud Management for the Non-VA Fee Care Program

Why We Did This Review

The Veterans Health Administration's (VHA's) Non-VA Fee Care Program pays non-VA medical providers to treat eligible veterans when medical services are not available at VA facilities or in emergencies when delays are hazardous to life or health. Annual fee care payments in this program have grown from about $1.6 billion in FY 2005 to about $3.8 billion in FY 2009. This review continues our assessment of non-VA fee care by evaluating the effectiveness of Fee Program fraud management.

The VA Office of Inspector General's *Audit of Veterans Health Administration's Non-VA Outpatient Fee Care Program* (Report 08-02901-185, August 3, 2009) concluded that VHA had overpaid outpatient fee claims in FY 2008 by $225 million.

What We Found

Federal law requires agencies to maintain controls that safeguard their assets against fraud; however VHA has not established controls designed to prevent and detect fraud for its Fee Program. VHA had not established fraud management controls primarily because it had not identified fraud as a significant risk to the Fee Program. Yet VHA's Fee Program is not significantly different from other health care programs that have identified numerous cases of fraud. More important, VHA lacks a system for determining the risk of Fee Program fraud. Yet, health care industry experts have estimated that 3 to 10 percent of all health care claims involve fraud and the Fee Program faces risks similar to other health care payment programs. In effect, the VHA Fee Program could be paying between $114 million and $380 million annually for fraudulent claims.

What We Recommended

We recommended that the Under Secretary for Health establish a fraud management program that includes such fraud controls as data analysis and high-risk payment reviews, system software edits, employee fraud training, and fraud awareness and reporting.

Agency Comments

The Under Secretary for Health agreed with our finding and recommendation and plans to complete all corrective actions by October 30, 2010. We consider these planned corrective actions acceptable and will follow up on their implementation.

(original signed by Linda A. Halliday, Deputy Assistant Inspector General for Audits and Evaluations for:)

BELINDA J. FINN
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Review Objective

This review evaluated the effectiveness of VHA's fraud management for the Non-VA Fee Care Program. We examined fee payment processes and controls, identified common fraud management practices of other health care organizations, and assessed Fee Program fraud management controls. We reviewed Fee Program fraud management at the national program office, consolidated Veterans Integrated Service Network (VISN) fee offices, and at VA Medical Centers (VAMCs).

Fee Program Overview

VHA's Fee Program pays non-VA medical providers to treat eligible veterans when medical services are not available at VA facilities or in emergencies when delays are hazardous to life or health. The Fee Program administers the delivery of inpatient, outpatient, prescription, and long-term care services.

The Fee Program has experienced rapid growth in the past four years. Annual fee payments have grown from about $1.6 billion in FY 2005 to about $3.8 billion in FY 2009. These services included inpatient care ($1.7 billion) and outpatient care ($2.1 billion). Furthermore, in FY 2009, VHA fee offices processed about five million fee claims.

Fee Program Responsibilities

VHA's Chief Business Office (CBO) oversees the Fee Program. The CBO's National Fee Program Office provides Fee Program policy, training, and program support to VISN and VAMC fee offices.

Four VISNs have established consolidated fee offices that process the fee claims for all VAMCs in their respective VISNs. However, most VAMCs administer the fee care programs for their areas. Each VISN or VAMC determines the organization, staffing, and management controls for its fee office.

Results of Previous Audits

The VA Office of Inspector General's *Audit of Veterans Health Administration's Non-VA Outpatient Fee Care Program* concluded that VHA needed to strengthen controls over outpatient fee care payments and that fee offices improperly paid 37 percent of their outpatient fee claims. The audit estimated that VHA overpaid $225 million for outpatient fee claims in FY 2008. The identification of such significant improper payments supports that controls are not in place to protect VHA against fraud and waste.

The Office of Inspector General's *Review of Outpatient Fee Payments at the VA Pacific Islands Health Care System* (Report Number 09-03055-103, March 16, 2010) determined that the VAMC had made duplicate payments for 13 percent of its outpatient fee claims at a cost of $49,571.

RESULTS AND RECOMMENDATIONS

Finding VHA Needs a Fee Care Fraud Management Program

Federal law requires agencies to maintain controls that safeguard their assets against fraud. However, VHA has not established controls designed to prevent and detect fraud for its Fee Program. VHA did not establish fraud management controls primarily because it had not identified fraud as a significant risk to the Fee Program. Further, VHA lacks a system for determining the risk of Fee Program fraud. Health care industry experts have estimated that 3 to 10 percent of all health care claims involve fraud and VHA's Fee Program faces risks similar to those of other health care payment programs. In effect, the Fee Program could be paying between $114 million and $380 million annually for fraudulent claims. Annual multi-million dollar fraud recoveries by other Federal health care agencies demonstrate the effectiveness of fraud management programs in controlling fraud.

Federal Mandate To Control Fraud

The Federal Managers' Financial Integrity Act of 1982 requires agency heads to establish controls that provide reasonable assurance that assets are safeguarded against fraud, waste, and abuse.

Risk of Fraud to the Fee Program

VHA lacks a system of assessing the risk of Fee Program fraud. Yet, we consider the potential risk of fraud to be significant, since: (1) health care experts have determined that substantial fraud exists throughout the health care industry, (2) the VHA Fee Program is not significantly different from other health care programs that have identified numerous cases of fraud, and (3) Fee Program payment controls do not provide adequate protection against fraudulent claims.

In March 2008, the National Healthcare Anti-Fraud Association estimated that fraud accounted for between 3 and 10 percent of all health care expenditures in the United States. If applied to the Fee Program, this estimate suggests that VHA could be paying between $114 million and $380 million for fraudulent claims, based on FY 2009 Fee Program expenditures of $3.8 billion.

We consider the potential risks of fraud to the Fee Program to be similar to those facing other health care payment agencies, such as the Centers for Medicare and Medicaid Services (CMS) and the Department of Defense TRICARE Management Activity (TMA). For example, one major risk to health care programs is provider fraud. According to the Health Insurance Association of America, provider fraud has accounted for approximately 80 percent of all health care fraud cases. We did not identify any material difference between the risk of an unscrupulous provider billing the Fee Program and the risk of the provider billing another agency, since the Fee

Program allows its beneficiaries to select any qualified provider to receive care. However, unlike the Fee Program, CMS and TMA have established controls specifically designed to prevent and detect provider fraud.

Weaknesses in fee payment processing controls also make the Fee Program susceptible to fraud in high-risk areas. The Federal Bureau of Investigation reported that some of the most prevalent fraud schemes involve duplicate charges and services billed but not rendered. In fact, recent OIG audits have found material weaknesses in Fee Program payment processes that allowed improper payments to be processed undetected in those areas.

Our tests of FY 2008 and FY 2009 fee payment data for potential fraud identified additional evidence that fee payment controls were not effective in preventing or detecting potential fraud. The following examples illustrate some of the internal control weaknesses that make VHA's Fee Program susceptible to fraud.

Duplicate Charges. A VAMC overpaid a physician $2,051 when a physician and the physician's practice group both charged VA for the same services. The overpayment occurred because claims processing controls did not ensure that duplicate charges would be identified. In addition, the VAMC did not have procedures for identifying possible fraud when it found duplicate payments.

Services Billed But Not Rendered. A VAMC paid a vendor to provide home health care services for a veteran. The vendor billed VA monthly, at a rate of $100 for each day it treated the veteran. In 2009, the vendor charged the VAMC $1,900 for home health care visits on dates as long as 6 weeks after the veteran had died. The fee office's claims processing system did not prevent payment of invoices submitted for deceased veterans, and the VAMC had no procedures for evaluating whether the claim was fraudulent.

Services Billed But Not Authorized. A VAMC made payments totaling $6,724 to a vendor for one veteran's therapy treatments that had no pre-authorization documentation on file. The fee office paid the invoices without verifying the need for the services or determining whether the charges were valid. We determined the charges were improper, since the vendor had also charged another VAMC for the same services. That VAMC had pre-authorized the services.

Management of Fraud in the Health Care Industry

Other government agencies and private organizations that process medical claims typically have fraud management programs to prevent and detect fraudulent payments. A 1999 Health Insurance Association of America

survey reported that over 90 percent of all health insurance companies surveyed had fraud management programs.

Both CMS and TMA established comprehensive fraud management controls to prevent and detect payment of fraudulent claims. Common fraud management controls implemented by CMS and TMA include:

- Ongoing data analysis and reviews of high-risk payments
- System software edit reviews
- Employee fraud training
- Establishing fraud awareness and reporting capabilities

Status of Fee Program Fraud Controls

VHA has not implemented fraud management controls for the Fee Program. Table 1 compares VHA's Fee Program controls with those of CMS and TMA. A discussion of each fraud management practice follows.

Table 1. Comparison of VHA Fraud Management Controls to Similar Health Care Programs

Fraud Control	Fee Program	CMS	TMA
Ongoing Data Analysis and Reviews of High-Risk Payments	No	Yes	Yes
System Software Edit Reviews	No	Yes	Yes
Employee Fraud Training	No	Yes	Yes
Fraud Awareness/Reporting	No	Yes	Yes

Ongoing Data Analysis and Reviews of High-Risk Payments

Although the CBO had begun data mining fee payment information to identify improper payments and sending listings of possible overpayments to VISN staff for review, it had not developed procedures for reviewing fee payments to detect possible fraud. In addition, officials from all 10 VISN and VAMC fee offices that we contacted reported they did not analyze fee payment data or review fee payments to detect possible fraud.

Although VHA's Financial Assistance Office and VA's Office of Business Oversight's Management Quality Assurance Service frequently reviewed samples of fee payments as part of their facility inspection programs, they selected fee payments for review randomly and did not perform fee reviews based on fraud risk assessments. Using such limited testing, neither of those offices reported identifying any cases of suspected fraud in the Fee Program.

In contrast, to detect fraud, CMS and TMA identify indicators of possible improper payments and then analyze data mining results to assess the risk of fraud on an on-going basis. Once fraud risks are assessed, they perform

reviews of payments in the high-risk areas identified to detect cases of suspected fraud.

For example, fraud examiners might review 20-40 claims per provider for provider-specific indications of fraud, such as spikes in billings for selected periods. These reviews can result in denial of payments, vendor suspensions, referrals to criminal investigation offices, improvements in fraud training and education, or recovery of payments.

System Software Edit Controls

Although some VHA fee offices now use claims processing software that automatically flags potential payment errors when processing fee claims, they have not used software edits to identify possible fraud.

VHA has been implementing the Fee Basis Claims System (FBCS), a commercial off-the-shelf program designed to be integrated into each fee office's payment system. FBCS has been programmed to automatically alert fee staff for specific types of billing errors during claims processing. When FBCS flags a possible error, fee the staff determines whether the payment should be paid, denied, or referred to staff with greater expertise for review.

Each fee office established its own referral criteria and procedures, and none of the VISN and VAMC fee offices contacted had established procedures for routinely identifying patterns in payment errors that indicate potential fraud. Of the 10 fee offices we contacted, officials from 5 reported that they currently use FBCS. All five fee offices confirmed that FBCS's integrated edits help reduce the number of payment errors, but none reported using FBCS edit information to detect potentially fraudulent claims.

In addition to having claims processing systems that automatically flag possible billing errors, CMS and TMA have processes that automatically refer certain high-risk claims, such as charges that exceed specified cost thresholds, to expert-level reviewers. Claims reviewers determine not only whether charges are valid, but also evaluate the reasons for overbillings and whether they are part of any fraud patterns. Further, if a provider's claim is flagged for a possible coding error that indicates fraud, the reviewer analyzes previous payments to determine if a pattern of coding-related overbilling exists. If the provider has a high incidence of overbilling, the claims reviewer can initiate a payment system edit requiring a review of all subsequent claims from the provider in order to both reduce the risk of overpayments and identify indications of intentional overbilling by the provider.

Employee Fraud Training

The CBO has not included fraud training as part of its current fee training program. The officials from all 10 VISN and VAMC fee offices we contacted also reported that their employees did not receive training on Fee Program fraud prevention and detection.

CMS and TMA have made fraud prevention and detection training an integral part of their fraud management programs. Fraud training includes providing mandatory training and disseminating fraud information within the organization using internal newsletters or websites. Such training familiarizes employees with fraud indicators and instructs them on how to report and document suspected cases of fraud.

Fraud Awareness and Reporting

The Fee Program did not routinely provide fraud awareness information to fee providers or beneficiaries and the CBO has not established fraud awareness and reporting requirements. In addition, none of the officials from the 10 VISN and VAMC fee offices we contacted reported providing fraud awareness information to fee providers or beneficiaries. Those officials also reported they did not track contacts with beneficiaries or reports of suspected fraud.

For example, the fee care authorization documents given to beneficiaries and non-VA providers did not contain fraud awareness information. Although beneficiaries' Explanations of Benefits statements instructed them to contact the VA facility whenever they have any questions or think there might be payment errors, these statements provided no information on reporting suspected fraud. Similarly, the CBO website did not provide fraud awareness information.

Providing fraud awareness information to both providers and beneficiaries is a valuable tool for preventing and detecting fraud. It reinforces proper billing practices, discourages fraud by raising awareness of fraud prevention and detection actions, and instructs them on how to report cases of suspected fraud.

Both CMS and TMA have fraud websites that provide information on fraudulent coding schemes, suspicious provider actions, and instructions on reporting fraud. CMS's Explanations of Benefits also provide fraud hotline numbers and instructions to beneficiaries on reporting suspected cases of fraud.

Publicizing annual fraud prevention and detection reports is another tool both organizations use to deter fraud. TMA displays its annual Program Integrity Operational Report on its Fraud and Abuse website. This report shows the results of its annual anti-fraud program activities, such as the number of fraud referrals, the number of providers that have been sanctioned, and the dollars recovered as a result of TMA's anti-fraud actions.

Why VHA Has Not Implemented Fraud Controls

VHA did not assess the risk of fraud for the Fee Program. Because VHA officials did not perceive fraud to be a high risk, VHA did not establish fraud management requirements. Another reason is that Fee Program managers have faced other major challenges and have had limited staff to manage the

program. Recent CBO Fee Program initiatives have included implementing a more effective automated fee payment processing system, coordinating various fee inspection programs, and standardizing fee training. Similarly, VISN and VAMC fee offices have focused their efforts on improving timeliness and accuracy of fee payments, not on preventing and detecting fraud. Of the 10 VISN and VAMC fee offices we contacted, none had established requirements for preventing or detecting fraud.

Benefits of Fraud Management Programs

We could not estimate the potential cost benefits of a fee care fraud management program. However, agencies with missions similar to the Fee Program produce significant results through their fraud management programs. In fact, both CMS and TMA have identified large cost savings resulting from their fraud management programs. CMS reported recovering $1.9 billion in fraudulent Medicare payments in FY 2008. Similarly, TMA reported receiving fraud-related judgments of $123 million in calendar year 2008.

Conclusion

Health care fraud continues to be a serious problem for the American health care system, and health care experts frequently identify fraud as a major reason for the increased cost of health care in the United States. Annual multi-million dollar fraud recoveries by CMS and TMA illustrate the benefits of fraud management programs. With expenditures of over $3.8 billion in FY 2009, VHA's Fee Program is also vulnerable to fraud. VHA needs to establish processes that assess the risk of fraud to the Fee Program and implement fraud controls designed to address the fraud risks identified.

Recommendation

We recommended that the Under Secretary for Health establish a fraud management program that includes such fraud controls as data analysis and high-risk payment reviews, system software edits, employee fraud training, and fraud awareness and reporting.

Management Comments and OIG Response

The Under Secretary for Health agreed with our finding and recommendation and provided an acceptable implementation plan.

The Under Secretary stated that VHA will develop a fraud management plan and sub-plans for data analysis, high-risk payment reviews, fraud awareness, and fraud reporting. VHA will also conduct employee fraud training and fee preauthorization training for its compliance officers. VHA plans to complete these actions by October 30, 2010.

We consider these corrective actions acceptable and will follow up on their implementation.

Appendix A Scope and Methodology

Period of Review

The period of our review was October 2009 through April 2010.

Methodology

We assessed Fee Program payment processes and operating controls by examining recent OIG audit files, interviewing CBO, VISN, and VAMC officials, and reviewing Fee Program policies and procedures.

We identified common practices of fraud management programs from anti-fraud publications and organizations having well-established fraud management programs, such as CMS and TMA. We then compared VHA's Fee Program controls against those benchmarks.

We conducted interviews and obtained relevant documentation from the CBO to identify current fraud management controls for the Fee Program. We also interviewed officials from offices that review Fee Programs to determine the standards and procedures used in their reviews.

To identify Fee Program fraud management controls in effect at VHA fee offices, we interviewed fee office, utilization review, and compliance officials at 10 facilities. These fee offices included 2 consolidated VISN fee offices that processed fee claims for 18 VAMCs. The 10 fee offices are listed below.

- Philadelphia VA Medical Center, Philadelphia, PA
- VA Mid-Atlantic Health Care Network Salem, VA
- Charlie Norwood VA Medical Center, Augusta, GA
- James A. Haley Veterans' Hospital, Tampa, FL
- Louis Stokes VA Medical Center, Cleveland, OH
- VA Medical Center, Battle Creek, Battle Creek, MI
- Edward Hines, Jr. VA Hospital, Hines, IL
- South Central VA Health Care Network, Jackson, MS
- Central Texas Health Care System, Temple, TX
- VA Southern Arizona Health Care System, Tucson, AZ

We also conducted a risk analysis of fee payment fraud indicators and reviewed FY 2009 fee payments to test two high-risk indicators of potential fraud in duplicate payments and billings for services not rendered.

Compliance with Government Inspections Standards

We conducted this review under the *Quality Standards for Inspections* (dated January 2005) issued by the President's Council on Integrity and Efficiency. Those standards require that the evidence supporting our findings, conclusions, and recommendations should be sufficient, competent, and relevant and should lead a reasonable person to sustain the findings, conclusions, and recommendations.

Appendix B Background

Definition of Health Care Fraud

The National Health Care Anti-Fraud Association defined health care fraud as an intentional deception or misrepresentation that an individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, the entity, or some other party.

Fraud Management Programs

According to the fraud management guide *Managing the Business Risk of Fraud*, developed jointly by the American Institute of Certified Public Accountants, Institute of Internal Auditors, and the Association of Certified Fraud Examiners, fraud management programs consist of the following major components:

Fraud Management Program Governance. A fraud management program should have written policies and procedures that convey the expectations of senior leaders regarding fraud management for the organization. These policies and procedures should address fraud management responsibilities and commitments, risk assessment, fraud awareness, reporting procedures, and corrective actions.

Fraud Risk Assessments. Fraud risk assessments are designed to identify where fraud may occur and who the perpetrators might be. They generally include three key elements: (1) identifying fraud risks, (2) assessing the likelihood and significance of fraud risks, and (3) responding to likely and significant fraud risks.

Fraud Prevention and Detection Controls. To address fraud risks, organizations should implement both fraud prevention and fraud detection controls. Fraud prevention encompasses the policies, procedures, training, and communication designed to stop fraud before it occurs. Fraud detection focuses on techniques designed to recognize whether fraud has occurred or is occurring.

Although preventive measures cannot ensure that fraud will not be committed, they are a primary means of controlling fraud. One method of preventing fraud is to promote fraud awareness. Making the existence of a fraud management program known through a wide variety of media reinforces the message that the organization is committed to combating fraud and serves as a deterrent to those who might otherwise be tempted to commit fraud.

The types of detection controls needed depend on the fraud risks identified. Detection controls include having hotlines and other fraud reporting mechanisms, inspections and other process controls, and data mining and other proactive fraud detection techniques specifically designed to identify

fraudulent activities. The organization should continuously monitor, evaluate, and improve its fraud detection techniques. If deficiencies are found, management should ensure that improvements and corrections are made as soon as possible.

Investigation and Corrective Actions. The organization should also establish processes for documenting, tracking, and investigating potential fraud cases. Follow-on actions could include criminal prosecutions, changes in internal controls or business processes, or extended investigations.

Common Fraud Prevention and Detection Controls

Examples of fraud prevention and detection controls commonly used by fraud management programs are listed below.

Data Analyses and Reviews:

- Use of centralized databases to record and track payment information
- Data analyses of payments for possible fraudulent billing patterns
- Post-payment reviews of high-risk areas such as duplicate payments
- Medical reviews of claims for appropriateness of the services billed
- Expanding reviews of claims, as needed
- Follow-up actions, such as changing system software edits, changing pre-payment processes, or initiating fraud investigations

System Software Edit Reviews:

- Automated pre-payment edits
- Post-payment reviews of flagged claims
- Follow-up actions, such as making adjustments in system software edits, tracking problem provider claims, or initiating fraud investigations

Employee Fraud Training:

- Training on latest fraud schemes
- Training on fraud reporting
- Training on fraud detection and controls

Fraud Awareness and Reporting:

- Fraud awareness information to providers and beneficiaries
- Instructions to providers and beneficiaries on reporting fraud
- Publicizing reports on fraud prevention and detection results

Appendix C Agency Comments

Department of Veterans Affairs

Memorandum

Date: May 17, 2010

From: Under Secretary for Health (10)

Subj: OIG Draft Report, Review of Fraud Management for the Non-Department of Veterans Affairs (VA) Fee Care Program, (Project No. 2010-0004-R8-0185, WebCIMS 444649)

To: Assistant Inspector General for Audits and Evaluations (52)

1. I have reviewed the draft report and concur with the recommendation. Attached is the Veterans Health Administration's (VHA) plan of corrective action for the report's recommendation.

2. VHA concurs with the report's recommendation to develop a fraud management program that includes such fraud controls as data analysis and high-risk payment reviews, system software edits, employee fraud training, and fraud awareness and reporting. VHA's Chief Business Office (CBO) will develop a data analysis and high-risk payment reviews sub-plan as well as an awareness and reporting plan to educate providers and Veterans. The CBO will also conduct employee fraud training. In addition, VHA's Compliance and Business Integrity Office will design training for VHA's compliance officers regarding proper preauthorization for Service-Connected Veterans who are authorized for non-VA/fee outpatient care.

3. Thank you for the opportunity to review the draft report. If you have any questions, please contact Linda H. Lutes, Director, Management Review Service (10B5) at (202) 461-7014.

Robert A. Petzel, M.D.

Attachment

VETERANS HEALTH ADMINISTRATION (VHA)
Action Plan

OIG Draft Report, Review of Fraud Management for the Non-Department of Veterans Affairs (VA) Fee Care Program, (Project No. 2010-0004-R8-0185, WebCIMS 444649)

Date of Draft Report: April 14, 2010

Recommendations/ Actions	Status	Completion Date

Recommendation 1. We recommend that the Under Secretary for Health establish a fraud management program that includes such fraud controls as data analysis and high-risk payment reviews, system software edits, employee fraud training, and fraud awareness and reporting.

VHA Comments

Concur

The Veterans Health Administration's (VHA) Chief Business Office (CBO) will:

- Develop a program integrity/fraud management plan by September 30, 2010.
- Develop a data analysis and high-risk payment reviews sub-plan by July 31, 2010.
- Develop a system software edit plan utilizing claim scrubber edits within the Fee Basis Claims System (FBCS) by October 30, 2010.
- Conduct employee fraud training and course modules by September 30, 2010. Initial training will take place May 17, 2010, at the CBO National Conference. In the future this training will occur annually.
- Develop a fraud awareness and reporting plan to educate providers and Veterans by September 30, 2010.

The Office of the Deputy Under Secretary for Health for Operations and Management (DUSHOM) will work with the CBO to implement training at the Veterans Integrated Service Network (VISN) level. The CBO will certify to the DUSHOM once training is completed.

	In process	See individual action items

The Compliance and Business Integrity (CBI) office, will design training for VHA's compliance officers regarding proper preauthorization for Service-Connected Veterans who are authorized for non-VA/fee outpatient care. The training will begin in June 2010. The goal of the training session is to improve oversight of the preauthorization process and provide an auditing tool for facility compliance officers on the identification of potential fraudulent activity. The DUSHOM will work with the CBI to implement this training at the VISN level. The CBI will certify to the DUSHOM once training is completed.

In process June 30, 2010

Veterans Health Administration
May 2010

Appendix D OIG Contact and Staff Acknowledgments

OIG Contact	Gary Abe (206) 220-6651
Acknowledgments	Ron Stucky Kevin Day Maria Afamasaga Randy Alley Tom Phillips Melinda Toom Sherry Ware

Appendix E Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

This report will be available in the near future on the OIG website at http://www.va.gov/oig/publications/reports-list.asp. This report will remain on the OIG website for at least 2 fiscal years after it is issued.