VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Transmission of Sensitive VA Data Over Internet Connections

March 6, 2013
12-02802-111

ACRONYMS AND ABBREVIATIONS

OIG	Office of Inspector General
CBOC	Community Based Outpatient Clinic
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act of 1996
MPLS	Multiprotocol Label Switching
OIT	Office of Information and Technology
PII	Personally Identifiable Information
VAMC	Veterans Affairs Medical Center
VISN	Veterans Integrated Service Network

Report Highlights: Review of Alleged Transmission of Sensitive VA Data Over Internet Connections

Why We Did This Review

The Office of Inspector General (OIG) evaluated the merits of an allegation that VA was transmitting sensitive data, including Personally Identifiable Information (PII) and internal network routing information, over unencrypted telecommunications carrier networks. In July 2012, the OIG informed the Assistant Secretary for Information and Technology of the possible security violations so VA could assess relative risks and take appropriate corrective actions.

What We Found

We substantiated the allegation that VA was transmitting sensitive data, including PII and internal network routing information, over an unencrypted telecommunications carrier network. Office of Information and Technology (OIT) personnel disclosed that VA typically transferred unencrypted sensitive data, such as electronic health records and internal Internet protocol addresses, among certain VA medical centers and Community Based Outpatient Clinics (CBOCs) using an unencrypted telecommunications carrier network.

VA has not implemented technical configuration controls to ensure encryption of sensitive data despite VA and Federal information security requirements. OIT personnel stated that sending unencrypted sensitive data to outpatient clinics and external business partners was a common practice at facilities across VA. OIT management acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged via a waiver; however, the use of a system security waiver was not appropriate.

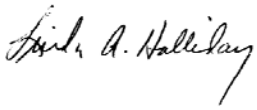
Without controls to encrypt the sensitive VA data transmitted, veterans' information may be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Further, malicious users could obtain VA router information to identify and disrupt mission-critical systems.

What We Recommend

We recommend the Assistant Secretary for Information and Technology identify the VA networks transmitting sensitive data over the unencrypted carrier networks and implement configuration controls to ensure encryption of such data. The Assistant Secretary should also require that OIT personnel complete specialized training emphasizing the importance of encrypting sensitive VA data transmitted across the Internet.

Agency Comments

The Assistant Secretary for Information and Technology concurred with our report recommendations and provided technical comments for consideration. The OIG will monitor implementation of the corrective action plans.



LINDA A. HALLIDAY
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

We conducted this review to determine the merits of an allegation that VA was transmitting sensitive data, including Personally Identifiable Information (PII) and internal network routing information, over unencrypted telecommunications carrier networks.

Background

The VA Midwest Health Care Network, also known as the Veterans Integrated Service Network (VISN) 23 within the Veterans Health Administration, serves more than 400,000 veterans enrolled to receive medical care residing in Iowa, Minnesota, Nebraska, North Dakota, South Dakota and portions of Illinois, Kansas, Missouri, Wisconsin, and Wyoming.

Allegation

In May 2012, a complainant contacted the VA Office of Inspector General (OIG) Hotline, alleging that certain VA medical centers (VAMCs) were transmitting sensitive information, including PII and internal network routing information, over unencrypted telecommunications carrier networks. More specifically, the complainant indicated that unencrypted data were transmitted among various VAMC networks using the South Dakota Network, which functions as the local telecommunications carrier network.

The complainant alleged that these security violations occurred at VAMCs located in Fort Meade, SD; Omaha, NE; and Sioux Falls, SD, which are in VISN 23. To determine the merits of this Hotline allegation, we visited the three VAMCs identified in the complaint letter. We interviewed VA's Office of Information and Technology (OIT) personnel to gain an understanding of existing data transmission practices and associated controls. In addition, we evaluated VA policies, procedures, and information security controls for transmission of sensitive data and related router configurations over telecommunications carrier networks.

Other Non-VA OIG Reports

Unencrypted sensitive VA data could be used to perpetrate various types of fraud, including tax fraud. To illustrate, the Treasury Inspector General for Tax Administration issued an audit report in July 2012 stating that fraudulent returns involving identity theft totaled $6.5 billion in 2011 and estimated that approximately $21 billion in fraudulent tax refunds from identity theft would be issued over the next 5 years.[1]

Additional Information

The following appendixes provide additional information.

- Appendix A provides pertinent background information.
- Appendix B provides details on our scope and methodology.
- Appendix C provides comments by the Assistant Secretary for Information and Technology on a draft of this report.

[1] *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft*, Treasury Inspector General for Tax Administration (Report of Audit No. 2012-42-080), July 19, 2012.

RESULTS AND RECOMMENDATIONS

Finding VA Transmission of Unsecured Sensitive Data

We substantiated the allegation that VA was transmitting sensitive data, including PII and internal network routing information, over an unencrypted telecommunications carrier network. OIT personnel disclosed that VA typically transferred unencrypted sensitive data, such as electronic health records and internal Internet protocol addresses, among certain VA medical centers and Community Based Outpatient Clinics (CBOCs) using an unencrypted telecommunications carrier network.

VA has not implemented technical configuration controls to ensure encryption of sensitive data despite VA and Federal information security requirements. OIT personnel stated that sending unencrypted sensitive data to outpatient clinics and external business partners was a common practice at facilities across VA. OIT management acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged.

Without controls to encrypt the sensitive VA data transmitted, veterans' information may be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Further, malicious users could obtain VA router information to identify and disrupt mission-critical systems essential to providing health care services to veterans.

Unencrypted Sensitive Data Transmitted

We substantiated the allegation that VA was transmitting sensitive data, including PII and internal network routing information, over an unencrypted telecommunications carrier network. During our site visits to the VAMCs in Fort Meade, SD; Omaha, NE; and Sioux Falls, SD, OIT personnel disclosed that VA routinely transferred unencrypted sensitive data among the VAMCs and CBOCs using a telecommunications carrier network, known as the South Dakota Network. Sensitive information included veterans' and dependents' names, Social Security numbers, dates of birth, and protected health information. The data also included the Veterans Health Information Systems and Technology Architecture's electronic health records and internal Internet protocol addresses.

We also noted that the Sioux Falls and Fort Meade VA medical facilities regularly used unencrypted telecommunications carrier networks to transmit unencrypted sensitive data to external organizations providing remote Teleradiology services. Teleradiology services involve electronically sending radiographic patient images, such as X-rays, and sensitive patient information from one location to another for the purpose of interpretation and/or consultation with radiologists.

VA's practice of transmitting unencrypted sensitive data was a violation of VA and Federal information security requirements. Specifically, VA's Handbook 6500, *Information Security Program*, requires that the electronic transmission of VA sensitive information must be encrypted in accordance with *Federal Information Processing Standards* (FIPS) 140-2. This publication provides security standards when organizations specify they will use encryption mechanisms to protect sensitive information. VA has specified encryption security protections for a number of external business partner connections that routinely exchange sensitive data. As such, VA needs to provide comparable encryption protections when transmitting electronic health records and sensitive data among VA medical facilities and CBOCs or other external organizations.

In addition, VA Handbook 6500 states that VA will comply with the requirements of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), which identifies encryption as a technical safeguard supporting access controls and transmission security. *The Health Information Technology for Economic and Clinical Health Act*, as part of the *American Recovery and Reinvestment Act of 2009*, requires the encryption of electronically transmitted health information and broadens the scope of privacy and security protections for protected electronic health information under HIPAA and increases the potential legal liabilities for noncompliance. Finally, VA Handbook 6500 also requires periodic training in computer security awareness and accepted computer security practices, including PII and HIPAA awareness, for all VA employees, contractors, and other users of sensitive VA information and systems.

Causes for Unsecured Data Transmissions

Despite VA and Federal information security requirements, VA has not implemented a configuration control that would ensure encryption of sensitive data. OIT personnel stated that sending unencrypted sensitive data to CBOCs and external business partners was a common practice within VISN 23 and other facilities across VA. OIT management acknowledged that certain facilities were transmitting such data over unencrypted telecommunications carrier networks. However, OIT management formally accepted the security risks associated with the potential loss or misuse of the data, as defined within VA systems security waiver documents.

VA developed these system security waivers to delay implementing encryption controls in the near term, while acknowledging the risks associated with the lack of technical configuration controls. Security waivers were signed by the Assistant Secretary for Information and Technology and the Acting Under Secretary for Health, Veterans Health Administration. FIPS 140-2 states that under certain exceptional circumstances, the heads of Federal agencies, or their delegates, may approve waivers. Nevertheless, FIPS 140-2 defines appropriate security standards when organizations specify they will use encryption mechanisms to protect sensitive information.

VA has implemented encryption security protections for a number of existing external business partner connections. Accordingly, implicit in the FIPS security requirements, the use of a system security waiver is not appropriate. VA has also specified in its information security policies and practices that it will use encryption controls to protect sensitive data. Moreover, VA and Federal information security requirements clearly call for the encryption of sensitive VA data and emphasize the importance of safeguarding this information.

Effects of Unsecured Data Transmissions

Without effective controls to encrypt the transmission of VA sensitive data, veterans' information remained vulnerable to interception and misuse by malicious users as data traversed unencrypted telecommunications carrier networks. As stated previously, unencrypted VA sensitive data could be used to perpetrate various types of fraud.

Malicious users could also use unprotected internal router information to gather information about the VA network infrastructure and disrupt mission-critical systems, essential to providing health care services to veterans. Given its unsecure data sharing practices, VA could potentially face various financial and other penalties for noncompliance with Federal laws that require safeguarding of protected health information. Encrypting sensitive data is critical as VAMCs in Fort Meade, SD; Omaha, NE; and Sioux Falls, SD, routinely transmit sensitive electronic health data to and from CBOCs and other external organizations in order to provide health care services to veterans across a wide geographic area. Further, VISN 23 serves more than 400,000 enrolled veterans and provides numerous specialized healthcare and research programs. As such, implementing adequate security protections is essential for safeguarding sensitive patient information and providing ongoing medical services to veterans.

Two prior VA Secretaries testified before Congress that the Department should be the "Gold Standard" in information security. Specifically, they indicated that VA must be the best in the Federal Government in protecting personal and health information, training and educating employees to achieve that goal, and instituting a culture that puts the custody of veterans' personal information first. The current VA Secretary also stated that veterans have suffered the consequences of careless information security practices in the past, including unintended exposure and loss of PII. He concluded that VA can, and must, do better.

Recommendations

1. We recommend the Assistant Secretary for Information and Technology identify VA networks transmitting unprotected sensitive data over unencrypted telecommunication networks and implement technical configuration controls to ensure encryption of such data in accordance with applicable VA and Federal information security requirements.

2. We recommend the Assistant Secretary for Information and Technology require that OIT personnel complete specialized training emphasizing the importance of encrypting sensitive VA data transmitted across public Internet connections.

Management Comments and OIG Response

The Assistant Secretary for Information and Technology concurred with our recommendations and provided technical comments for our consideration. Following is a summary of VA's technical comments and our response.

Management Comments Regarding Unencrypted Transmission of Sensitive VA Data

The Assistant Secretary for Information and Technology did not agree with the assertion that PII and internal network routing information were being transmitted over unsecured Internet connections. He nonetheless acknowledged that VA transmits PII over privately segmented networks to support service to veterans. Further, the Assistant Secretary stated that OIT employs an industry telecommunications carrier network, using Multiprotocol Label Switching (MPLS) network links, to provide a segmented network for transmitting PII. OIT acknowledged these MPLS network links are not currently employing encryption.

The Assistant Secretary stated OIT will review and ensure VA networks are not transmitting unprotected sensitive data over public Internet connections and will immediately correct such issues, if found. In response to our Hotline complaint, in May 2012, OIT authorized implementation of a Department-wide encryption solution in Fiscal Year 2013 that will address VA's information security requirements for protecting the transmission of sensitive VA data.

OIG Response

Based on interviews with OIT personnel at VA medical centers as well information provided by the complainant, we maintain that PII and router information were being transmitted unencrypted through the South Dakota Network, a telecommunications carrier that also provided Internet services to customers outside of VA. Nonetheless, we commend OIT for performing a review of the locations associated with the Hotline complaint and inspecting MPLS communication networks to ensure proper segmentation of VA networks from Internet connections. We recognize that using MPLS networks can segment data traffic from unsecured Web connections. However, we believe the risk remains that sensitive VA data and router information can be compromised when it is transmitted across unencrypted telecommunications carrier networks outside of VA's span of technical control. More specifically, a MPLS network alone does not provide encryption, integrity, or authentication protections for the transmission of

sensitive data and such services may be vulnerable to denial of service or sniffing attacks by malicious users.

The Assistant Secretary for Information and Technology acknowledged these information security risks by stating OIT will review technical network communications practices across the enterprise and take corrective actions without hesitation. Further acknowledging the information security risks discussed in this report, OIT plans to implement a VA-wide encryption solution to protect sensitive data transmitted across telecommunications carrier networks. This solution will use Advanced Encryption Standard cryptography so VA can employ network security controls while utilizing existing MPLS carrier networks. As the Assistant Secretary suggests, we have revised the wording in this report to the extent possible to use "telecommunications carrier network" rather than "Internet" to clarify the means discussed to transmit VA data.

Management Comments Regarding Specialized Training

The Assistant Secretary for Information and Technology stated that the mandated, annual Privacy and Information Security Awareness course details specific guidance and policy related to protecting VA data in all forms to include protecting information using encryption when transmitted via the Internet. For employees with significant information security responsibilities, VA's Information Technology Workforce Development has specialized training courses available to provide guidance on using encryption tools. Additionally, VA will immediately develop and implement an awareness campaign that addresses the importance of data protection and the requirement to use encryption.

OIG Response

We believe OIT's actions are responsive to the intent of our recommendation. We will monitor implementation of these actions and will close the recommendation when we receive sufficient evidence demonstrating VA progress in addressing the issues identified.

Appendix A Background

VISN 23 Overview

Within the Veterans Health Administration, the VAMCs in Fort Meade, SD; Omaha, NE; and Sioux Falls, SD, are part of the VA Midwest Health Care Network, also known as VISN 23. The Network serves more than 400,000 veterans enrolled to receive medical care and residing in Iowa, Minnesota, Nebraska, North Dakota, South Dakota, and portions of Illinois, Kansas, Missouri, Wisconsin, and Wyoming. The Veterans Health Information Systems and Technology Architecture is an enterprise-wide application used throughout the Veterans Health Administration to manage sensitive electronic health records and data related to healthcare services provided to these veterans.

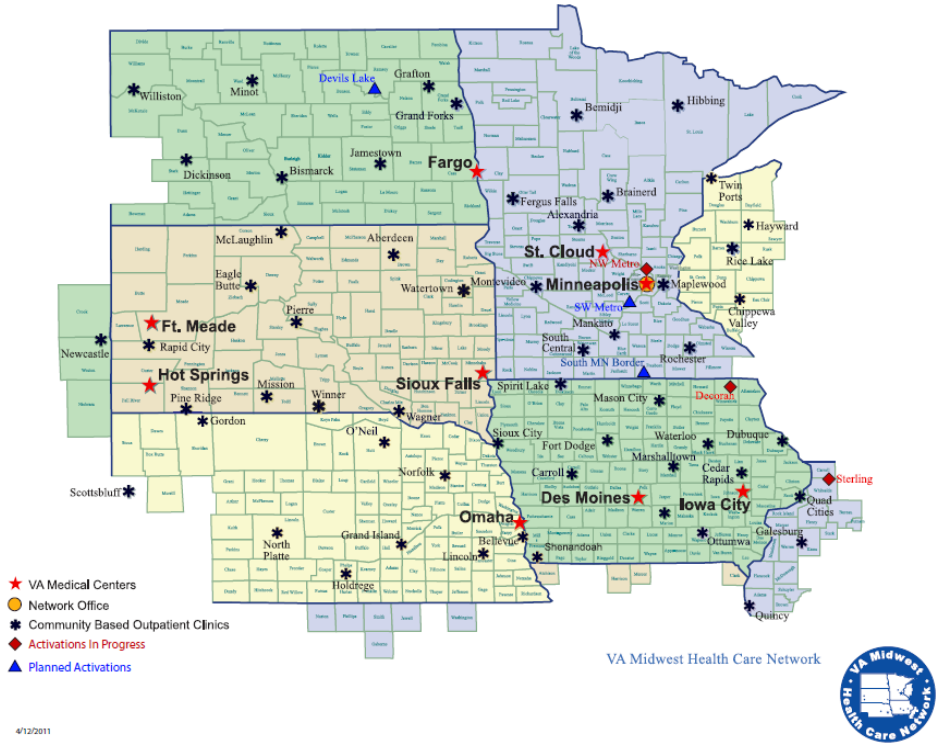
VISN 23 Specialized Programs and Research

VISN 23 has numerous specialized programs and research activities that potentially involve the use of sensitive VA data. In the VISN, an array of specialized programs are available for veterans that cannot be adequately managed in primary care clinics and general outpatient mental health clinics. These special programs include rural health, spinal cord injury and rehabilitation, polytrauma rehabilitation, traumatic brain injury, kidney transplants, and bariatric surgery.

VISN 23 also helps advance health care for veterans by performing research in health and brain sciences, chronic diseases, and vision loss. VISN 23 health care services are delivered through an integrated system of 4 residential rehabilitation treatment programs, 8 community living centers, 8 hospitals and 56 CBOCs. The Network employs over 10,000 full-time employees and has an annual operating budget of $2 billion. The map in the following Figure shows VISN 23 locations.

Figure

VISN 23 Locations



Source: VISN 23 website information as of July 2012

Appendix B Scope and Methodology

To conduct our review, we examined applicable statutes and VA policies and procedures regarding information security requirements for the encryption of sensitive data. Our review evaluated the merits of a VA Hotline allegation that certain VAMCs were transmitting sensitive information over an unsecured industry telecommunications carrier network, including PII and internal network routing information.

To accomplish the review, we conducted fieldwork at VAMCs located in Fort Meade, SD; Omaha, NE; and Sioux Falls, SD. We interviewed OIT personnel and evaluated VA policies, procedures, and information security controls, including router configurations, to support the transmission of sensitive data over an industry telecommunications carrier network. We performed all fieldwork from May 2012 through September 2012.

Data Reliability

We did not request computer-processed data for this review. We evaluated the sufficiency and accuracy of information provided regarding VA policies, procedures, and information security controls.

Government Standards

We conducted our review in accordance with *Quality Standards for Inspection and Evaluation* published by the Council of the Inspectors General on Integrity and Efficiency. We planned and performed the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objective.

Appendix C Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs

Memorandum

Date: February 1, 2013

From: Assistant Secretary for Information and Technology (005)

Subj: OIG Draft Report, Review of Alleged Transmission of Sensitive VA Data Over Internet Connections

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

1. Thank you for your evaluation of an allegation that VA is transmitting sensitive data, including Personally Identifiable Information (PII) and internal network routing information, over unsecured Internet connections. The Office of Information and Technology (OIT) appreciates the Inspector General's review of allegation of fraud, waste or abuse of OIT programs and especially into matters related to the potential exposure of Veterans' personal information.

2. OIT concurs with the Office of Inspector General (OIG) recommendations and the actions already taken are described in the attached. However, OIT does not agree with the assertion that PII and internal network routing information are being transmitted over unsecured Internet connections. OIT employs service offerings from industry telecommunications carriers that are privately segmented from other public traffic and that secure internal routing information from exposure to unauthorized entities. These carrier services provide VA with a private network and do not place traffic on the Internet. It is necessary, in serving our Veterans, to transmit PII. The network links in question are not currently employing encryption but these transmissions are crossing only the private VA network and are not exposed to or traversing the Internet.

3. After learning of the allegation, OIT immediately engaged in a comprehensive review of the locations where the complaints were focused and subsequently determined that the allegation is unsubstantiated. The review was conducted utilizing subject matter experts from outside of the geography and organization in the report. The communications circuits in the geography in question were inspected, the configuration of the associated network equipment was reviewed, and the network administrators were interviewed. All of the findings conclusively substantiated that traffic is traversing only VA's private network and is not utilizing

4. the Internet, or otherwise publicly exposed, in any way. The telecommunications carrier for these communications links was also interviewed to validate the nature and configuration of their service offering. The carrier confirmed that the communications links in questions are private Multiprotocol Label Switching (MPLS) that provide a secure, privately segmented network to VA. A letter from the telecommunications carrier is also attached.

5. Also attached is a technical explanation and diagrams demonstrating how sensitive information is routed between VA facilities. Although VA does not concur with the Inspector General's findings in this area, OIT has initiated a review to ensure that the current practice described in the aforementioned technical documentation is being consistently applied across the VA enterprise, and if exposures are found, OIT will correct those exposures without hesitation.

6. OIT also concurs with OIG's recommendation regarding training and already has a long standing practice in place. VA requires that personnel complete specialized training emphasizing the importance of encrypting sensitive data. The mandated annual Privacy and Information Security Awareness course details specific guidance and policy related to protecting VA data in all forms to include protecting information using encryption when transmitted via the Internet. Additionally, if an employee's role includes significant information security responsibilities, they are required to take role-based information security training through which additional data protection direction is provided that is specific to the employee's job. IT Workforce Development also has specialized training courses available to provide guidance for using encryption tools and will immediately develop an awareness campaign that addresses the issue of data protection and the requirement to use encryption. This campaign will be implemented within the next two months.

7. We appreciate your time and attention to our information technology and data protection programs. If you have any questions, contact me at (202) 461-6910.

Roger W. Baker

Attachment

Office of Information and Technology
Response to Draft OIG Report
"Review of Alleged Transmission of Sensitive VA Data Over Internet Connections"

Recommendation 1: We recommend the Assistant Secretary for Information and Technology identify VA networks transmitting unprotected sensitive data over public Internet connections and implement technical configuration controls to ensure encryption of such data in accordance with applicable VA and Federal information security requirements.

OIT Response: (Concur per above Memorandum.) Though OIT disagrees with the assertion that PII was being transmitted over the public Internet and has substantiated that the allegation is incorrect, it does concur with the recommendation to perform a review.

On December 24, 2012, OIT directed a review to ensure that no VA networks are transmitting unprotected sensitive data over public Internet connections and will immediately correct such issues, if found.

On May 4, 2012, OIT authorized the implementation of a Group Encrypted Transport VPN (GET VPN) Intranet solution for deployment in Fiscal Year 2013 that will address VA 6500 Appendix D requirements for Transmission Confidentiality.

Recommendation 2: We recommend the Assistant Secretary for Information and Technology require that OIT personnel complete specialized training emphasizing the importance of encrypting sensitive VA data transmitted across public Internet connections.

OIT Response: (Concur per above Memorandum.) The mandated annual Privacy and Information Security Awareness course details specific guidance and policy related to protecting VA data in all forms to include protecting information using encryption when transmitted via the Internet. This course is an annual requirement for all VA staff and contractors and is required to gain and maintain access to VA systems.

Additionally, if an employee's role includes "significant information security responsibilities" they are also required to take Role-Based INFOSEC training where additional data protection direction is provided that is specific to the employee's job. There are also specialized training courses available to provide guidance for using encryption tools.

In addition to this existing training, IT Workforce Development will immediately develop an awareness campaign that addresses the issue of data protection and the requirement to use encryption and implement this campaign within the next two months.

We request closure of this recommendation based on the evidence provided above and in the supporting documentation identified below.

Appendix D Office of Inspector General Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman, Director Jack Henserling William Hill Ryan Nelson

Appendix E Report Distribution

VA Distribution

Office of the Secretary
Veterans Health 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's Web site at http://www.va.gov/oig. This report will remain on the OIG Web site for at least 2 fiscal years.