Department of Veterans Affairs

Office of Inspector General

# AUDIT OF DEPARTMENT OF VETERANS AFFAIRS PROCUREMENT OF DESKTOP COMPUTERS WITH MODEMS

*VA can enhance its computer network security and reduce procurement costs by eliminating the unneeded acquisition of desktop computers with modems.*

Report No. 04-03100-66 January 11, 2005

VA Office of Inspector General
Washington, DC 20420

**To Report Suspected Wrongdoing in VA Programs and Operations**

**Call the OIG Hotline – (800) 488-8244**

**DEPARTMENT OF VETERANS AFFAIRS**
**Office of Inspector General**
**Washington, DC 20420**

**TO:** Assistant Secretary for Information and Technology (005)
Acting Assistant Secretary for Management (004)

**SUBJECT:** Audit of Department of Veterans Affairs Procurement of Desktop Computers With Modems (Report No. 04-03100-66)

1. The Office of Inspector General (OIG) conducted an audit of Department of Veterans Affairs (VA) purchases of desktop computers (workstations) off of its Procurement of Computer Hardware and Software-2 (PCHS-2) contract. This audit was completed as part of a project initiative[1] to determine the effectiveness and efficiency of selected VA Information Technology (IT) contracts.

2. The audit found that VA's acquisition of workstations should not include modems[2] unless the need is justified. Workstations procured for use as part of VA's computer network do not generally require modems, unless needed for remote access,[3] or used for required maintenance of medical equipment. The unnecessary presence of modems in workstations connected to VA's computer network increases its network IT security vulnerability and procurement costs. We found that VA activities are not required to justify the need for modems included in workstations purchased off the PCHS-2 contract. Since VA began purchasing workstations off of this contract in April 2002, at least 3,396[4] included modems. Including modems in these workstations added $84,900 to VA's procurement costs ($25 per workstation).

3. Prior reviews conducted by our office have shown that the use of modems has been a VA IT security vulnerability for several years. Potential hackers can use modems to circumvent network security and gain unauthorized access to sensitive information and data. Additionally, VA's Windows NT Enterprise Security Policy specifically limits

[1] Audit of Selected Information Technology Contracts, Project No. 2004-03100-D2-0429.

[2] A device that adapts a terminal or computer to a telephone line converting the computer's digital pulses into audio frequencies (analog) for the telephone system, and converts the frequencies back into digital pulses at the receiving side. This process allows a direct connection and transfer of information between individual workstations, both inside and outside of VA's network.

[3] The ability of a computer in one location to connect to a device that is at another location or site.

[4] We were unable to obtain complete information on VA purchases of workstations with modems off the PCHS-2 contract. The purchases identified are based on partial sales information provided by the PCHS-2 vendors.

their use. VA can reduce its information security program risk and procurement costs by better controlling the acquisition and use of modems in its computer network operations.

4. On October 19, 2004, we issued an Advisory Letter to the Assistant Secretary for Information and Technology (005) and to the Acting Assistant Secretary for Management (004) detailing our concerns about VA's acquisition and use of modems. Given the information security risk associated with modem use, the Advisory Letter was provided to management so appropriate corrective actions could be taken. We recommended the following actions:

- Require specific justification for acquisition of modems, including the approval of the local facility Information Security Officer (ISO).
- Disable modems in workstations currently connected to VA's network, unless it is determined that they are needed.
- Modify the PCHS-2 contract to exclude offering workstations with modems as a standard configuration.

5. In response to the Advisory Letter findings and recommended actions, we were advised[5] that program officials in the Office of Acquisition and Materiel Management (OA&MM) and the Office of Cyber and Information Security (OCIS) would coordinate to develop a policy directive addressing our concerns for signature by the Assistant Secretary for Information and Technology.

6. On November 15, 2004, the Assistant Secretary for Information and Technology issued a Department-wide memorandum on the installation of modems in workstations. (See Appendix A on pages 4-5 for the Assistant Secretary's memorandum.) The memorandum highlights the IT security risk associated with use of modems and discusses actions being taken to better control their acquisition and use. Key actions include the following:

- Facility directors were requested to review all workstations in their facilities and remove all modems unless they are justified and a waiver has been granted.
- All workstations that contain modems should be tracked by the responsible ISO in accordance with existing administration and staff office policies and procedures.
- System security plans must reference or contain risk mitigation strategies for workstations containing modems that are connected to VA's network.
- PCHS-2 contract will be modified to remove purchase options for workstations with modems with the exception of those buys that have been justified by the responsible ISO and approved by OCIS.

[5] November 2, 2004, email received from the Acting Associate Deputy Assistant Secretary for Acquisitions. On November 23, 2004, the Acting Assistant Secretary for Management issued a memorandum to the Assistant Secretary for Information and Technology offering to assist in development of VA-wide policy on use of modems, and complete necessary modifications to the PCHS-2 contract.

7. The planned corrective actions are acceptable and address the actions recommended in our Advisory Letter. We will follow up on the planned actions until they are completed.

*(original signed by Gerald Grahe,*
*Deputy Assistant Inspector General*
*for Auditing for:)*

MICHAEL L. STALEY
Assistant Inspector General
for Auditing

# Results of Audit

## Introduction

We reviewed VA purchases of workstations off of the PCHS-2 contract to identify those that included modems. The PCHS-2 contract is a mandatory source for all VA purchases of IT hardware and software products. The contract was awarded in April 2002 for a base year and four option years, with a maximum value of $1.375 billion. Through August 2004, VA activities had purchased 124,405 workstations off of the PCHS-2 contract.

## Scope of Work

We reviewed the PCHS-2 contract files maintained by the responsible Contracting Officer (CO) in OA&MM located in VA Central Office (VACO). We also contacted the PCHS-2 vendors and obtained sales information on workstations purchased by VA activities that included modems. VA does not maintain consolidated information on PCHS-2 contract purchases that identifies how each workstation is configured. We discussed our findings and obtained input from the CO and other OA&MM program officials. We also met with OCIS program officials to obtain input on actions needed to better control the introduction of modems into VA's computer network.

The audit was conducted in accordance with generally accepted government auditing standards for staff qualifications, independence, and due professional care; field work standards for planning, supervision, and evidence; and reporting standards for performance audits.

## Results

The unnecessary inclusion of modems in workstations connected to VA's network introduces a security vulnerability to VA systems and data and additional procurement costs that can be avoided.

Use of Modems is a Long Standing VA IT Security Vulnerability Area

During each of the annual OIG information security audits completed since Fiscal Year (FY) 2001,[6] we identified the existence of modems involving workstations connected to VA's computer network. During the current audit, network scanning[7] detected 307

[6] Audit of Department of Veterans Affairs Information Security Program, Report No. 00-02797-001, October 24, 2001; Report No. 01-02719-27, December 4, 2002; and, Report No. 02-03210-43, December 9, 2003.

[7] A scan is an automated remote probing of network devices to determine their operating systems and configurations.

active[8] modems at the VA medical centers visited. The use of modems while workstations are connected to VA's computer network can allow hackers to circumvent network security and gain unauthorized access to sensitive information and data. This can occur because the use of modems circumvents network security protection measures in place as part of VA's firewall.[9]

Due to the security vulnerability associated with using modems, the acquisition of them for workstations connected to VA's computer network should be limited and approved only when needed (See Appendix A on page 4 for the Assistant Secretary's memorandum that provides examples of justified use of modems). Under the current procedures for ordering workstations off of the PCHS-2 contract, VA activities purchase workstations with modems without any specific justification of need. This situation allows the continued introduction of modems into VA's network, even though VA policy limits their use.

### VA Security Policy Limits Use of Modems

VA's Windows NT Enterprise Security Policy issued in January 2000, specifies that "Use of unsecured modem connections, particularly in conjunction with software products such as PC AnyWhere, will be discontinued in *all* cases where more secure remote access is available. In addition, the use of individual workstation modems for inbound remote access is not allowed."

During our discussion of the audit findings with OCIS officials, they acknowledged that additional action is needed to better control the introduction and use of modems in VA's computer network operations. This includes requiring justification for the acquisition of modems and establishing better oversight and tracking of those that are in use. OCIS officials indicated that the current policy guidance will be strengthened to establish a justification/approval process for the acquisition and use of modems by VA activities. OCIS officials also indicated that they will coordinate with OA&MM officials to identify needed changes to the PCHS-2 contract to restrict purchase options for modems.

### PCHS-2 Contract Allows Unrestricted Purchase of Modems

Our review of the PCHS-2 contract specifications found that modems can be included in most workstations purchased, without any justification of need. In fact, 2 of the 4 contract vendors authorized to fill purchase orders include modems as a standard configuration for some of their workstations. One vendor offers eight workstation models that include modems while another vendor offers two workstation models that include modems.

[8] This means that the modem was being used while the workstation was connected to VA's network.

[9] A network node set up as a boundary to prevent traffic from one segment to cross over to another. Firewalls are used to improve network traffic, as well as for security purposes.

Based on the sales information obtained from PCHS-2 vendors, we reviewed 24,641 workstation purchases (covering the period April 2002 through August 2004) and identified 2,232 workstations purchased with modems as a standard configuration. In addition to these purchases, we identified 1,164 workstations purchased with modems not included as a standard configuration item.

For an additional 99,764 workstations purchased by VA activities during the period reviewed, we were unable to obtain specific vendor sales information that identified the number of workstations that contained modems. The PCHS-2 vendors acknowledged that they know that some number of these workstations included modems. However, they were not able to identify the specific number of purchases that were made.

Planned VA Purchases of Workstations Are Significant and Require Better Controls Over the Acquisition and Use of Modems

Adequately controlling the acquisition and use of modems is important due to the significant planned VA purchases of workstations. Over the potential 5-year term of the PCHS-2 contract, it is estimated that 207,000 workstations will be purchased. VA is in the third year of the contract and had purchased 124,405 workstations through August 2004. This leaves an estimated 82,595 workstations that could be purchased during the remaining term of the contract, if it is extended for the full 5 years. VA's planned actions to strengthen the controls over the acquisition and use of modems, discussed in the Assistant Secretary's memorandum, should help ensure that the significant number of future planned purchases of workstations do not inappropriately include modems.

The PCHS-2 contract is a mandatory procurement source for workstations purchased by VA activities. As such, VA needs to ensure that these purchases do not include the unnecessary acquisition of modems and the resulting procurement cost of $25 per workstation. The audit found that at least 3,396 workstations VA purchased off the PCHS-2 contract included modems, at a total cost of $84,900. Since we could not identify complete vendor sales information on modems purchased, we are unable to project the extent of future procurement savings to VA by avoiding unneeded acquisition of modems. Eliminating any unnecessary purchases of modems in the future will save VA procurement resources that can be used in providing health care and delivering benefits to the Nations veterans.

## Conclusion

VA acquisition of workstations should not include modems unless the need for them is justified. The unnecessary presence of modems in workstations connected to VA's computer network increases network IT security vulnerability and procurement costs. VA's planned corrective actions in response to our findings should result in better control over the acquisition and use of modems. We will follow up on the planned actions until they are completed.

**Appendix A**

# Assistant Secretary for Information and Technology Memorandum

**Department of Veterans Affairs**

# Memorandum

Date: November 15, 2004

From: Assistant Secretary for Information and Technology (005)

Subj: Limitations on the Installation of Modems in Desktop Computers

To: Under Secretaries, Assistant Secretaries, and Other Key Officials

1. Telephone modems installed in or attached to desktop computers connected to the VA network can create a potentially serious security risk. If a modem is used to dial into an Internet service provider or other network while the desktop computer is connected to the VA network, a bridge is created between the two networks. This can allow for the unmonitored and uncontrolled compromise of sensitive VA data, and lead to infection of the VA network by viruses or other malicious software from the external network.

2. There is seldom a sufficient justification for having a modem in a VA desktop computer. Many organizations in the Department have instituted policies that restrict the use of modems and require justification for their use. Waiver processes are also in place, and waivers have been granted for specific situations for which there is no suitable alternative. The following are examples of situations that might justify the use of modems:

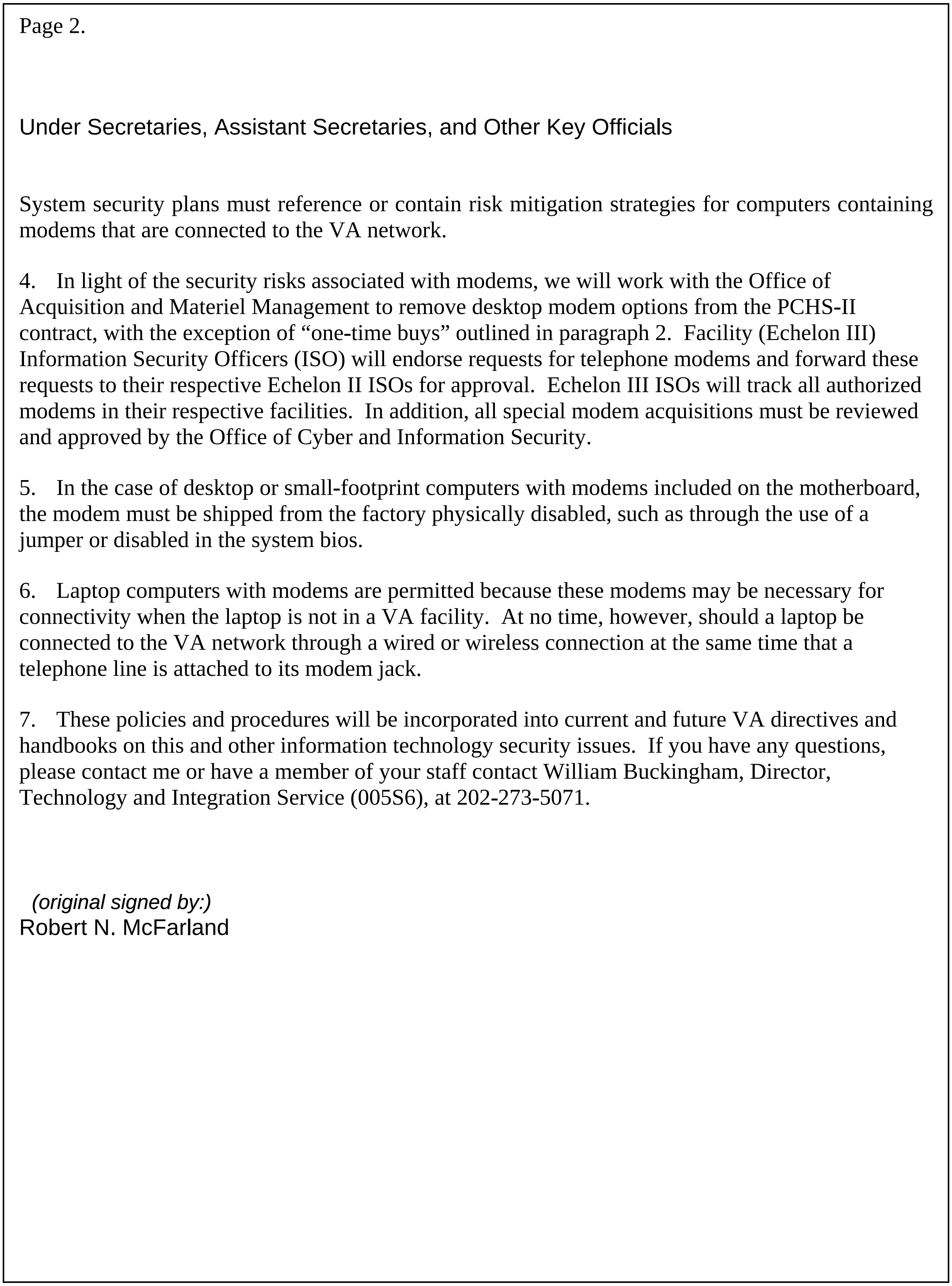
a. **Stand Alone -** The desktop computer is provided to a veterans rehabilitation center that lacks VA network connectivity, and the modem is used to provide an Internet connection for training purposes.

b. **Remote Access -** A telecommuter uses a VA-provided desktop computer at home where a telephone modem is used for dialup connection to the VA network.

c. **Medical Equipment -** The desktop computer is a component of medical equipment that is adequately segregated from the rest of the VA network on a virtual local area network (VLAN), and the modem is only used for required maintenance of the medical equipment. The telephone line should be disconnected from this computer except when maintenance is being performed.

3. There are still numerous desktop computers containing modems that are connected to the VA network where the use of modems is uncontrolled. Facility Directors are requested to review all desktop computers in their respective facilities and remove all resident modems unless they are specifically justified and a waiver has been granted. All desktop computers that contain modems should be tracked in accordance with existing Administration and staff office policies and procedures.

**Appendix A**



Page 2.

Under Secretaries, Assistant Secretaries, and Other Key Officials

System security plans must reference or contain risk mitigation strategies for computers containing modems that are connected to the VA network.

4. In light of the security risks associated with modems, we will work with the Office of Acquisition and Materiel Management to remove desktop modem options from the PCHS-II contract, with the exception of "one-time buys" outlined in paragraph 2. Facility (Echelon III) Information Security Officers (ISO) will endorse requests for telephone modems and forward these requests to their respective Echelon II ISOs for approval. Echelon III ISOs will track all authorized modems in their respective facilities. In addition, all special modem acquisitions must be reviewed and approved by the Office of Cyber and Information Security.

5. In the case of desktop or small-footprint computers with modems included on the motherboard, the modem must be shipped from the factory physically disabled, such as through the use of a jumper or disabled in the system bios.

6. Laptop computers with modems are permitted because these modems may be necessary for connectivity when the laptop is not in a VA facility. At no time, however, should a laptop be connected to the VA network through a wired or wireless connection at the same time that a telephone line is attached to its modem jack.

7. These policies and procedures will be incorporated into current and future VA directives and handbooks on this and other information technology security issues. If you have any questions, please contact me or have a member of your staff contact William Buckingham, Director, Technology and Integration Service (005S6), at 202-273-5071.

*(original signed by:)*
Robert N. McFarland

Appendix B

# OIG Contact and Staff Acknowledgments

| | |
|---|---|
| OIG Contact | Stephen Gaskell, Director, Central Office Operations Division (202-565-4098) |
| Acknowledgments | Michael Bravman, Project Manager<br>Ursula Johnson<br>Jeff McGowan<br>Tonya Shorts |

Appendix C

# Report Distribution

## VA Distribution

Secretary (00)
Deputy Secretary (001)
Executive Secretariat (001B)
Chief of Staff (00A)
Acting Under Secretary for Health (10B5)
Deputy Under Secretary for Health for Operations and Management (10N)
Assistant Secretary for Public and Intergovernmental Affairs (002)
Acting Assistant Secretary for Management (004)
Assistant Secretary for Information and Technology (005)
Assistant Secretary for Policy and Planning (008)
Acting Associate Deputy Assistant Secretary for Cyber and Information Security (005S)
Acting Associate Deputy Assistant Secretary for Acquisitions (049A)
Deputy Assistant Secretary for Congressional Affairs (009C)
General Counsel (02)
Office of the Medical Inspector (10M1)
Deputy Assistant Secretary for Public Affairs (80)
Director, Management and Financial Reports Service (047GB2)

## Non-VA Distribution

Office of Management and Budget
Government Accountability Office
Congressional Committees (Chairmen and Ranking Members):
Committee on Governmental Affairs, United States Senate
Committee on Veterans' Affairs, United States Senate
Committee on Appropriations, United States Senate
Subcommittee on VA, HUD, and Independent Agencies, Committee on Appropriations, United States Senate
Committee on Veterans' Affairs, United States House of Representatives
Committee on Appropriations, United States House of Representatives
Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, United States House of Representatives
Subcommittee on Benefits, Committee on Veterans' Affairs, United States House of Representatives
Subcommittee on VA, HUD, and Independent Agencies, Committee on Appropriations, United States House of Representatives
Staff Director, Committee on Veterans' Affairs, United States House of Representatives

Staff Director, Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, United States House of Representatives

This report will be available in the near future on the OIG's Web site at http://www.va.gov/oig/52/reports/mainlist.htm. This report will remain on the OIG Web site for at least 2 fiscal years after it is issued.