The Use of Personal Digital Assistants Poses Significant Security Risks

July 2004

Reference Number: 2004-20-126

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 16, 2004

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The Use of Personal Digital Assistants Poses Significant Security Risks (Audit # 200420021)

This report presents the results of our review of controls over Personal Digital Assistants (PDA). The overall objective of this review was to determine whether the Internal Revenue Service (IRS) had implemented effective policies and procedures to adequately control the purchase, distribution, and use of PDAs.

Since the early 1990s, PDAs have become increasingly popular due to their portability and computing capabilities. PDAs can perform many of the same functions as laptop computers, but they lack multiple security controls that are available for laptops and other computers. The portability of PDAs and their capacity to store sensitive data pose significant security risks for the IRS. To minimize the risks, the IRS requires that only PDAs certified as having adequate security capabilities be purchased and that the Chief Information Officer (CIO) approve all purchases.

In summary, the IRS has purchased 427 PDAs for key personnel who may be directly involved in ensuring the continuity of operations during an emergency. These PDAs encrypt data, were certified as secure, and were approved by the CIO.

However, the IRS has over 2,000 uncertified PDAs that can connect to the IRS network. Without the approval of the CIO, business units purchased the PDAs as a business tool for managers and employees to use while traveling. When synchronized to a network computer, the PDAs provide a backdoor into the network and bypass many of the existing security detection controls. Since these PDAs do not encrypt data, they could provide access to sensitive information, such as taxpayer data, if lost or stolen.

We could not account for the PDAs that had been purchased by the business units because the business units did not maintain inventories and distribution records for these devices. As an alternative, we used IRS software that scanned the network to

identify computers depicting PDA synchronization software. We tested 125 computers in 4 locations and found that several employees and contractors had installed unauthorized software to allow them to connect their personal PDAs to the IRS network. Some PDAs contained unencrypted sensitive information, such as step-by-step instructions for allowing access to large IRS databases containing taxpayer information and systems used to process travel vouchers.

Approximately 85 percent of the employees in our sample did not make use of the password feature available on their PDAs. In general, employees were not aware of the sensitivity of the information they had placed on their PDAs. None of the IRS employees in our sample had been provided any information regarding the risks of using PDAs and the controls necessary to reduce the risks.

We recommended the CIO establish firm procedures and time periods to either replace or upgrade PDAs with a solution certified by the Chief, Mission Assurance. Those PDAs that remain in use should be inventoried and monitored for compliance with security controls. We also recommended that the CIO continue to scan the network to identify and remove unauthorized synchronization software, and periodically remind employees and contractors of the risks associated with PDAs and the procedures they should take to minimize risk.

Management's Response: The CIO concurred with our recommendations and will implement actions to ensure PDAs connected to the IRS network are in compliance with appropriate security controls. The CIO will select a security package that has password and encryption capabilities and establish a process for removing or replacing all uncertified PDAs on the IRS network.

Also, the End User Equipment and Services (EUES) organization will conduct a semiannual scan of IRS networks to identify workstations that have synchronization software and issue a report identifying the users and their locations. A member of the EUES staff will be assigned the responsibility of removing all unauthorized synchronization software and uncertified PDAs from the IRS network. In addition, employees and contractors will be informed about the risks associated with PDAs and the prohibition against connecting personal equipment to the IRS Intranet and network. Management's complete response to the draft report is included as Appendix IV.

Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

The Use of Personal Digital Assistants Poses Significant Security Risks

Background

Since the early 1990s, the Personal Digital Assistant (PDA) has evolved from being a device of very limited function, compatibility, and capacity to being a highly functional extension of a user's desktop environment. Capacity, connection options, and processing power have all increased dramatically, while the applications and uses for PDAs are becoming increasingly complex. At the same time, decreasing prices and the increasing use of multifunction devices are helping fuel the rapid proliferation of PDAs.

In spite of their popularity and potential productivity benefits, PDAs pose risks to an organization's security. The very portability that makes a PDA so useful and attractive to its users threatens security. It increases the PDA's vulnerability to theft or loss and makes it a highly portable tool for circumventing security from within an organization. A study showed approximately 250,000 handheld devices were left behind or lost in United States airports in 2001.[1] Most of those devices likely contained information useful to hackers and others with no need to know proprietary information.

PDAs generally lack the security self-protection capabilities that are available for other computers, thereby causing concern over the protection of sensitive material downloaded to a PDA. When PDAs are purchased, user authentication is generally not enabled; if user authentication is enabled, it may be weak or easily circumvented. Also, information on PDAs is usually not automatically encrypted, making encryption the responsibility of the user.

PDAs that offer wireless communication capabilities generally increase the security risk to organizations. Wireless transmissions may be intercepted and, if inadequately encrypted, reveal their contents. The cellular capabilities of some recent PDAs are a significant reason for concern. PDAs could be connected to an organization's network or a desktop computer and at the same time be connected to some nonsecure network, providing an unsecured conduit into the organization by circumventing

[1] Richard Price, "The PDA as a Threat Vector," SANS Institute (March 2003).

the organization's firewall. In addition, viruses and other malicious software that attack the PDA itself are beginning to emerge and can be expected to proliferate as the PDA platform continues to become more compatible with, and connected to, more common target systems.

This review was performed at the Internal Revenue Service (IRS) National Headquarters in Washington D.C., and the IRS offices in New Carrollton, Maryland; New York, New York; and Oakland, California, during the period January through February 2004. We reviewed PDAs in the Wage and Investment, Small Business/ Self-Employed, Large and Mid-Size Business, and Tax Exempt and Government Entities Divisions and in the Agency-Wide Shared Services function.

The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

The Internal Revenue Service Has Purchased and Distributed Thousands of Uncertified Personal Digital Assistants

In May 2003, the Chief Information Officer (CIO) expressed concern over the proliferation of PDAs within the IRS, including both Federal Government and personally owned devices. The CIO believed actions were needed to establish control of the devices, manage the risks associated with them, and enforce existing security prohibitions. To minimize the risks, the IRS requires that only PDAs certified as having adequate security capabilities be purchased and that the CIO approve all purchases.

However, these procedures have not been effective in adequately controlling the use of PDAs. We noted the following conditions:

- Purchases of PDAs were not properly authorized.
- PDAs were not properly controlled and inventoried.
- Employees did not follow security procedures when using PDAs.

These conditions increase the risk that unauthorized persons could access the IRS network to disrupt operations or steal taxpayer information. Lost or stolen PDAs could also provide access to unencrypted sensitive information.

Purchases of PDAs were not properly authorized

The IRS permits the use of a PDA for any employee with a business reason, provided the PDA is certified, accredited, and capable of encrypting transmissions. The IRS has purchased 427 PDAs for key personnel who may be directly involved in ensuring the continuity of operations during an emergency. These PDAs provide real-time email capabilities, encrypt data, were certified as secure, and were approved by the CIO as required.

However, the CIO estimates the IRS has over 2,000 uncertified PDAs that can connect to the IRS network. Business units purchased the uncertified PDAs without the prior approval of the CIO and bypassed existing procedures to purchase PDAs for managers and employees to use while traveling. We found no documentation that business units assessed the security risks before purchasing the PDAs.

PDAs were not properly controlled and inventoried

We could not account for the PDAs that had been purchased by the business units because the business units did not maintain inventories and distribution records for these devices. IRS inventory analysts stated that the cost of individual PDAs was not considered substantial enough to warrant creation of a PDA inventory.

IRS procedures require that all sensitive equipment be inventoried, no matter the cost. Particularly because of their inherent risks, PDAs should have been inventoried regardless of costs.

Employees did not follow security procedures when using PDAs

We judgmentally selected 125 computers in 4 locations that had been identified as having PDA synchronization software.[2] We confirmed 88 employees had PDAs that were

[2] Without the availability of a valid inventory, the IRS used TIVOLI® software to scan the network and identified 2,565 computers with PDA synchronization software installed. While this technique was the only one available to locate PDAs, it was not accurate because the software can only scan computers connected to the network at the time of the scan.

used to access the IRS network.[3] Several of the PDAs we reviewed contained unencrypted sensitive but unclassified data. For example, four PDAs contained sensitive IRS data, such as step-by-step instructions for allowing access to large IRS databases containing taxpayer information and systems used to process travel vouchers. Another PDA stored a 100-page crisis communications plan that contained IRS employee and building information. Other PDAs included email attachments referencing a Limited Official Use Memorandum of Understanding and a CIO database.

In our sample, 75 (85 percent) of 88 employees did not make use of the password feature available on their PDAs. In addition, many employees were generally not aware of the sensitivity of the information, such as emails, that they had placed on their PDAs. We learned that IRS PDA users often set their PDA email function to automatically download their inbox to the unsecured PDA each time they connect to the network. This practice increased the risk that sensitive data could be inadvertently placed on the PDA.

We determined that, in addition to those PDAs purchased by the business units, employees and contractors had connected their personal PDAs to the IRS network. Twelve IRS employees or contractors were using personal PDAs, and five employees or contractors had installed their own synchronization software onto IRS computers. Three employees or contractors had computers with unauthorized wireless and/or cell phone software installed.

Also, we identified the following three potential integrity issues that will be referred to the Treasury Inspector General for Tax Administration Office of Investigations for further review:

[3] Although we sampled 125 computers, we confirmed that only 88 employees had PDAs. We believe the difference exists because employees could have returned their PDAs without removing the synchronization software, some employees may have never been issued a PDA, and synchronization software could have been removed after we selected our sample.

- A contractor had self-installed synchronization software onto his or her desktop to enable the contractor to use an unauthorized PDA with this computer. The synchronization log indicated the contractor had downloaded two pornographic Internet web sites onto the PDA. In addition, the contractor had installed unauthorized software on this desktop that allowed him or her to communicate outside the IRS network via a modem, a high-risk practice specifically prohibited by the IRS. A telephone line had been connected directly to this desktop computer, indicating the contractor may have used the modem.
- A contractor with synchronization software installed on his or her desktop claimed he or she never used the software. Upon review of the synchronization log, we noted synchronization occurred on September 3, 2003. The contractor stated he or she was on vacation at that time, left the PDA in the cradle, and did not know who used the desktop and synchronization software.
- One laptop was loaned out to an employee without removal of the synchronization software, providing the employee the opportunity to connect a personal PDA or other unauthorized device to the laptop.

Business units did not provide employees with guidance on how to use the PDAs in a secure manner. None of the IRS employees in our sample were given any information regarding the risks of using PDAs and the controls necessary to reduce the risks.

In December 2003, the CIO sent a draft memorandum to the business units reminding them of the security risks associated with PDAs and the need to protect sensitive data. The CIO encouraged business units to purchase the PDA currently certified for use if real-time email capabilities were required. For those employees not requiring that capability, the CIO indicated uncertified PDAs currently in use could continue to be used until a certified device could replace them. No specific procedures or time periods were provided for accomplishing these actions.

Recommendations

The CIO should:

1. Establish firm measures and time periods to either replace or upgrade PDAs with a solution certified by the Chief, Mission Assurance.

Management's Response: The CIO will select a security package with password and encryption capabilities and establish a process (including measures and time periods) for removing or replacing existing PDAs on the network that are not certified.

2. Inventory and monitor all PDAs in use for compliance with security controls.

Management's Response: The Director, End User Equipment and Services (EUES), has assigned a Contracting Officer's Technical Representative to inventory all PDAs now in use. The EUES organization will scan the network to confirm that all PDAs connected to the network comply with security controls.

3. Continue to scan the network to identify computers with synchronization software and follow up to determine whether personal PDAs are being used. Unauthorized synchronization software should be removed from networked computers.

Management's Response: The EUES organization will conduct a semiannual scan of the IRS networks, identify the workstations that have synchronization software, and issue a report that matches the assigned user and location of the workstation. The report will be distributed to the EUES organization Area Directors, who will designate a staff member to take appropriate action to remove all unauthorized synchronization software and wireless devices from the network.

4. Periodically remind employees and contractors that connecting personal equipment, such as PDAs, to the IRS network is prohibited.

Management's Response: The Modernization and Information Technology Services organization will inform employees and contractors, when it provides initial service,

that connecting personal equipment to the IRS Intranet and network is prohibited. In addition, the Director of Assurance Programs in the Office of Mission Assurance incorporated PDA training in the Annual Security Awareness Program for Calendar Year 2004, advising employees that connecting personal equipment such as PDAs to the IRS network is prohibited. This is ongoing training that was scheduled to begin in late June 2004. The Director of Assurance Programs will also coordinate with the Procurement function in the Agency-Wide Shared Services organization to identify the means to effectively communicate reminders to contractors that connecting personal equipment, such as PDAs, to the IRS network is prohibited.

5. Provide training to those employees with authorized PDAs and advise them of the risks associated with PDAs. The training should address the need for using passwords and encrypting sensitive data.

Management's Response: The EUES organization will inform employees about the risks associated with PDAs when it provides them with initial service. Also, the Director of Assurance Programs has incorporated PDA training in the Annual Security Awareness Program for Calendar Year 2004. The training advises employees of the associated risks and the need for using passwords and encrypting sensitive data. Training was scheduled to begin in late June 2004.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) had implemented effective policies and procedures to adequately control the purchase, distribution, and use of Personal Digital Assistants (PDA).

I. To determine whether IRS management had established sufficient policies, procedures, and guidelines to ensure PDAs were used in a secure manner, we:

A. Reviewed all current policies and procedures to determine whether there were specific criteria and standards for the use of PDAs and whether security controls pertaining to sensitive but unclassified information and emails were adequate.

B. Evaluated the types of security risks PDA use poses to the IRS network.

C. Using TIVOLI® software to scan the IRS network, identified a population of 2,565 computers with PDA synchronization software installed and judgmentally selected 4 IRS offices (sites) based on which locations had among the highest numbers of computers with PDA software. We chose a judgmental sample for efficiency and because we did not plan to project results. The four sites selected were IRS Headquarters, Washington, D.C.; New Carrollton, Maryland; New York, New York; and Oakland, California.

D. Interviewed End User Equipment and Services organization and Modernization and Information Technology Services (MITS) organization Territory Managers at the four sites to determine whether requirements for the use of PDAs were disseminated to PDA users and whether PDA users had been provided training on the reduction of risks relative to PDAs.

E. Judgmentally selected 30 computers at 3 sites and 35 at a fourth site, for a total of 125 computers, from the 2,565 computers identified by the TIVOLI® software and confirmed that 88 of those employees and contractors still had PDAs. We interviewed the 88 PDA users identified by the TIVOLI® scan at the 4 sites to determine how they used PDAs and what information they stored on their PDAs. We also evaluated their PDAs, synchronization software, and logs to determine what PDA functions were used and whether sensitive but unclassified information was stored on the PDAs.

II. To determine whether controls were adequate to account for all PDAs received and distributed, we:

A. Interviewed MITS organization management and inventory analysts to determine procedures and policies for tracking PDAs.

B. Evaluated any available documentation for purchasing, tracking, or accounting for PDA use.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald H. Horn, Audit Manager
Jody L. Kitazono, Senior Auditor
Abraham Millado, Senior Auditor
William Simmons, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief, Mission Assurance OS:MA
Acting Director, Portfolio Management OS:CIO:R:PM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Management Controls OS:CFO:AR:M
Audit Liaisons:
    Chief Information Officer OS:CIO:M
    Chief, Mission Assurance OS:MA

Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATIC N OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
JUL 07 2004

July 6, 2004

MEMOF ANDUM FOR ACTING DEPUTY INSPECTOR FOR AUDIT

FROM: W. Todd Grams
Chief Information Officer

SUBJE CT: Management Response to Draft Audit Report – The Use of Personal Digital Assistants Poses Significant Security Risks (Audit # 200420021) – ECMS # 0405-5Z5LV3BL

Thank ou for the opportunity to comment on your draft audit concerning the security risks of Personal Digital Assistants (PDAs) and Personal Electronic Devices (PEDs). Based on your audit findings, and subsequent discussions with my staff and other officials in the Internal Revenue Service (IRS), it is clear that we must take a more aggres ive approach to the management of PDAs/PEDs.

To that end, this week I will issue a memorandum that:

- Reminds all employees of their roles in ensuring that PDAs are operated with a minimal level of risk to the IRS.
- Announces our transition plan for securing all PDAs across the agency.

Our ne w approach:

- Was developed in close consultation with the Office of Mission Assurance and the IRS Business Units (the Business Units are the chief owners and beneficiaries of the PDAs).
- Balances the need to meet Business Unit demands for the benefits of PDAs while minimizing security risks to the agency.
- Reflects all of your recommendations.

Detail s of our approach are provided in the attached management response. Thank you a ain for the opportunity to comment on your draft audit.

None of the material in the draft report warrants protection under the Freedom of Inform ation Act or other applicable laws.

If you h ıve questions, please call me at (202) 622-6800, or a member of your staff may call Thc nas Mulcahy, Manger, Program Oversight Office, at (202) 283-6063.

Attachn ent

MITS END USER EQUIPMENT & SERVICES and MISSION ASSURANCE
Corrective Actions in Response to Draft Audit Report –
Use of PDAs Poses Significant Security Risks
(Audit # 200420021)

IDENTITY OF RECOMMENDATION #1

The Chief Information Officer (CIO) should establish firm measures and time periods to either replace or upgrade PDAs with a solution certified by the Chief, Mission Assurance.

CORRECTIVE ACTION #1
The CIO will select a security package with password and encryption capabilities, and establish a process (including measures and time periods) for removing or replacing existing PDAs on the network that are not certified.

IMPLEMENTATION DATE:

COMPLETED _____ **PROPOSED** ~~February 1, 2005~~

RESPONSIBLE OFFICIAL(S)

Chief Information Officer
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRECTIVE ACTION MONITORING PLAN #1

Point of-Contact: Peggy Gladwell, Chief, Technical Services (EUES)

MI TS END USER EQUIPMENT & SERVICES and MISSION ASSURANCE
Corrective Actions in Response to Draft Audit Report –
Use of PDAs Poses Significant Security Risks
(Audit # 200420021)

IDENTI Y OF RECOMMENDATION #2

The CIC should inventory and monitor all PDAs in use for compliance with security controls

CORRE CTIVE ACTION #2
The Dir ctor, End User Equipment, and Services (EUES), has assigned a Contracting Officer's Technical Representative (COTR) to inventory all PDAs now in use. EUES will scan the network to confirm that all PDAs connected to the network comply with security controls (see corrective action #3 for details)

IMPLE IENTATION DATE:

COMPL ETED _____ **PROPOSED** November 1, 2004

RESPC NSIBLE OFFICIAL(S)

Chief Information Officer
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRE CTIVE ACTION MONITORING PLAN #2

Points- of-Contact:
Phil Sharp, Chief Asset Management. – monitor inventory status
Allan Roberts, Acting Chief, Enterprise Systems Management – scans the network
Marci Metzner, Acting Chief, Data Security Operations – security controls

MI TS END USER EQUIPMENT & SERVICES and MISSION ASSURANCE
Corrective Actions in Response to Draft Audit Report –
Use of PDAs Poses Significant Security Risks
(Audit # 200420021)

IDENTI1 Y OF RECOMMENDATION #3

The CIC should continue to scan the network to identify computers with synchronization software and follow up to determine whether personal PDAs are being used. Unauthc rized synchronization software should be removed from networked computers.

CORRE CTIVE ACTION #3
EUES w ill conduct a semi-annual scan of the IRS networks, identify the workstations that hav e synchronization software, and issue a report that matches the assigned user and thei location to the workstation. The report will be distributed to the Acting Director EUES' direct reports (Area Directors) who will designate a member of his or her staff to take appropriate action to remove all unauthorized synchronization software and wire less devices from the network.

IMPLEM IENTATION DATE:

COMPL ETED _____ **PROPOSED** September 1, 2004

RESPC NSIBLE OFFICIAL(S)

Chief In ormation Officer
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRE CTIVE ACTION MONITORING PLAN #3

Point-o -Contact: Allan Roberts, Acting Chief (ESM)

MI TS END USER EQUIPMENT & SERVICES and MISSION ASSURANCE
Corrective Actions in Response to Draft Audit Report –
Use of PDAs Poses Significant Security Risks
(Audit # 200420021)

IDENTI Y OF RECOMMENDATION #4

The CIC should periodically remind employees and contractors that connecting persona equipment, such as PDAs, to the IRS network is prohibited.

CORRE CTIVE ACTION #4a
MITS w l inform employees and contractors that connecting personal equipment to the IRS intr net and network is prohibited when they provide initial service.

IMPLEI IENTATION DATE:

COMPL ETED _____ **PROPOSED** ~~October 1, 2004 (EUES)~~

RESPC NSIBLE OFFICIAL(S)

Chief In ormation Officer
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRE CTIVE ACTION MONITORING PLAN #4a

Point-o -Contact: Ric Grau, Chief, Training Project Office

CORRE CTIVE ACTION # 4b
The Dir ector of Assurance Programs, Mission Assurance, incorporated training on PDAs i the Annual Security Awareness Program for calendar year 2004 advising employ ees that connecting personal equipment, such as PDAs, to the IRS network is prohibi ed. This is on-going training. This training is to begin in late June 2004.

IMPLE MENTATION DATE:

COMP ETED **PROPOSED** **July 15, 2004**

RESPC NSIBLE OFFICIAL(S)

Chief, I Mission Assurance
Director, Assurance Programs (OS:MA:AP)

MI TS END USER EQUIPMENT & SERVICES and MISSION ASSURANCE
Corrective Actions in Response to Draft Audit Report –
Use of PDAs Poses Significant Security Risks
(Audit # 200420021)

CORRE CTIVE ACTION MONITORING PLAN #4b

Corr ctive action will be completed within 30 days.

CORRE CTIVE ACTION # 4c
The Dir ctor of Assurance Programs, Mission Assurance, will coordinate with Procure nent, Agency-Wide Shared Services, to identify the means to effectively commu icate reminders to contractors that connecting personal equipment, such as PDAs, t the IRS network is prohibited.

IMPLE IENTATION DATE:

COMPL ETED **PROPOSED** December 15, 2004

RESPC NSIBLE OFFICIAL(S)

Chie f, Mission Assurance
I irector, Assurance Programs (OS:MA:AP)

CORRE CTIVE ACTION MONITORING PLAN #4c

The corrective action will be monitored on a monthly basis until completed.

MITS END USER EQUIPMENT & SERVICES and MISSION ASSURANCE
Corrective Actions in Response to Draft Audit Report –
Use of PDAs Poses Significant Security Risks
(Audit # 200420021)

IDENTITY OF RECOMMENDATION #5

The CIO should provide training to those employees with authorized PDAs, and advise them of the risks associated with PDAs. The training should address the need for using passwords and encrypting sensitive data.

CORRECTIVE ACTION #5a
EUES will inform employees about the risks associated with PDAs, when they provide them with initial service. (Mission Assurance will provide employees periodic reminders and refresher training on risks as described in Corrective Action # 5b).

IMPLEMENTATION DATE:

COMPLETED _____ **PROPOSED** October 1, 2004

RESPONSIBLE OFFICIAL(S)

Chief Information Officer
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRECTIVE ACTION MONITORING PLAN

Point-of Contact: Ric Grau, Chief, Training Project Office

MITS END USER EQUIPMENT & SERVICES and MISSION ASSURANCE
Corrective Actions in Response to Draft Audit Report –
Use of PDAs Poses Significant Security Risks
(Audit # 200420021)

CORRECTIVE ACTION #5b

The Director of Assurance Program, Mission Assurance, has incorporated training on PDAs in the Annual Security Awareness Program for calendar year 2004. The training advises employees of the associated risks and the need for using password and encrypting sensitive data. Training is to begin in late June 2004.

IMPLEMENTATION DATE:

COMPLETED **PROPOSED** July 15, 2004

RESPONSIBLE OFFICIAL(S)

Chief, Mission Assurance
Director, Assurance Programs (OS:MA:AP)

CORRECTIVE ACTION MONITORING PLAN

Corrective action will be completed within 30 days. Training is reviewed annually.