A Comprehensive Program for Preventing and Detecting Computer Viruses Is Needed

June 2000

Reference Number: 2000-20-094

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 14, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - A Comprehensive Program for Preventing and Detecting Computer Viruses Is Needed

This report presents the results of our review of the Internal Revenue Service's (IRS) program for preventing and detecting the spread of computer viruses. In summary, we found that the IRS does not have an effective program for preventing and detecting computer viruses. We recommended that the Chief Information Officer designate a senior official to be responsible for managing the IRS virus prevention program and overseeing its effective implementation. The responsible official needs to focus on (1) developing effective procedures for keeping anti-virus software current, (2) establishing controls for ensuring all updates have been successfully accomplished, (3) creating a system for gathering information for evaluating the program, (4) ensuring that virus incident reports are prepared, and (5) preparing plans for responding quickly and effectively to major computer virus outbreaks.

IRS management agreed with our recommendations. Their written response discusses several corrective actions that will improve the reported conditions. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

Copies of this report are being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions, or your staff may call Scott Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Executive Summary

Computer viruses are malicious programs designed to spread unauthorized, visible, and sometimes destructive functions throughout information systems and networks. The likelihood of an organization experiencing a computer virus is increasing tremendously, with newer viruses being more complex and difficult to detect. Statistics on the extent and impact of viruses within the Internal Revenue Service (IRS) were not available because the IRS did not have a system for tracking such data. However, we estimated the possible annual cost to the IRS of responding to and cleaning up viruses, and the negative impact on productivity caused by computer down time, could be at least $500,000, and up to $11.5 million, based on data from industry sources.

The overall objective of this review was to determine if the IRS had an effective program for preventing and detecting the spread of computer viruses.

Results

The IRS does not have an effective program for preventing and detecting computer viruses. As a result, viruses have gone unchecked and undetected. The IRS continued to spread the Melissa virus almost a year after it was first detected. The Melissa virus propagates in the form of an e-mail message containing an infected Word document as an attachment. The following deficiencies occurred as a result of inadequate virus protection management.

Anti-virus Software Was Not Current and Operating Properly on Internal Revenue Service Computers

Computers were inadequately protected against viruses. Anti-virus software was either not operating properly or did not have recent updates on many computers we tested. The IRS lacked effective procedures for keeping software current and ensuring that updates were successfully installed. During our January through March 2000 testing, we found many computers that had not received the updates necessary to detect the Melissa virus.

The Internal Revenue Service Lacks Data for Measuring the Effectiveness of Its Virus Protection Activities

The IRS did not compile information needed for evaluating trends, problems, and the overall effectiveness of its virus prevention activities. For example, the IRS did not have statistics on how often computers became infected with viruses or detected viruses. The IRS did not track the cost of infections, such as lost productivity and clean-up time, that

would be useful in understanding the full magnitude of virus protection and the need for additional resources. IRS management believed that required virus incident reports were rarely prepared when infections occurred.

The Internal Revenue Service Does Not Have a Formal Response Capability for Resolving Major Computer Virus Outbreaks

The IRS was not adequately prepared to respond to major computer virus outbreaks. It did not have a coordinated virus response plan setting forth the procedures and mechanisms to be put in place, such as how to seek technical assistance or disseminate alerts throughout the organization. A response team had not been formed.

Summary of Recommendations

We recommended that the Chief Information Officer designate a senior official to be responsible for managing the IRS virus prevention program and overseeing its effective implementation. The responsible official needs to focus on (1) developing effective procedures for keeping anti-virus software current on both networked and portable notebook computers, (2) establishing controls for ensuring all updates have been successfully accomplished, (3) creating a system for gathering information for evaluating the program, (4) ensuring that virus incident reports are prepared, and (5) preparing plans for responding quickly and effectively to major computer virus outbreaks.

Management's Response: IRS management agreed with our findings and recommendations and has assigned responsibility for directing and overseeing the implementation and effectiveness of virus protection efforts to a senior level executive. Their response details the responsibilities of that executive to include developing procedures and controls for updating virus software, program evaluation, incident report preparation, and the formation of an effective response capability to future virus attacks.

Management’s complete response to the draft report is included as Appendix IV.

Objective and Scope

Our objective was to determine if the IRS had an effective computer virus prevention program.

Our overall objective was to determine if the Internal Revenue Service (IRS) had an effective program for preventing and detecting the spread of computer viruses. To accomplish this objective, we reviewed requirements, procedures, and guidelines for (1) keeping anti-virus software current on servers and workstations, (2) formulating contingency plans for when virus outbreaks occur, including disseminating warnings and advice when new viruses are discovered, and (3) overseeing the virus protection program.

Our work included:

1. Reviewing virus program requirements and guidance in the Computer Security Act of 1987,[1] the Internal Revenue Manual (IRM), IRS' Information Systems Security Procedural Guide, and documents issued by the Office of Management and Budget, Department of the Treasury, and National Institute of Standards and Technology.
2. Reviewing virus program guidance issued by private sector industry sources.
3. Interviewing officials, management, and staff responsible for managing and overseeing computer security, and obtaining national and local virus program procedures.
4. Reviewing IRS virus communications and computer virus incident reports.
5. Testing a sample of servers and workstations to determine whether anti-virus software was properly operating and contained recent anti-virus software updates.

Our audit work was performed at the IRS' National Office and two area offices belonging to IRS'

[1] The Computer Security Act of 1987, Pub. L. No. 100-235

Information Systems (IS) organization between December 1999 and March 2000, in accordance with *Government Auditing Standards*. Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

Computer viruses are a serious threat to computer systems.

Computer viruses, malicious programs designed to spread unauthorized, visible, and sometimes destructive functions throughout information systems and networks, pose a serious and increasing threat to computer systems. The probability of an organization experiencing a computer virus has approximately doubled in each of the last four years, according to ICSA.net, an Internet security assurance services firm. Along with this growth has been the creation of more complex viruses that are increasingly difficult to detect. Some viruses are capable of causing major damage such as system crashes, corruption of file systems, and extensive loss of data. However, the most costly aspect of viruses is not the direct damage they may inflict but the cost of responding to and cleaning up viruses and the negative impact on productivity caused by computer down time. Aside from the dollar impact, organizations that spread viruses could have their credibility seriously damaged.

ICSA.net recently reported that viruses were expected to cost U.S. companies over $2 billion in 1999. It also recently reported that the Melissa virus, one of the fastest growing viruses ever detected, cost North American businesses between an estimated $93 and $385 million in actual damages during the 1 week following its release and infected more than 1 million personal computers in North America. The Melissa virus propagates in the form of an e-mail message containing an infected Word document as an attachment. Statistics on the extent and cost impact of viruses within the IRS were not available because the IRS did not have

a system in place for tracking such data. However, based on data from a recent virus survey performed by ICSA.net, the cost of virus infections to a large organization similar to the IRS could possibly be at least $500,000, and up to $11.5 million, annually.

Results

The IRS does not have an effective program for preventing and detecting computer viruses. Anti-virus software was not current or operating properly on IRS computers. The IRS lacked data for monitoring virus prevention activities. And, the IRS does not have a formal plan to respond to virus outbreaks.

As a result, viruses can go unchecked and undetected. For example, the IRS continued to spread the Melissa virus almost a year after the virus was first discovered. The deficiencies we found occurred because the IRS did not centrally direct and oversee virus prevention efforts. Accountability had not been assigned to an executive or senior manager. We believe that our recommendations, in conjunction with the centralization of information system activities currently underway, should enable management to more effectively administer virus prevention and detection efforts.

Anti-virus Software Was Not Current and Operating Properly on Internal Revenue Service Computers

We found anti-virus protection deficient on a significant number of computers tested.

Our tests of computers at four major IRS locations found a significant number of servers and workstations inadequately protected against computer viruses. The anti-virus protection on these computers was not operating properly and not kept current with the latest updates, making the computers vulnerable to becoming infected with and spreading viruses. The IRM requires that computers be properly protected with IRS approved

anti-virus software and that the software be kept current with the latest software updates.

We randomly tested a total of 183 computers consisting of 52 servers and 131 workstations. Anti-virus protection on 56 percent of them was inadequate to guard against viruses. These deficiencies are listed below. The total of these items represents more than 56 percent because some computers were deficient in more than 1 category.

- There were 55 computers (30 percent) with outdated virus scan engines; 87 percent of these 55 outdated scan engines were incapable of detecting the Melissa virus.[2] The scan engine is the part of the software application that searches for the presence of viruses.
- There were 49 computers (27 percent) that had not received updates for detecting new viruses in at least 4 weeks. Industry sources commonly recommend that updates for detecting new viruses be installed at least that often. These files provide information to the scan engine enabling it to detect specific viruses.
- There were 29 computers (16 percent) that did not have the latest version of the anti-virus software application.
- There were 19 computers (10 percent) that either did not have anti-virus software installed or did not have the software turned on.
- There were 16 computers (9 percent) not using the virus warning capabilities of their word processing software.

The IRS lacked effective procedures for ensuring the successful updating of anti-virus software.

The IRM contains requirements for updating anti-virus software. However, it does not specify how often software should be updated and does not contain formal procedures for implementing software updates. Without updates, anti-virus software is not able to detect newly

[2] The Melissa virus was discovered on March 26, 1999, and is considered one of the fastest spreading viruses ever created.

created viruses. The methods used to update anti-virus software differed at the two IS area offices we reviewed, but neither was successful at keeping the software properly running and sufficiently updated to adequately guard against viruses.

One IS area office used the automatic update feature of the anti-virus software, which routinely loads updates from a specified file location on a specified day and time. However, we found that the automatic update settings were incorrect in many of the exceptions we cited above. The other IS area office updated servers by using technicians to individually load updates to each of the servers. That office also used a software program to install updates simultaneously to large groups of workstations from a remote computer. However, problems with the settings and the operation of these methods were present in many of the exceptions we cited above.

The IRS also did not have a process for updating anti-virus software on notebook computers. Such computers may not be connected to a network and can not be updated using the procedures described above. We tested four notebook computers, all of which were not being updated. Employees indicated that they received new notebook computers without any instructions on how to update the anti-virus software.

To properly manage risks, procedures need to be in place for ensuring that virus protection is implemented effectively and remains effective over time. The IRS did not require that spot checks or other methods of verification be performed to confirm that updates were being achieved as intended.

The Internal Revenue Service Lacks Data for Measuring the Effectiveness of Its Virus Protection Activities

The IRS lacks data for monitoring the effectiveness of its virus activity.

The IRS does not compile information summarizing its virus detection activity. For example, officials told us they do not collect statistics on the number of times their computers have become infected with viruses or have detected viruses. Without the recording of such information, the IRS does not have data for evaluating trends, problems, resource needs, and the overall effectiveness of its virus detection activities.

The IRM contains one virus-related reporting requirement. It requires that a Virus Incident Report be prepared when a virus incident occurs. Some of the key information captured in this report includes (1) how the virus was acquired, (2) whether safeguards in place were adequate, and (3) whether additional safeguards were needed. These reports could provide a basis for:

- Monitoring the volume of virus activity.
- Identifying weaknesses in IRS virus prevention activities.
- Formulating corrective actions to strengthen virus protection.
- Determining whether corrective actions to strengthen virus protection have a positive effect in reducing further infection.

For example, several Virus Incident Reports prepared between April and November 1999 indicated that workstations became infected because they were not using the latest virus detection updates, an indication that the updating process might not be performing successfully. Outdated virus detection updates was the second most common deficiency we found in our tests.

IS management told us that no analysis of Virus Incident Reports was done and that they believed that these reports were rarely prepared, thereby limiting the usefulness of the data.

The Internal Revenue Service Does Not Have a Formal Response Capability for Resolving Major Computer Virus Outbreaks

The IRS lacks a formal response capacity for responding to major outbreaks of viruses.

We found that the IRS was not adequately prepared to respond to major computer virus outbreaks. While the IRM contains procedures for isolating, identifying, eradicating, and reporting viruses, it does not address how other important virus response activities are to be coordinated and carried out, such as how information on newly reported viruses is to be disseminated to management and users. Officials from the IRS National Office and two IS area offices told us that an emergency response plan to deal specifically with major virus outbreaks did not exist. A planned response capability is needed for reacting quickly when major computer virus outbreaks occur. Without such formal response capability, viruses can seriously affect operations and be costly.

A planned and coordinated virus response capability generally consists of a designated response team with the particular skills and broad range of experience needed to take control of a major virus outbreak. The team takes responsibility for the overall management and resolution of the outbreak by having procedures and mechanisms in place to:

- Determine why the virus is spreading and formulate the corrective actions needed to stop it.
- Disseminate virus alerts to management and users.
- Alert key agency directors and notify computer security, information systems, data processing, legal, public affairs, and law enforcement officials.
- Obtain technical assistance from vendors and investigative agencies.
- Deal with media inquiries.

Recommendations

We recommend that:

1. The IRS Chief Information Officer formally assign to a senior official the responsibility for directing and overseeing the implementation and effectiveness of the IRS' virus prevention efforts.
2. The official responsible for the virus program should develop and implement IRS-wide procedures detailing the frequency and steps to be followed for reliably updating anti-virus software on both networked and portable notebook computers.
3. The official responsible for the virus program should establish controls for ensuring all updates have been successfully accomplished.
4. The official responsible for the virus program should develop a system for gathering information to help analyze and monitor the effectiveness of the program's virus detection and prevention activities.
5. The official responsible for the virus program should strengthen procedures for ensuring that employees comply with the IRM requirements for preparing Virus Incident Reports.
6. The official responsible for the virus program should form a virus response team and develop procedures for the various activities that need to be quickly coordinated and carried out when major virus outbreaks occur.

Management's Response: Management assigned responsibility for directing and overseeing the implementation and effectiveness of the IRS' virus prevention efforts to the Director, Telecommunications. That individual's responsibilities will include:

1. Coordinating with the Program Manager for Tier 3 Operations (personal computers and networks) to develop and implement procedures for updating anti-virus software on both networked and portable notebook computers.

2. Establishing controls for ensuring all updates have been successfully accomplished.
3. Developing a monitoring system to ensure the effectiveness of the program's virus detection and prevention activities.
4. Strengthening procedures to ensure compliance with requirements for preparing Virus Incident Reports.
5. Forming a virus response team to effectively respond to virus attacks.

Conclusion

Effective virus prevention efforts are needed to guard computer systems against the serious and rapidly growing threats posed by viruses. The IRS has likely spent large amounts in responding to virus outbreaks and can expect to spend much more, unless accountability for virus prevention and detection is established and more emphasis is placed on this program.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to determine if the Internal Revenue Service (IRS) had an effective program for preventing and detecting the spread of computer viruses. To accomplish this objective, we:

I. Determined whether the IRS had effective requirements, procedures, and guidelines for keeping anti-virus software current on its servers and workstations and for making sure that updates were successfully installed.

A. Reviewed the Internal Revenue Manual (IRM), Information Systems Security Procedural Guide, and the Department of the Treasury Security Manual for sections related to keeping anti-virus software current and ensuring that such updates are successfully installed.

B. Reviewed computer security reference material issued by the U.S. General Accounting Office, the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), ICSA.net, and others to determine their recommended virus prevention policies and practices.

C. Interviewed Information Systems (IS) security management and staff from two IS area offices, and a security oversight official in the IRS National Office to determine their procedures for updating anti-virus software on networked, non-networked, and notebook computers. Obtained copies of their written instructions and guidelines.

D. Interviewed IS security management and staff from two IS area offices and a security oversight official in the IRS National Office to determine how management ensures that anti-virus updates have been successfully installed on all workstations and servers. Obtained copies of their written instructions and guidelines.

E. Determined whether operational reviews found instances in which anti-virus software was not updated.

F. Tested anti-virus software updating procedures by checking the software on a sample of servers and workstations at four major sites within two IS area offices between January and March 2000. We reviewed a total of 183 computers at these four locations by randomly selecting servers and workstations throughout the office building. We considered a computer to have inadequate virus protection if (1) it did not have the latest software version that the IRS was using, (2) its virus detection files had not been updated in at least four weeks, (3) it did not have anti-virus software installed or it was not turned on, or (4) the virus warning built into word processing software was not turned on.

II. Determined whether the IRS had adequate contingency plans for responding to virus outbreaks/infections, including procedures for disseminating warnings when new viruses are discovered.

A. Reviewed the IRM, Information Systems Security Procedural Guide, and Department of the Treasury Security Manual for sections pertaining to virus contingency plans and the reporting/dissemination of information on newly discovered viruses.

B. Reviewed OMB and NIST reference materials to determine recommended practices for virus contingency planning and the reporting/dissemination of information on new viruses.

C. Interviewed IS security management and staff from two IS area offices and a security oversight official in the IRS National Office about their virus contingency plans and procedures for reporting/disseminating information on newly discovered viruses.

D. Obtained copies of communications that had been issued on newly discovered viruses.

III. Determined how virus prevention activities were managed and overseen.

A. Reviewed the IRM, Information Systems Security Procedural Guide, and Department of the Treasury Security Manual for sections covering how virus activities should be managed and monitored, such as those pertaining to management information, reporting, and operational reviews.

B. Reviewed OMB and NIST reference materials to determine recommended ways to manage and evaluate virus prevention programs, such as the collection of data and reports.

C. Interviewed IS security management and staff from two IS area offices and a security oversight official in the IRS National Office to determine their roles and responsibilities in managing and overseeing virus prevention activities and the organizational chain of command over virus protection activities.

D. Interviewed IS security management and staff from two IS area offices and a security oversight official in the IRS National Office to determine how they manage and oversee virus prevention activities and if they have reports, data, tables, reviews, or other documentation that were used to oversee and track virus prevention activities.

Appendix II

Major Contributors to This Report

Scott Wilson, Associate Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald Horn, Audit Manager
Richard Borst, Senior Auditor
Charles Ekholm, Auditor
Midori Ohno, Auditor

Appendix III

Report Distribution List

Chief Information Officer IS
Director, Office of Security and Privacy Oversight IS:SPO
Director, Security, Evaluation and Oversight IS:SPO:S

Appendix IV

Management's Response to the Draft Report

COMMISSIONER

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

May 30, 2000

MEMORANDUM FOR TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

FROM: for Charles O. Rossotti
Commissioner of Internal Revenue

SUBJECT: Response to Draft Audit Report – A Comprehensive Program for Preventing and Detecting Computer Viruses is Needed

Thank you for the opportunity to comment on your draft report and recommendations concerning further work needed by the Internal Revenue Service to establish a comprehensive program for preventing and detecting computer viruses. In reviewing your draft report, we generally agree with its findings and recommendations.

Protecting systems resources and records from harm by computer viruses is a top priority for the IRS. We continue to improve our virus prevention, detection, and reaction capabilities.

Since the Melissa virus a year ago, the IRS has made substantial progress. This was demonstrated on May 8, 2000 when we encountered the destructive LoveBug virus that affected computer systems throughout the world. Even though the IRS received over 8 million virus-bearing e-mails, our staff minimized the impact on operations by standing up a nationwide coordination center, shutting down systems to contain the virus, installing new software to cleanse the virus, and telling all users to delete infected messages and not open attachments. Other factors that enabled us to be successful were earlier infrastructure initiatives to (1) convert to a single e-mail system with a standard configuration, (2) establish an automated distribution capability, and (3) centralize and reduce our e-mail servers from 800 to 180.

Attached are our comments. This letter, attachment, and your draft report are designated as "LIMITED OFFICIAL USE" documents because of the sensitive weaknesses and vulnerabilities addressed. In this regard, they should be

restricted to only officials with a "need to know" and should not be released publicly.

If you have any questions, please contact Toni Zimmerman, Deputy CIO (Operations), at 202-622-0260 or have a member of your staff contact Al Whitley, Director, Telecommunications at 202-283-0990.

Attachment

Attachment

MANAGEMENT RESPONSE TO DRAFT AUDIT REPORT – A COMPREHENSIVE PROGRAM FOR PREVENTING AND DETECTING COMPUTER VIRUSES IS NEEDED

Recommendation #1

The IRS Chief Information Officer formally assign, to a senior official, the responsibility for directing and overseeing the implementation and effectiveness of the IRS' virus prevention efforts.

Assessment of Cause

IS needs to make a senior official in IS Operations responsible for directing and overseeing the implementation and effectiveness of the IRS' virus prevention efforts.

Corrective Action #1

The responsibility for directing and overseeing the implementation and effectiveness of the IRS' virus prevention efforts has been assigned to the Director, Telecommunications. He will designate this to a senior manager who will have it as his/her primary responsibility by July 1, 2000.

Implementation Date of Corrective Action #1

Completed	Proposed
	1 July 2000

Responsible Officials for Corrective Action #1

Director, Telecommunications

Corrective Action #1 Monitoring Plan

IS will track the progress of this corrective action through a series of weekly meetings.

1

MANAGEMENT RESPONSE TO DRAFT AUDIT REPORT – A COMPREHENSIVE PROGRAM FOR PREVENTING AND DETECTING COMPUTER VIRUSES IS NEEDED

Recommendation #2

The official responsible for the virus program should develop and implement IRS-wide procedures detailing the frequency and steps to be followed for reliably updating anti-virus software on both networked and portable notebook computers.

Assessment of Cause

The IRS lacks standard service-wide procedures detailing the frequency and steps to be followed for reliably updating anti-virus software on both networked and portable notebook computers.

Corrective Action #2

The Program Manager for Tier 3 Operations will, by 31 December 2000, develop and implement IRS-wide procedures detailing the frequency and steps to be followed for reliably updating anti-virus software on both networked and portable notebook computers. These procedures will be coordinated with the official responsible for the virus program.

Implementation Date of Corrective Action #2

Completed	**Proposed**
	31 December 2000

Responsible Officials for Corrective Action #2

Chief Information Officer IS
Deputy Chief Information Officer (Operations) IS
Director, IS Field Operations

Corrective Action #2 Monitoring Plan

Same as recommendation #1

MANAGEMENT RESPONSE TO DRAFT AUDIT REPORT – A COMPREHENSIVE PROGRAM FOR PREVENTING AND DETECTING COMPUTER VIRUSES IS NEEDED

Recommendation #3

The official responsible for the virus program should establish controls for ensuring all updates have been successfully accomplished.

Assessment of Cause

IRS lacks standard service-wide controls for ensuring all updates to virus protection software have been accomplished.

Corrective Action #3

The official responsible for the virus program will, by 31 March 2001, establish controls for ensuring all updates have been successfully accomplished.

Implementation Date of Corrective Action #3

Completed	**Proposed**
	31 March 2001

Responsible Officials for Corrective Action #3

Chief Information Officer IS
Deputy Chief Information Officer (Operations) IS
Director, Telecommunications

Corrective Action #3 Monitoring Plan

Same as recommendation #1.

MANAGEMENT RESPONSE TO DRAFT AUDIT REPORT – A COMPREHENSIVE PROGRAM FOR PREVENTING AND DETECTING COMPUTER VIRUSES IS NEEDED

Recommendation #4

The official responsible for the virus program should develop a system for gathering information to help analyze and monitor the effectiveness of the program's virus detection and prevention activities.

Assessment of Cause

IRS lacks a standard service-wide system for gathering information to analyze and monitor the effectiveness of virus protection and prevention activities.

Corrective Action #4

The official responsible for the virus program will, by 1 June 2001, develop a system for gathering information to help analyze and monitor the effectiveness of the program's virus detection and prevention activities.

Implementation Date of Corrective Action #4

Completed	Proposed
	1 June 2001

Responsible Officials for Corrective Action #4

Chief Information Officer IS
Deputy Chief Information Officer (Operations) IS
Director, Telecommunications

Corrective Action #4 Monitoring Plan

Same as recommendation #1

MANAGEMENT RESPONSE TO DRAFT AUDIT REPORT – A COMPREHENSIVE PROGRAM FOR PREVENTING AND DETECTING COMPUTER VIRUSES IS NEEDED

Recommendation #5

The official responsible for the virus program should strengthen procedures for ensuring that employees comply with the IRM requirements for preparing Virus Incident Reports.

Assessment of Cause

IRS needs to strengthen procedures for ensuring that employees comply with the IRM requirements for preparing Virus Incident Reports.

Corrective Action #5

The official responsible for the virus program will, by 31 December 2000, strengthen procedures for ensuring that employees comply with the IRM requirements for preparing Virus Incident Reports.

Implementation Date of Corrective Action #5

Completed	Proposed
	31 December 2000

Responsible Officials for Corrective Action #5

Chief Information Officer IS
Deputy Chief Information Officer (Operations) IS
Director, Telecommunications

Corrective Action #5 Monitoring Plan

Same as recommendation #1

MANAGEMENT RESPONSE TO DRAFT AUDIT REPORT – A COMPREHENSIVE PROGRAM FOR PREVENTING AND DETECTING COMPUTER VIRUSES IS NEEDED

Recommendation #6

The official responsible for the virus program should form a virus response team and develop procedures for the various activities that need to be quickly coordinated and carried out when major virus outbreaks occur.

Assessment of Cause

IRS lacks a central virus response team with service-wide responsibility and authority along with procedures required for the various activities that need to be coordinated and carried out when major virus outbreaks occur.

Corrective Action #6

The official responsible for the virus program will, by 31 December 2000, form a virus response team with service-wide authority and develop procedures for the various activities that need to be coordinated and carried out when major virus outbreaks occur.

Implementation Date of Corrective Action #6

Completed

Proposed
31 December 2000

Responsible Officials for Corrective Action #6

Chief Information Officer IS
Deputy Chief Information Officer (Operations) IS
Director, Telecommunications

Corrective Action #6 Monitoring Plan

Same as recommendation #1.