

Office of Inspector General



December 6, 2000
Audit Report No. 00-049


Computer Virus Protection Program



DATE: December 6, 2000

TO: John F. Bovenzi, Chief Operating Officer

Donald C. Demitros, Chief Information Officer and Director
Division of Information Resources Management

FROM: 
David H. Loewenstein
Assistant Inspector General

SUBJECT: *FDIC's Computer Virus Protection Program*
(Audit Report No. 00-049)

The Office of Inspector General (OIG) has completed an audit of the Federal Deposit Insurance Corporation's (FDIC) Computer Virus Protection Program (CVPP). This audit was performed to assess the Corporation's ability to identify, contain, and clean computer viruses.

BACKGROUND

The Division of Information Resources Management's (DIRM) Information Security Staff (ISS) reported 45,000 FDIC computer virus incidents during the first three quarters of 1999. A computer virus is a specially designed computer program that has the ability to replicate itself and modify other programs. This program may contain malicious instructions that disrupt a computer's proper operation or destroy programs and other data stored in a computer. The FDIC defines a computer virus incident as each occurrence of a virus being detected by FDIC computer virus protection software (CVPS). Computer viruses normally target the most popular or commonly used systems to achieve the greatest disruption.

The economic impact of computer virus contamination is determined by considering the expense of eliminating the virus and restoring the infected computer to its pre-contaminated state. This expense also includes, in terms of time, lost productivity and potential loss of data. If computer virus contamination is left unchecked, the extent of this expense may be significant. For example, an August 1999 computer security publication reported that, "Computer virus attacks have cost businesses \$7.6 billion in 1999."¹ Another possible impact of computer virus contamination, although less direct than the economic one, is the FDIC's loss of public trust due to perceived weaknesses in its computer virus protection capabilities.

¹ Securitysense, Volume 2, No.10, August 1999, Page 1.

The FDIC CVPP started on April 9, 1991 with the issuance of the CVPP Directive, Circular 1360.2. At that time the CVPP focused on minimizing computer virus contamination of employee desktop microcomputers introduced through diskettes and spread through file-sharing using segregated FDIC local area networks. Over the past 9 years, the CVPP has grown in complexity to keep pace with the rapid advancement of information technology and its deployment within the FDIC. The CVPP Directive, Circular 1360.2, has been updated twice, in 1996 and in 1997, to enhance its effectiveness and adapt it to changing conditions.

The expanded program now addresses computer virus contamination originating through electronic mail and data transfers originating over the Internet, the FDIC Intranet, and, to a lesser extent, through diskettes and compact disks. At our audit's commencement, the FDIC used several computer virus protection software products to safeguard the FDIC's technical infrastructure that consisted of 14,635 computers, including 438 network servers, 10,210 desktop computers, and 3,987 laptop microcomputers. Network servers, desktop computers, and laptop microcomputers support communication functions and system-user office work. The FDIC's CVPP also addresses network access by FDIC employees and contractors conducting official business at external locations after normal operating hours.

Staffing to support the FDIC's CVPP is comprised of DIRM ISS, the DIRM Helpdesk, DIRM system administrators, and, to a lesser extent, appointed information security officers (ISO) from each of the FDIC's divisions and offices. With the exception of DIRM ISS, staff support for virus protection is provided on an as-needed basis and is usually part-time. DIRM ISS has assigned two employees full-time, one employee part-time, and six contractors part-time to support the CVPP.

In addition to staff support, the primary CVPP component used to safeguard FDIC computer resources from virus contamination is the software. CVPS are commercially available products designed to detect and eradicate viruses and notify responsible parties about the detection and eradication incident. At the commencement of our audit, the FDIC used several CVPS products, including VirusScan, Webshield and Netshield by Network Associates; Inoculin by Computer Associates; Norton Anti-Virus by Symantec; and F-Secure by F-Secure Corporation.

DIRM's ISS Director has identified computer virus prevention as the highest priority within the Corporation's IT security program. Prior to the audit's commencement, he established a Computer Security Incident Response Team (CSIRT) to provide more timely response to computer virus emergencies.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of the audit was to determine the effectiveness and efficiency of the FDIC's CVPP. To accomplish this objective, we interviewed DIRM ISS, Helpdesk, and Local Area Network (LAN) management personnel. We also interviewed ISOs from the Legal Division, Chairman's Office, Division of Supervision, Division of Finance, Division of Administration, and the Division of Resolutions and Receiverships. Additionally, we researched CVPP best practices and reviewed

FDIC CVPP policies, standards, and procedures. Furthermore, we assisted DIRM's ISS Director in identifying solutions to improve FDIC's CVPP program. Solutions arrived at during the audit included DIRM's implementing real-time virus protection for FDIC NT servers and increasing the frequency of CVPS signature file updates for the FDIC's laptop computers.

Our audit focused on the FDIC CVPP's capability to prevent, detect, and eradicate computer virus contamination. During our audit, we judgmentally sampled 52 FDIC computers in the Washington, D.C., area to assess whether CVPS was functioning in accordance with management's intentions. Our sample consisted of 19 desktop computers, 14 network servers and 19 laptop computers drawn from a Washington, D.C., area population of 5,227 desktop computers, 236 network servers and 769 laptop microcomputers.

To accomplish sample testing, we employed computer virus simulators that would cause CVPS to trigger an alert without putting FDIC computer resources at risk of viral contamination. We also verified whether FDIC computers that were susceptible to computer virus contamination indeed had CVPS protection. Furthermore, we determined whether the FDIC CSIRT responded to computer virus emergencies in a timely manner. The audit was performed between November 1999 and August 2000 in accordance with generally accepted government auditing standards.

RESULTS OF AUDIT

We concluded that the FDIC CVPP was generally effective in minimizing the exposure from computer virus contamination. However, we identified possible improvements to further reduce the probability of computer virus contamination within the Corporation. Specifically, we identified several mission critical and operationally significant computers that were not afforded protection by CVPS and other instances where CVPS was not fully utilized. We also noted that CVPS maintenance could be strengthened and that the CVPP policies, standards, and procedures needed to be updated and expanded to reflect current risks and operations. We communicated this information to DIRM's ISS Director during our audit. DIRM's ISS Director initiated corrective action during audit fieldwork to address some of these issues.

The effectiveness of the FDIC's CVPP was demonstrated during the global attack of the "I Love You" computer virus. The actions taken by DIRM's ISS to protect corporate assets minimized the impact of the attack. Specifically, DIRM ISS was able to develop and institute firewall filters attuned to viral characteristics provided by the CSIRT. This special filter prevented the virus from reaching FDIC computer resources. Because of the early warning provided by the CSIRT, the FDIC fared better than many other federal agencies. For example, the Social Security Administration required 5 days to become fully functional and completely remove the virus from its systems. Additionally, the Department of Labor's recovery required over 1,600 employee and 1,200 contractor hours.

COMPUTER VIRUS PROTECTION PROGRAM WOULD BENEFIT FROM A THOROUGH RISK ASSESSMENT

The absence of a thorough risk assessment to guide refinement of the CVPP resulted in protection that was not always fully effective. CVPS was not resident on some susceptible FDIC systems and was not fully employed on others. For those systems without CVPS, stringent software configuration management² was not in place to serve as a compensating protection mechanism. System users could disable CVPS without DIRM ISS notification and did not always use power-up passwords³ to safeguard their desktop and laptop computers. Furthermore, an advanced CVPS detection feature, heuristics analysis, was not being used to guard against newer, more sophisticated viruses.

Although DIRM's ISS Director informally evaluated the vulnerabilities to the FDIC's IT resources when he joined the Corporation in January 1999, a formal, documented risk assessment of the FDIC CVPP had not been performed. Assessing risk is a prudent prerequisite to implementing effective computer virus protection techniques. The Office of Management and Budget Circular A-130: *Management of Federal Information Resources*, and the U.S. General Accounting Office's *Federal Information System Controls Audit Manual (FISCAM)*, both require periodic risk assessments as part of an effective information resources management program.

During the period of April 1991 to December 1998, the FDIC CVPP evolved, according to DIRM ISS, based upon specific virus incidents that faced the Corporation. The FDIC addressed the threat from computer viruses, but its approach was characterized as more reactive than proactive. Since its inception in April 1991, the FDIC CVPP has been supported by one primary directive, Circular 1360.2, *FDIC Computer Virus Protection Program*. The directive has been updated twice in an effort to ensure its consistency with existing practices. Although procedures for the FDIC's virus protection program were developed and updated, DIRM ISS had not developed a formal strategic plan or a risk assessment to support the CVPP program before 1999. In light of these circumstances, the new DIRM ISS Director performed a preliminary vulnerability assessment during the second quarter of 1999. A formal strategic plan to support the CVPP was then officially established in October 1999.

As a consequence of not performing a thorough risk assessment, some FDIC computers were not afforded the protection of computer virus protection software. Specifically, we noted that Sun Solaris, IBM Mainframe, Lucent Private Branch Exchanges, and Cisco Routers and Switches were not afforded virus protection software. Most of these computers either make use of a version of the Unix operating system (or an operating system with a Unix component) or transfer information to or from a computer with a Unix operating system derivative. These computers are involved in varying degrees of internal and external data communication activity and support mission critical FDIC systems. The Unix operating system's susceptibility to computer virus contamination was

² A process whereby computer programs are tightly controlled to detect and record all changes.

³ Power-up passwords are the primary security mechanism for preventing local access to a computer's hard disk drive.

first recognized in 1989 by computer virus researchers.

While stringent software configuration management can provide a compensating control to the absence of CVPS, this practice was not consistently used within the FDIC. However, the absence of stringent software configuration management has been addressed in the OIG's recent audit report entitled *FDIC's IT Configuration Management Program* (Report Number 00-038) and will not be addressed further within this audit report.

While we noted that the FDIC's Windows NT network servers were equipped with CVPS, we found that the virus protection software was not fully utilized. Specifically, these network servers did not use resident computer virus protection software in a real-time mode. Rather, such software was run in a batch mode,⁴ usually overnight. According to DIRM LAN management personnel, NT server virus-protection software was not used in a real-time mode due to network performance problems.

While desktop and laptop systems have real-time virus detection capabilities through another CVPS, the FDIC user community can easily disable this computer virus protection software without automatic notification to DIRM ISS by the subject computer. FDIC's exposure, due to users' ability to disable virus protection software without automatic notification, is increased if individuals other than the intended user can access the desktop. Power-up passwords are the primary security mechanism for preventing local access to a computer's hard disk drive. Audit testing of 38 desktop and laptop computers revealed that system users had not used power-up passwords to restrict access on any of the computers.

FDIC's CVPP Directive, Circular 1360.2 requires that power-up passwords be used. Power-up passwords can prevent unauthorized computer access and the introduction of computer viruses by third parties. Access to the hard drive permits access to all FDIC software and data contained on it. However, DIRM ISS's planned implementation of cryptography with smart-card technology provides a compensating control to alleviate the need for power-up passwords. Accordingly, no recommendation regarding power-up password use will be made in this report.

In addition to users being able to circumvent desktop and laptop real-time CVPS, the FDIC had not implemented the heuristic analysis feature available within its CVPS. Heuristic analysis is a state-of-the-art anti-virus technique that can detect new viruses before they have the chance to contaminate a computer. Specifically, heuristic analysis involves identifying destructive program code before the code is executed. Heuristic analysis is the primary method to detect both new and polymorphic⁵ computer viruses, such as those that recently contaminated worldwide computer networks.

We brought these issues to DIRM's attention during the course of our audit. In response to some of these issues, DIRM's ISS Director initiated corrective action during the process of fieldwork.

⁴ A program is resident but dormant on a computer and requires manual intervention to execute.

⁵ A computer virus that modifies itself each time it replicates to avoid detection by CVPS.

Specifically, he budgeted for Unix computer virus protection software and plans to employ an external computer virus expert to perform a CVPP risk assessment. In addition, he has initiated research to identify computer virus protection program software that can be used on FDIC NT servers in a real-time mode. Furthermore, he has activated the heuristic analysis feature contained in CVPS. DIRM officials also advised that other IT initiatives limit their current ability to restrict users from disabling virus protection software, but that future planned activities would address this issue. The DIRM officials also agreed to continue to research interim options for restricting users' ability to disable virus software. Management's actions and plans to address these issues have and will provide benefits to the Corporation. Because some of DIRM's planned actions are not yet complete and because virus protection activities are dynamic in nature, except as noted, we are including recommendations for each of the issues discussed in this section.

Recommendations

We recommend that the Chief Information Officer and Director, DIRM, ensure that:

- (1) A formal and thorough risk assessment of the FDIC CVPP is conducted and the results used as the basis for future enhancements to computer virus protection within the Corporation.
- (2) Virus protection software is acquired and implemented for mission critical or operationally significant Unix-based computers within the Corporation, such as Sun Solaris and Oracle .
- (3) Computer virus protection software for Windows NT servers be improved or replaced to provide real-time coverage.
- (4) DIRM ISS continues to research methods of preventing the user community's capability to disable virus protection software used on FDIC desktop workstations and laptop computers without DIRM ISS notification. Once an optimal method is identified, DIRM ISS should implement it on a timely basis.
- (5) Available heuristic analysis features of computer virus protection software used by the FDIC is activated.

COMPUTER VIRUS PROTECTION SOFTWARE MAINTENANCE NEEDS IMPROVEMENT

CVPS signature file updates⁶ were not performed at least weekly to minimize the risk of viral contamination. In addition, complete documentation supporting testing of CVPS upgrades, testing of signature-file updates, and management approval of CVPS configuration settings was not established and retained. Also, sufficient numbers of qualified DIRM ISS staff may not exist to

⁶ The process of adding new virus characteristics to the existing, applicable database within CVPS.

effectively handle the CVPP workload and FDIC laptop computer users are not accessing the FDIC network frequently enough to receive the latest CVPS signature-file updates. Furthermore, the CVPS alert generation function did not always work as intended by management and generated alerts were not consistently received by the CSIRT or captured in weekly statistical reports to management.

At the audit's inception, FDIC desktop and laptop CVPS non-emergency signature-file updates occurred on a monthly basis. Although more frequent updates were observed for network-connected desktop computers in response to viral emergencies, testing of signature file updates was limited to re-verifying the detection of three viruses recently encountered at the FDIC. Additionally, the DIRM ISS Director indicated that all CVPS signature file updating for laptop computers was often less frequent due to extended periods of disconnection from the FDIC networks. We also noted that test documentation supporting CVPS upgrades and signature-file updates was incomplete in terms of test purpose, methods, and results. Finally, we noted a lack of evidence supporting management approval of CVPS configuration settings.⁷

Due to the proliferation of computer viruses and the volume of new virus activity, signature file updates should be applied to FDIC computers as soon as they are made available by the CVPS vendor. For example, the 1999 FDIC National Information Security Officer Conference reported that at least 10 new viruses are created per day. Testing of virus signature file updates should be sufficient to ensure CVPS continued and proper operation. Furthermore, such testing should ensure that files, updated to detect available new virus signatures, correctly detect the new viruses.

Complete documentation should be established and retained to substantiate the test's purpose, methods, and results. Evidence of management review and approval of CVPS configuration settings should be retained to provide an official record substantiating that settings conform to management's intentions and to facilitate accountability over their specification.

Monthly virus signature file update frequency, limited signature file update testing, incomplete CVPS test documentation, and undocumented CVPS configuration-setting management approval are the result of shifting operational priorities. Such shifting priorities are driven by DIRM ISS's extremely heavy workload. Additionally, some laptop users do not consistently access the FDIC network frequently enough to facilitate receipt of CVPS signature file updates. For example, the unique nature of Division of Supervision field operations makes frequent access to FDIC networks inconvenient.

As a result of the cited conditions, new computer viruses may not be detected and eradicated by existing CVPS, and the CVPS itself may not function as represented by the vendor. In addition, CVPS operation and testing may not conform to management's intentions, all of which may permit viral contamination of FDIC computer resources. Examples of these effects are illustrated by our audit test results. First, the method⁸ used to invoke CVPS on desktop computers influenced

⁷ Specified operating parameters that govern how the software will function.

⁸ CVPS can be invoked by either scanning a file or by attempting to use (read, write, delete) a file.

whether an alert message was sent to the CSIRT in response to a detected virus. Second, on 13 of 19 desktop computers and 13 of 14 network servers evaluated, CSIRT did not receive simulated virus alerts and accordingly, did not respond to them. Third, viral alerts generated from detected external-electronic-mail-message viruses were not sent to the message originator. Fourth, with 13 of 19 desktop computers, 13 of 14 network servers, and all external email tested, generated virus alerts were not captured in weekly virus statistical reports used by the DIRM ISS Director to measure the effectiveness of the CVPP. The details of these test exceptions were communicated to DIRM ISS during the audit.

We brought these issues to the attention of DIRM's ISS Director during the course of our audit. In response to some of the conditions cited, the DIRM ISS Director initiated a research effort early in the audit to identify and implement an automated method for enforcing the timely receipt of signature file updates by laptop computer users. He also instituted weekly, as opposed to monthly, CVPS signature file updates. Management's actions and plans to address these issues have and will provide benefits to the Corporation. Because some of DIRM's planned actions are not yet complete and because virus protection activities are dynamic in nature, we are including recommendations for each of the issues discussed in this section.

Recommendations

We recommend that the Director, DIRM, ensure that:

- (6) CVPS signature-file updates be performed as frequently as possible, preferably weekly, to minimize the risk of viral contamination.
- (7) Complete documentation supporting the testing of CVPS upgrades and signature-file updates is established and retained in accordance with FDIC record retention policy.
- (8) Management approval of CVPS configuration settings is established and retained in accordance with FDIC record retention policy.
- (9) All uncleaned virus alerts generated by CVPS are consistently communicated to the CSIRT by the contaminated computer for follow-up and captured in weekly statistical reports to DIRM's ISS Director.

We further recommend that the FDIC Chief Operating Officer direct:

- (10) All FDIC laptop computer users to access the FDIC network, preferably weekly but at least monthly, using their laptop computers to receive CVPS signature file updates.

COMPUTER VIRUS PROTECTION PROGRAM POLICIES, STANDARDS AND PROCEDURES NEED TO BE EXPANDED AND UPDATED

DIRM Directive 1360.2, the overarching CVPP policy that was revised on April 29, 1997, is comprehensive and contains instructions for virus recovery to assist system users in minimizing computer damage. We further noted that the CSIRT Procedure⁹ addressed the disposition of viruses detected through FDIC CVPS. However, we noted that Directive 1360.2 did not contain certain information regarding computer virus prevention, detection, and eradication that, if included, would enhance it and the entire FDIC CVPP.

We found that the policy would be enhanced in terms of virus prevention if it included the following:

- Requirements that CVPS be used on all FDIC computers.
- Descriptions of alternate virus protection methods, such as stringent software configuration management, to be used when CVPS is not commercially available for a given FDIC computer.
- Technical supplements describing CVPS used at the FDIC and the software features selected, such as heuristics analysis, to minimize risk of contamination.
- Directions for using the recently installed central clearing computer for the purpose of inspecting and removing viruses prior to installation and execution on corporate computers.
- Instructions on how non-FDIC organizations with access to FDIC computer resources should comply with the CVPP.
- Information addressing FDIC employee and contractor virus awareness and protection training.
- Process descriptions on establishing and maintaining the frequency of virus signature file updates.
- Descriptions of newly developed, recurring virus protection tasks such as the firewall filtering used by DIRM ISS to counteract the recent “I Love You” virus incident.

We also found that the policy would be enhanced in terms of virus detection if it included the following:

- Directions on using the CSIRT to perform analysis of new viruses and a description of the current role of the DIRM Help Desk and the Information Security Officers (ISOs) relative to their participation in the CVPP.
- Explanations regarding the use of multiple virus scanning and viral alert methods on FDIC computers.
- Guidance on using the recently created virus incident database as a reference tool.

In addition, we found that the policy would be enhanced in terms of virus eradication if it included the following:

- Guidance on proper measures to be taken to remove computer viruses from compact disks and diskettes and on measures to take for sending newly detected viruses to outside virus labs for further analysis.
- Reference to supplemental CVPP policies and procedures, such as *Home Use of FDIC Anti-*

⁹ A recent procedure that governs how the Computer Security Incident Response Team operates.

virus Software and CSIRT Procedures with descriptions of their intended purpose.

Current and complete policies, standards, and procedures ensure that complex areas, such as computer virus protection, operate in accordance with management's intentions. In addition, such policies, standards and procedures provide employees with a written reference that is especially helpful for infrequently performed duties. GAO's FISCAM stipulates that management periodically assess the appropriateness of security policies and procedures as well as compliance with them.

DIRM ISS has focused its human resources principally on dealing with computer virus incidents facing the Corporation. As a result, maintenance of relevant directives became a secondary concern. FDIC employees may not be fully aware of effective actions to employ when faced with a computer virus contamination incident. Complete policies and procedures will help ensure that corporate information technology resources will not be exposed to significant risk if crucial steps are omitted or misunderstood. Furthermore, without the benefit of proper documentation, DIRM ISS staff members responsible for performing anti-viral related tasks may not be able to perform their duties in a repeatable manner. This lack of regularity could result in system down-time, significantly impairing corporate operations and thereby weakening public confidence and trust in the FDIC.

We brought these issues to DIRM's attention during the course of our audit. In response, DIRM's ISS Director initiated a review of all policies and procedures related to the CVPP. Because this analysis is not yet complete and because virus protection activities are dynamic in nature, we are including a recommendation to continue the review of existing policies and procedures.

Recommendations

We recommend that the Chief Information Officer and Director, DIRM, ensure that:

- (11) DIRM ISS continues with its review of all policies and procedures currently in place relative to the CVPP.
- (12) Upon the successful completion of the policy and procedure review, DIRM ISS develop and implement security policies that depict updated CVPP operational requirements and include, but are not limited to, the areas of computer virus prevention, detection, and eradication described above.

CORPORATION COMMENTS AND OIG EVALUATION

On November 6, 2000, the Chief Information Officer and Director, Division of Information Resources Management, provided a written response to the draft report. The responses are presented in Appendix I of this report. Subsequent to the November 6 response, DIRM provided additional information regarding recommendation 10, directed to the FDIC's Chief Operating

Officer.

Based on discussions between the Chief Operating Officer and the Chief Information Officer and Director, DIRM, the FDIC agrees with recommendation 10. Currently, e-mails are issued to all DOS and DCA Field Offices and all Field Office Representatives every 2 weeks notifying all staff to update their laptop CVPS signature files. By February 15, 2001, the COO will issue a memorandum to all FDIC employees requiring all laptop users to access the FDIC intranet at least once a month and download the latest CVPS signature file updates to their laptops. In 2001, DIRM will explore several options to enhance the ease with which laptop users can update the CVPS files. Current alternatives that are being investigated include assessing the feasibility of new software which will support “automatic” updates of CVPS files whenever a laptop user accesses the network.

The Corporation’s response to the draft report provided the elements necessary for management decisions on the report’s recommendations. Therefore, no further response to this report is necessary. Appendix II presents management’s proposed action on our recommendations and shows that there is a management decision for each recommendation in this report.

November 6, 2000

TO: David H. Loewenstein
Assistant Inspector General

FROM: Donald C. Demitros, Director 

SUBJECT: DIRM Management Response to the Draft OIG Report Entitled, "Audit of the FDIC's Computer Virus Protection Program" (Audit Number 99-906)

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report and generally agrees with the findings and recommendations. We were especially gratified that the audit found a "generally effective" program and recognized our efforts during the "I Love You" incident. We agree that this discipline requires constant improvement and vigilance. Responses to each of the specific recommendations (1 through 9, 11 and 12) directed to DIRM are provided below. Recommendation number 10 was directed to the Chief Operating Officer.

Management Decision:

Recommendations: We recommend that the Director, DIRM, ensure that:

- (1) A formal and thorough risk assessment of the FDIC Computer Virus Protection Program (CVPP) is conducted and the results used as the basis for future enhancements to computer virus protection within the Corporation.

DIRM Response: DIRM conducted a preliminary vulnerability assessment of the CVPP during the second quarter of 1999 and this OIG audit serves as an additional assessment. OMB A-130 requires such an assessment for major applications and general support systems but not a computer virus program. The current program has saved the Corporation millions of dollars in terms of possible down time and as compared to other agencies and the private sector. In accordance with its IS Strategic Plan, DIRM is implementing solutions to further strengthen the virus protection program. DIRM will have a vendor independently review and verify that the implemented solutions are effective in mitigating the virus risks to the Corporation. DIRM currently anticipates that this will be completed by June 30, 2001, after all the identified measures are put in place.

- (2) Virus protection software is acquired and implemented for mission critical or operationally significant Unix-based computers within the Corporation, such as Sun Solaris and Oracle.

DIRM Response: The industry has not reported any Solaris or Oracle viruses in the "wild"

for over a decade. The anti-virus vendor community is selling anti-virus software that operates on the UNIX environment but that cannot be tested against the UNIX file systems as there are no UNIX-specific viruses identified for the platform. The 2001 implementation of DIRM's new configuration management methodologies will serve as an added precaution to insure that the ten FDIC employees who are responsible for software installation and/or maintenance on UNIX servers do not install software that might contain other types of viruses. DIRM will evaluate any promising UNIX-specific anti-virus packages when they become available in the anti-virus software community.

- (3) Computer virus protection software for Windows NT servers be improved or replaced to provide real-time coverage.

DIRM Response: Following a Request for Information (RFI) and a formal evaluation of several anti-virus software packages, DIRM has selected Trend Micro. This product will provide the real-time coverage as well as the centralized reporting. Implementation is targeted to begin in December of 2000.

- (4) DIRM ISS continues to research methods of preventing the user community's capability to disable virus protection software used on FDIC desktop workstations and laptop computers without DIRM ISS notification. Once an optimal method is identified, DIRM ISS should implement it on a timely basis.

DIRM Response: In August 2000 DIRM ISS began the evaluation of Vshield 4.5 as a potential means of mitigating this risk. This newer version may make it harder for the user to disable the anti-virus software. DIRM ISS and the technical infrastructure staff will complete this evaluation by March 31, 2001. Note that DIRM is limited in being able to control user actions due to an insecure operating system (Windows 95). The pending upgrade to Windows 2000 may also further reduce or eliminate this vulnerability.

- (5) Available heuristic analysis features of computer virus protection software used by the FDIC are activated.

DIRM Response: This feature was activated nationwide in August 2000 with the exception of laptops, which will be completed by the end of the year.

- (6) CVPS signature-file updates be performed as frequently as possible, preferably weekly, to minimize the risk of viral contamination.

DIRM Response: As of January 2000 DIRM is implementing weekly updates for the servers and biweekly updates for the desktop. The website available for laptop users to download anti-virus updates is also updated every two weeks.

- (7) Complete documentation supporting the testing of CVPS upgrades and signature-file updates is established and retained in accordance with FDIC record retention policy.

DIRM Response: By November 15, 2000 DIRM ISS will provide complete documentation supporting the testing of upgrades and signature updates.

- (8) Management approval of CVPS configuration settings is established and retained in accordance with FDIC record retention policy.

DIRM Response: By January 15, 2001 DIRM ISS will publish management approved configuration settings for the following platforms: Desktop, Laptop, Servers, and NT Workstations. These settings will be published on a public folder, made available to DIRM, and retained in accordance with FDIC record retention policy.

- (9) All uncleaned virus alerts generated by CVPS are consistently communicated to the CSIRT by the contaminated computer for follow-up and captured in weekly statistical reports to DIRM's ISS Director.

DIRM Response: DIRM is purchasing the Trend Micro anti-virus software for NT servers and Exchange servers to be implemented by December 31, 2000. This software will provide centralized alerts for the server. The desktop software provides alerts for uncleaned viruses with the exception of a manual scan where the user invokes the anti-virus software from the programs menu. When a virus is found during a manual scan the user only gets one option and that is to clean the virus. However, no alert is generated. If the software cannot clean the virus, it will stop the user from executing or copying the file. An attempt by the user to copy or execute the file will trigger the real-time anti-virus software that will in turn trigger an alert. Therefore, DIRM ISS believes that there is minimal risk to the Corporation. However, to remain proactive in the timely identification of uncleaned viruses, DIRM ISS will continue to work with the leading virus vendors. To that end, ISS requested in September 2000 that Network Associates, Inc. (NAI) consider the enhancement of their centralized alert feature during manual scans as a product enhancement. NAI agreed to consider the request.

We further recommend that the FDIC Chief Operating Officer direct:

- (10) All FDIC laptop computer users to access the FDIC network, preferably weekly but at least monthly, using their laptop computers to receive CVPS signature file updates.

DIRM Comment: This action item was assigned to the Chief Operating Officer (COO).

- (11) DIRM ISS continues with its review of all policies and procedures currently in place relative to the CVPP.

DIRM Response: DIRM ISS will complete its initial review of its CVPP policies and procedures by December 31, 2000.

- (12) Upon the successful completion of the policy and procedure review, DIRM ISS develop and implement security policies that depict updated CVPP operational requirements and include, but are not limited to, the areas of computer virus prevention, detection, and eradication described above.

DIRM Response: DIRM ISS will continue to improve its CVPP and implement policies and procedures that depict the improved CVPP. The revised version of the anti-virus directive (Circular 1360.2) is anticipated to be developed and in the Corporate Directive Clearing process by March 31, 2001.

Please address any questions to DIRM's Audit Liaison, Rack Campbell, on (703) 516-1422.

APPENDIX II

MANAGEMENT RESPONSES TO RECOMMENDATIONS

The Inspector General Act of 1978, as amended, requires the OIG to report the status of management decisions on its recommendations in its semiannual reports to the Congress. To consider FDIC's responses as management decisions in accordance with the act and related guidance, several conditions are necessary. First, the response must describe for each recommendation

- the specific corrective actions already taken, if applicable;
- corrective actions to be taken together with the expected completion dates for their implementation; and
- documentation that will confirm completion of corrective actions.

If any recommendation identifies specific monetary benefits, FDIC management must state the amount agreed or disagreed with and the reasons for any disagreement. In the case of questioned costs, the amount FDIC plans to disallow must be included in management's response.

If management does not agree that a recommendation should be implemented, it must describe why the recommendation is not considered valid. Second, the OIG must determine that management's descriptions of (1) the course of action already taken or proposed and (2) the documentation confirming completion of corrective actions are responsive to its recommendations.

This table presents the management responses that have been made on recommendations in our report and the status of management decisions. The information for management decisions is based on management's written responses to our report.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
1	DIRM will have a vendor independently review and verify that implemented solutions are effective in mitigating the virus risks to the Corporation.	June 30, 2001	Vendor report on virus risks	None	Yes
2	The 2001 implementation of DIRM's new configuration management methodologies will serve as an added precaution to ensure that the ten FDIC employees who are responsible for software installation and/or maintenance on UNIX servers do not install software that might contain other types of viruses. DIRM will evaluate any promising UNIX-specific anti-virus packages when they become available in the anti-virus software community.	December 31, 2001	New configuration management methodologies	None	Yes
3	Following a Request for Information (RFI) and a formal evaluation of several anti-virus software packages, DIRM has selected Trend Micro. This product will provide the real-time coverage as well as the centralized reporting.	December 2000	System implementation notification	None	Yes
4	In August 2000, DIRM ISS began the evaluation of Vshield 4.5 as a potential means of mitigating this risk. This newer version may make it harder for the user to disable the anti-virus software. DIRM ISS and the technical infrastructure staff are continuing with this evaluation.	March 31, 2001	Evaluation report	None	Yes
5	This feature was activated nationwide in August 2000 with the exception of laptops, which will be completed by the end of the year.	December 31, 2000	Computer virus software configuration documentation	None	Yes
6	As of January 2000 DIRM is implementing weekly updates for the servers and biweekly updates for the desktop. The website available for laptop users to download anti-virus updates is also updated every two weeks.	Completed	Computer virus protection program documentation	None	Yes

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
7	By November 15, 2000 DIRM ISS will provide complete documentation supporting the testing of upgrades and signature updates.	November 15, 2000	Computer virus software test documentation	None	Yes
8	By January 15, 2001 DIRM ISS will publish management approved configuration settings for the following platforms: Desktop, Laptop, Servers, and NT Workstations. These settings will be published on a public folder, made available to DIRM, and retained in accordance with FDIC record retention policy.	January 15, 2001	Approved computer virus software configuration settings	None	Yes
9	To remain proactive in the timely identification of uncleaned viruses, DIRM ISS will continue to work with the leading virus vendors. To that end, ISS requested in September 2000 that Network Associates, Inc. (NAI) consider the enhancement of their centralized alert feature during manual scans as a product enhancement. NAI agreed to consider the request.	Completed	Letter to NAI requesting enhancement	None	Yes
10	The COO will issue a memorandum to all FDIC employees by February 15, 2001, requiring all laptop users to access the FDIC intranet at least once a month and download the latest CVPS signature file updates to their laptops.	February 15, 2001	Memorandum from COO	None	Yes
11	DIRM ISS will complete its initial review of its CVPP policies and procedures by December 31, 2000.	December 31, 2000	Notification of CVPP policies and procedure review completion	None	Yes
12	DIRM ISS will continue to improve its CVPP and implement policies and procedures that depict the improved CVPP. The revised version of the anti-virus directive (Circular 1360.2) is anticipated to be developed and in the Corporate Directive Clearing process by March 31, 2001.	March 31, 2001	Revised CVPP policies and procedures	None	Yes