



*The City of New York
Office of the Comptroller
Bureau of Financial Audit
EDP Audit Division*

WILLIAM C. THOMPSON, JR.
Comptroller

**Follow-Up Audit Report
On the Department of Employment
Local Area Network/Wide Area Network**

7F02-110

April 17, 2002

The City of New York
Office of the Comptroller
Bureau of Financial Audit
EDP Division

**Follow-up Audit Report on the
Department of Employment
Local Area Network/
Wide Area Network**

7F02-110

SUMMARY OF FINDINGS AND CONCLUSIONS

This follow-up audit determined whether the New York City Department of Employment (DOE) implemented recommendations made in a previous audit entitled, *Audit Report of the Department of Employment Local Area Network/ Wide Area Network* (Audit No.7A97-124, issued June 20, 1997). The earlier audit evaluated the effectiveness of management's control over DOE's local area network (LAN) and wide area network (WAN) in the areas of physical security, logical security, department operations, and disaster recovery/contingency planning. In our current audit, we discuss the recommendations we made earlier, as well as the implementation status of those recommendations. We also discuss new findings and recommendations based on our current review.

In our previous audit we made 19 recommendations to DOE, all of which been implemented. The details of these recommendations and their implementation status follow. DOE should:

1. "Submit a 'new need' request to OMB to hire two or three more persons to document and resolve current and future change requests." **IMPLEMENTED**
2. "Design a problem reporting form with an identical format to the Problem Ticket Screen on the HEAT [Help-desk Expert Automation Tool] system. This form could be mailed or faxed to the Help Desk and entered into the HEAT system, thereby ensuring that all problems are captured on the HEAT system." **IMPLEMENTED**
3. "Modify the HEAT system so that analysts can review problem tickets on-line, and if they determine that a change request should be generated, they can bring up a new screen that captures the Problem Ticket Number and Problem Ticket Date from the system. This would then allow the analyst to enter information on the scope and description of the changes, programming resources required, and the name of the authorizing manager." **IMPLEMENTED**

4. “Provide the Help Desk with formal procedures to regularly update users as to the status of their change requests.” **IMPLEMENTED**
5. “Ensure that all servers are equipped with console locks so that LAN administrators and operators can lock the servers whenever they leave the server room.” **IMPLEMENTED**
6. “Password-protect the console for each server. This can easily be achieved by either using the Supervisory password or assigning a password through the Novell Monitor utility so that only authorized personnel can have access to these servers.” **IMPLEMENTED**
7. “In the short term, add a timeout function to workstations in the Windows environment by utilizing the screen saver option under the desktop of the control panel icon with the password-protected option turned on. In the long term, DOE could standardize workstation security by purchasing a software package, such as Intermission or LockIt.” **IMPLEMENTED**
8. “Secure the backup router and test router (when it is found) in either the server room or in a locked hardware storage room.” **IMPLEMENTED**
9. “Develop a security request form to be completed by employees whenever they request an addition, modification, or deletion to their access privileges.” **IMPLEMENTED**
10. “Create formal security procedures for recording and tracking changes in access privileges for the LAN, ACMS [Automated Case Management System], or any other software applications.” **IMPLEMENTED**
11. “Implement DoITT’s suggestion for developing a business recovery plan by purchasing a readily available off-the-shelf product; e.g., AIM/SAVE 2000 by Advanced Information Management. IMOA [Information Management and Operational Analysis] can use the software in gathering and organizing the required data. This software provides all the steps to assist IMOA in implementing a disaster recovery plan.” **IMPLEMENTED**
12. “Identify anti-virus software for the network and ensure that it is installed and operational on all the servers. It is also important to routinely update the virus detection patterns so that the network is shielded from newly developed viruses.” **IMPLEMENTED**
13. “Finalize the installation of the Norton Anti-Virus software throughout the network so that there will be a uniform anti-virus software protection that is operational on all the workstations.” **IMPLEMENTED**
14. “Change the parameters of the Netshield software to scan incoming data for viruses.” **IMPLEMENTED**

15. “Inform contractors of the contaminating effects of a virus in a network environment. IMO management should also provide guidelines and recommendations for installing anti-virus software packages, and, if possible, insert a clause into their contracts requiring that contractors install anti-virus software.” **IMPLEMENTED**
16. “Establish some form of documentation or logs for the following: daily LAN shift reports for operational purposes, system maintenance log for managerial purposes, backup logs (a checklist of file servers), and server and router configuration and settings for references purposes.” **IMPLEMENTED**
17. “Update the Network Operations Manual for Department of Employment Automated Information System Version 1.3.” **IMPLEMENTED**
18. “Determine the quantity of ‘Year 2000’ non-compliant equipment at DOE and contractor sites and evaluate whether a software patch can be applied to correct the internal system date routine or, if not, how and when the workstations will be replaced, before year 2000.” **IMPLEMENTED**
19. “Monitor software usage by using the software package, Norton Administrator, to centralize many of the network administrative functions. It should also make an effort to clean up the software, which is no longer under license or maintenance contract, but is still installed on the workstations.” **IMPLEMENTED**

New Findings and Recommendations

DOE does not test and update its disaster recovery plan annually, as required by Comptroller’s Directive #18, § 10.4, which states that “Periodic reviews and updates are necessary to insure that the business continuation plan remains current. A comprehensive test should be conducted annually.” According to DOE’s Director of Network Systems, the disaster recovery plan was last tested in November 1999. Annual testing of the plan is essential to ensure it is current and relevant so that it will function as intended in an emergency.

In addition, DOE’s disaster recovery plan does not identify an alternate processing site where DOE could resume critical data processing operations in the event of a disaster at the Data Center. Such a site is recommended by Directive 18. Moreover, the plan does not indicate under what circumstances the agency would declare a disaster. Directive 18 states that one of the “primary elements” of a disaster recovery plan is “a pre-arranged agreement” describing the circumstances under which a disaster is to be declared.

DOE has not has not regularly updated its inventory of workstations, network hardware and software, and other system components. § 10.5 of Directive 18 states that “special attention must be devoted to the accurate inventorying of workstation and PC technical specifications, configurations, network software and hardware, network operating hardware and software, and application software.” Finally, DOE has not updated its Network Operations Manual since June 1998 to take into account changes in its operations. Directive 18 § 9.7 states that agency information processing functions are to be “reviewed and updated periodically.”

We recommend that DOE ensure that its disaster recovery plan conforms to the requirements of Directive 18. Specifically DOE should:

- Update and conduct comprehensive tests of the plan annually.
- Arrange for an alternate processing site.
- Indicate and formalize under what circumstances the agency would declare a disaster.
- Update its inventory of workstations, network hardware and software and other system components as needed.
- DOE should also periodically update its Network Operations Manual to take into account changes in its operations.

Agency Response

The matters covered in this report were discussed with officials from DOE during and at the conclusion of this audit. A preliminary draft report was sent to DOE officials and discussed at an exit conference held on March 12, 2002. On March 13, 2002, we submitted a draft report to DOE officials with a request for comments. We received a written response from DOE on April 5, 2002. DOE agreed with the audit's findings and recommendations. The full text of the DOE response is included as an addendum to this report.

**OFFICE OF THE COMPTROLLER
NEW YORK CITY
DATE FILED: April 17, 2002**

INTRODUCTION

Background

The New York City Department of Employment (DOE) provides employment services to economically disadvantaged, unemployed, and under-employed people. DOE's Local Area Network (LAN) consists of five Compaq Proliant file servers (computers that store the data files and application programs) with Novell Netware 4.11 operating systems. The servers are connected to 135 workstations with Windows 95 or 98 operating systems. Each of the five servers performs a different data processing function including telecommunications, the Automated Case Management System (ACMS), and LAN backup processing.

DOE's Wide Area Network (WAN) connects its LAN file servers to the Department Of Information Technology and Telecommunications (DoITT) for access to the New York City Payroll Management System (PMS), Financial Management System (FMS), and Vendex. In addition, DOE receives and transmits data via dial-up modem to approximately 132 employment training contractors. Each contractor manages its own network and has DOE's ACMS application installed on its file servers. The contractors enter their transactions into ACMS daily. DOE then updates its master database daily by downloading the data from the contractors' file servers via dial-up modem.

Objectives, Scope, and Methodology

This follow-up audit determined whether the 19 recommendations contained in a previous audit entitled, *Audit Report of the Department of Employment Local Area Network/Wide Area Network* (Audit No.7A97-124, issued June 20, 1997), were implemented.

Audit fieldwork began in November 2001 and ended in December 2001. To meet our objectives, we:

- toured the Data Center and examined whether DOE implemented the physical and system security measures recommended in the previous audit;
- reviewed and analyzed DOE's disaster recovery plan;
- reviewed and examined the Help-desk Expert Automation Tool (HEAT) system to ensure that all user requests were accurately recorded, serviced, and tracked; and,
- examined a sample of 51 of the 135 DOE workstations to determine whether they contained uniform anti-virus program and password controls.

We used Comptroller's Internal Control and Accountability Directive 18, *Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems (Directive 18)*, issued June 29, 1998, as the audit's criteria.

This audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and included tests of the records and other auditing procedures considered necessary. This audit was performed in accordance with the City Comptroller's audit responsibilities, as set forth in Chapter 5, § 93, of the New York City Charter.

Agency Response

The matters covered in this report were discussed with officials from DOE during and at the conclusion of this audit. A preliminary draft report was sent to DOE officials and discussed at an exit conference held on March 12, 2002. On March 13, 2002, we submitted a draft report to DOE officials with a request for comments. We received a written response from DOE on April 5, 2002. DOE agreed with the audit's findings and recommendations. The full text of the DOE response is included as an addendum to this report.

RESULTS OF THIS FOLLOW-UP AUDIT

Previous Finding: “IMOA [Information Management and Operational Analysis] lacks the staff to effectively respond to outstanding problems associated with software change requests.”

Previous Recommendation #1: DOE should: “Submit a ‘new need’ request to OMB to hire two or three more persons to document and resolve current and future change requests.”

Previous Agency Response: “Within existing authorized headcount, the Department is in the process of hiring a Director of Network Systems, two Network Administrators, a part-time evening Network Administrator and a Programmer Analyst. With the exception of the Director of Network Systems, candidates for the above positions have been selected and are awaiting approval by the Vacancy Control Board. As soon as a candidate is identified for the Director of Network Systems, the Department will seek approval by the Vacancy Control Board. In addition, authorization to hire two FoxPro Programmer/Analysts and three Powerbuilder Programmer and Systems Analysts has been requested. These additional staff, along with current technical staff, will enhance the Department’s ability to resolve current and future change requests in a timely fashion.”

Current Status: IMPLEMENTED

Since the previous audit, DOE hired 13 people to fill positions in its Automated Information System Department (AIS), formerly known as IMOA. We believe that with this additional staffing, AIS can adequately track software change requests and ensure that they are resolved in a timely manner.

Previous Finding: “There is no standard method for capturing and recording change requests received from the users.”

Previous Recommendation #2: DOE should: “Design a problem reporting form with an identical format to the Problem Ticket Screen on the HEAT system. This form could be mailed or faxed to the Help Desk and entered into the HEAT System, thereby ensuring that all problems are captured on the HEAT system.”

Previous Agency Response: “The Department will ensure that all problems are captured on the HEAT Help Desk System.”

Current Status: IMPLEMENTED

DOE personnel now use a standard form for submitting change requests to the Help Desk. Users can mail or fax completed forms to Help Desk personnel so that all pertinent information can be recorded and tracked on the HEAT system. Therefore, we consider this recommendation implemented.

Previous Finding: “There is no request form that would enable contractors and internal users to enter the following information:

- the scope and description of the changes (what needs to be done and which programs and data files need to be changed);
- the programming resources required; and
- a managerial signature authorizing the change.”

Previous Recommendation #3: DOE should: “Modify the HEAT system so that analysts can review problem tickets on-line, and if they determine that a change request should be generated, they can bring up a new screen that captures the Problem Ticket Number and Problem Ticket Date from the system. This would then allow the analyst to enter information on the scope and description of the changes, programming resources required, and the name of the authorizing manager.”

Previous Agency Response: “A new screen will be generated in the HEAT system in order to track programming fixes. This new screen will contain information such as problem ticket being referenced, date, description of problem, description of necessary changes, programming/resources required, and name of authorizing manager. This approach will ensure that change requests can be referenced back to problem tickets. It will be implemented by December 31, 1997.”

Current Status: IMPLEMENTED

DOE developed two new information screens—the Journal screen and the Assignment/Reassignment screen—on the HEAT System that can be used by DOE analysts to track, record, and review programming fixes and related management authorizations. Therefore, we consider this recommendation implemented.

Previous Finding: “There is no standard method for capturing and recording change requests received from users.”

Previous Recommendation #4: DOE should: “Provide the Help Desk with formal procedures to regularly update users as to the status of their change requests.”

Previous Agency Response: “The Department has established a procedure for a 48 hour call-back to users as a Help Desk standard. With the hiring of additional staff, as per the response to recommendation #1, the Department will have the capacity to make call-backs to users in a more timely fashion and record this activity as a journal entry in the HEAT system. The journal entry will include the date, time of call, name of the DOE contact person, and the name of the user contacted. Recommendation #4 will be implemented by December 31, 1997.”

Current Status: IMPLEMENTED

DOE now has formal procedures describing the responsibilities of Help Desk personnel. These procedures require that the Help Desk respond to user problems within 48 hours and

record specific information about user problems on the HEAT System. Therefore, we consider this recommendation implemented.

Previous Finding: “The server room is not protected against unauthorized access. The server room door is always open, allowing non-network staff, consultants, and contractors full access to the room.”

Previous Recommendation #5: DOE should: “Ensure that all servers are equipped with console locks so that LAN administrators and operators can lock the servers whenever they leave the server room.”

Previous Agency Response: “The Department implemented this recommendation in May, 1997.”

Current Status: IMPLEMENTED

The entrance door to DOE's server room is now locked and an alarm system was installed and activated. Therefore, we consider this recommendation implemented.

Previous Finding: With regard to protecting file servers, the report stated “it is possible to prevent unauthorized access to the servers by use of password controls.”

Previous Recommendation #6: DOE should: “Password-protect the console for each server. This can easily be achieved by either using the Supervisory password or assigning a password through the Novell Monitor utility so that only authorized personnel can have access to these servers.”

Previous Agency Response: “The Department implemented this recommendation in May, 1997.”

Current Status: IMPLEMENTED

DOE has instituted adequate password protection on its five servers. Passwords, which are changed every 60 days, are required to obtain access to the servers. Therefore, we consider this recommendation implemented.

Previous Finding: “Most of the workstations at DOE are not protected against unauthorized use if they are left unattended. After users log on to the network, the workstations are not secured in the Windows environment.”

Previous Recommendation #7: DOE should: “In the short term, add a timeout function to workstations in the Windows environment by utilizing the screen saver option under the desktop of the control panel icon with the password-protected option turned on. In the long term, DOE could standardize workstation security by purchasing a software package, such as Intermission or LockIt.”

Previous Agency Response: “Once the network infrastructure is upgraded, the Department will activate the Windows timeout function in all workstations to enhance security. This will be implemented by December 31, 1997.”

Current Status: IMPLEMENTED

DOE added a timeout function within the Windows environment and has standardized it by using Screen Pass 3.0 to prevent user deactivation of this function on its 135 workstations. Therefore, we consider this recommendation implemented.

Previous Finding: “During our initial visit to the LAN area, we found three routers: a primary router in the server room, a backup router on one LAN administrator's desk, and a test router on the other LAN administrator's desk.”

Previous Recommendation #8: DOE should: “Secure the backup router and test router (when it is found) in either the server room or in a locked hardware storage room.”

Previous Agency Response: “The Department implemented this recommendation in May, 1997.”

Current Status: IMPLEMENTED

DOE's primary and backup routers are bolted to equipment racks in the server room, the racks are bolted to the floor, and the test router is stored in a locked cabinet. Accordingly, we consider this recommendation implemented.

Previous Finding: “DOE has no formal tracking process to monitor requests, by either DOE staff or consultants, for DOE software access privileges. There is no record of the requestor, the reasons for the access, or management authorization.”

Previous Recommendation #9: DOE should: “Develop a security request form to be completed by employees whenever they request an addition, modification, or deletion to their access privileges.”

Previous Agency Response: “The Department will develop written procedures using the HEAT system to record and track any modification in access privileges. Any modification in access privileges will be recorded as a journal entry in HEAT software, including

verification on the need for the change from the supervisor on the staff member requesting the change. This procedure will be implemented by December 31, 1997.”

Previous Recommendation #10: DOE should: “Create formal security procedures for recording and tracking changes in access privileges for the LAN, ACMS, or any other software applications.”

Previous Agency Response: “The Department will develop formal procedures using the HEAT system to record and track changes in access privileges for the LAN, ACMS, and any other software. Any modification in access privileges will be recorded as a journal entry in HEAT software, including verification of need of change from the supervisor of the staff member requesting the change. This procedure will be implemented by December 31, 1997.”

Current Status: IMPLEMENTED

DOE developed a standard request form within the HEAT system to be completed by Help Desk personnel and authorized by management when users request additions, modifications, or deletions to their access privileges. In addition, DOE developed formal procedures for recording and tracking changes in access privileges for all agency applications. Therefore, we consider recommendations #9 and #10 implemented.

Previous Finding: “IMOA does not have a formal disaster recovery plan for restoring ACMS processing at an alternate site in the event that the LAN at 220 Church Street becomes inoperable.”

Previous Recommendation #11: DOE should “Implement DoITT’s suggestion for developing a business recovery plan by purchasing a readily available off-the-shelf product; e.g., AIM/SAVE 2000 by Advanced Information Management. IMOA can use the software in gathering and organizing the required data. This software provides all the steps to assist IMOA in implementing a disaster recovery plan.”

Previous Agency Response: “The Department implemented DoITT’s suggestion. In February, 1997, we acquired a readily available off-the-shelf product, Palindrome Software, and are following the steps for implementing a disaster recovery plan.”

Current Status: IMPLEMENTED

DOE developed and tested a disaster recovery plan for restoring all agency applications, including ACMS, in the event the agency’s central LAN facility becomes inoperable. Therefore, we consider this recommendation implemented.

Previous Finding: “We found that DOE has installed an anti-virus software package, NetShield, on only four out of nine file servers.”

Previous Recommendation #12: DOE should: “Identify anti-virus software for the network and ensure that it is installed and operational on all the servers. It is also important to routinely update the virus detection patterns so that the network is shielded from newly developed viruses.”

Previous Agency Response: “The Department has already installed anti-virus software on all file servers located at 220 Church Street. On a monthly basis, AIS staff will obtain the latest virus signature files in order to shield the network from any new viruses. Uniform anti-virus software protection for all workstations will be installed when the upgrading of the Department’s network system is completed by December 31, 1997.”

Current Status: IMPLEMENTED

DOE installed McAfee Netshield on all agency servers and updates the software weekly. Therefore, we consider this recommendation implemented.

Previous Finding: “Only 8 out of 250 workstations had an anti-virus package loaded on the workstation.”

Previous Recommendation #13: DOE should: “Finalize the installation of the Norton Anti-Virus software throughout the network so that there will be a uniform anti-virus software protection that is operational on all the workstations.”

Previous Agency Response: “The Department will ensure that uniform anti-virus software protection for all workstations will be installed when the upgrading of the Department’s network system is completed by December 31, 1997.”

Current Status: IMPLEMENTED

DOE installed Norton Anti-Virus Software on all workstations. Therefore, we consider this recommendation implemented.

Previous Finding: “Netshield has a feature that allows it to scan for viruses coming into the server from the WAN, but DOE does not use this feature.”

Previous Recommendation #14: DOE should: “Change the parameters of the Netshield software to scan incoming data for viruses.”

Previous Agency Response: “The Department implemented this recommendation in May, 1997.”

Current Status: IMPLEMENTED

DOE now uses the McAfee Netshield software on its servers to scan incoming data for viruses. Therefore, we consider this recommendation implemented.

Previous Finding: “Contractors reported that many of their sites are not virus-protected.”

Previous Recommendation #15: DOE should: “Inform contractors of the contaminating effects of a virus in a network environment. IMOA Management should also provide guidelines and recommendations for installing anti-virus software packages, and, if possible, insert a clause into their contracts requiring that contractors install anti-virus software.”

Previous Agency Response: “The Department will distribute a memorandum to all DOE contractors regarding the contaminating effects of a virus and will provide guidelines by December 31, 1997 for purchasing and installing anti-virus software packages. Language on installing anti-virus software will be inserted in future contracts.”

Current Status: IMPLEMENTED

DOE issues an annual memo to its contractors reminding them of the need to install anti-virus software on their networks. DOE determined that it could not include language requiring its contractors to install anti-virus software. However, DOE attaches virus information sheets and software installation instructions to its contracts. Therefore, we consider this recommendation implemented.

Previous Finding: “IMOA has inadequate documentation for LAN administrative functions. We found the documentation incomplete in the following areas:

- logs for unscheduled downtime,
- system maintenance logs, and
- turnover documents for events such as file server down time and systems error message.”

Previous Recommendation #16: DOE should: “Establish some form of documentation or logs for the following:

- Daily LAN shift reports for operational purposes,
- System maintenance log for managerial purposes,
- Backup logs (a checklist of file servers), and
- Server and router configuration and settings for reference purposes. “

Previous Agency Response: “The Department will establish a log system to record the aforementioned information by December 31, 1997.”

Current Status: IMPLEMENTED

DOE now maintains logs that document daily LAN operations, system maintenance, and server and router configuration. We found that the logs were current and contained all required information. Therefore, we consider this recommendation implemented.

Previous Finding: IMOA has inadequate documentation for LAN administrative functions.”

Previous Recommendation #17: DOE should: “Update the Network Operations Manual for Department of Employment Automated Information System Version 1.3.”

Previous Agency Response: “The Department will update the Network Operations Manual for Department of Employment Automated Information System Version 1.3 by December 31, 1997.”

Current Status: IMPLEMENTED

In June 1998, subsequent to our prior audit, DOE updated its Network Operations Manual. Therefore, we consider this recommendation implemented.

Previous Finding: “The CSS 486 computers purchased for the AIS project are not ‘Year 2000’ compliant. We conducted tests on 30 CSS 486 personal computers by changing the system date to 12-31-99, 11:58 p.m. The system date reverted back to FRI 01-04-1980 when the machine was rebooted ten minutes later.”

Previous Recommendation #18: DOE should: ‘Determine the quantity of ‘Year 2000’ non-compliant equipment at DOE and contractor sites and evaluate whether a software patch can be applied to correct the internal system date routine or, if not, how and when the workstations will be replaced, before year 2000.’

Previous Agency Response: “The Department is currently engaged in the City-wide Year 2000 Project. This project required that each City agency complete a Year 2000 Compliance Survey. The Department is complying with the request to survey its own facilities and those of its contractors. The majority of our contractors have complied with the request and returned the completed surveys. The Department has forwarded the completed surveys to the Mayor’s Office of Operations. The Department will continue to follow-up with those contractors who have not yet returned the surveys.”

Current Status: IMPLEMENTED

The Comptroller’s Office audited DOE’s Year 2000 compliance (Audit No.7A99-116 entitled, *New York City Department of Employment’s Data Processing Preparation for the Year 2000*, issued February 9, 1999) and confirmed that all computers and applications were Year 2000 compliant. Therefore, we consider this recommendation implemented.

Previous Finding: “DOE has exceeded the number of authorized licenses for computer software. For example, there are 108 users for Microsoft Word for Windows version 6.0, but DOE is only licensed for 100 copies. Moreover, Microsoft PowerPoint version 4.0 is licensed for two copies, but there are 23 copies out on the workstations.”

Previous Recommendation #19: DOE should: ‘Monitor software usage by using the software package, Norton Administrator, to centralize many of the network administrative functions. It should also make an effort to clean up the software, which is no longer under license or maintenance contract, but is still installed on the workstations.’

Previous Agency Response: ‘‘The Department will monitor software usage using the Norton Administrator; will install/operate all software on the network; and will remove software from the PC workstations of DOE staff when the network infrastructure project is completed. This will be implemented by December 31, 1997.’’

Current Status: IMPLEMENTED

Although DOE is currently using Norton Administrator, they have plans to replace it with ZenWorks.¹ Norton Administrator is no longer supported by its manufacturer and therefore is an inadequate tool for detecting software that was recently installed on the network. As an added precaution, the Director of Network Systems stated that his staff also manually inspects all workstations monthly for unauthorized software. Therefore we consider this recommendation implemented.

NEW FINDINGS AND RECOMMENDATIONS

DOE's Disaster Recovery Plan Is Not In Compliance With Directive 18

DOE does not test and update its disaster recovery plan annually, as required by Comptroller’s Directive #18, § 10.4, which states that, ‘‘Periodic reviews and updates are necessary to insure that the business continuation plan remains current. A comprehensive test should be conducted annually.’’ According to DOE's Director of Network Systems the disaster recovery plan was last tested in November 1999. Annual testing of the plan is essential to ensure it is current and relevant so that it will function as intended in an emergency.

DOE’s disaster recovery plan does not identify an alternate processing site where DOE could resume critical data processing operations in the event of a disaster at the Data Center. Such a site is recommended by Directive 18. Moreover, the plan does not indicate under what circumstances the agency would declare a disaster. Directive 18 states that one of the ‘‘primary elements’’ of a disaster recovery plan is ‘‘a pre-arranged agreement’’ describing the circumstances under which a disaster is to be declared.

DOE has not regularly updated its inventory of workstations, network hardware and software and other system components. § 10.5 of Directive 18 states that ‘‘special attention must be devoted to the accurate inventorying of workstation and PC technical specifications,

¹ According to the literature provided, ZenWorks has many more features than Norton does, including the capability to enforce end-user desktop policies (which would eliminate the need for third party software) and hardware/software inventory monitoring.

configurations, network software and hardware, network operating hardware and software, and application software.” Finally, DOE has not updated its Network Operations Manual since June 1998 to take into account changes in its operations. Directive 18 § 9.7 states that agency information processing functions are to be “reviewed and updated periodically.”

Recommendations

We recommend that DOE ensure that its disaster recovery plan conforms to the requirements of Directive 18. Specifically DOE should:

1. Update and conduct comprehensive tests of the plan annually.

Agency Response: “The Department agrees with this recommendation. Beginning this year, the Department’s Information Management (IM) Unit intends to test the Disaster Recovery Plan by October of each year.”

2. Arrange for an alternate processing site.

Agency Response: “The Department agrees with this recommendation. DOE will conduct research into its options, including costs, for alternate data processing sites in the metropolitan area, during the next six months. Although DOE does not currently have in place arrangements for an alternate processing site, DOE does send weekly full backup tapes of the network data set to off-site storage in Connecticut. Thus, in the event of a disaster that does not disable the LAN itself, DOE can retrieve these tapes to restore its data set as of the end of the prior week.”

3. Indicate and formalize under what circumstances the agency would declare a disaster.

Agency Response: “DOE agrees with this recommendation. The circumstances under which the agency would declare a disaster are currently being drafted. This document will be incorporated into the Department’s Disaster Recovery Plan.”

4. Update its inventory of workstations, network hardware and software and other system components as needed.

Agency Response: “The Department agrees with this recommendation. DOE’s MIS will update the NDS (Network Directory Services) Objects in the Disaster Recovery Plan. These Objects or user ID’s show the number of workstations connected to the LAN. File server, Router, Hub and Switch hardware will be updated in the Visio Network Diagrams in the Disaster Recovery Plan. LAN Operating System (software) and other System components will also be updated into the Department’s Disaster Recovery Plan. This will be completed by May 2002. Going forward, it will be updated as needed.”

5. DOE should also periodically update its Network Operations Manual to take into account changes in its operations.

Agency Response: “The Department agrees with this recommendation. A re-draft of the Network Operations Manual has been prepared for preliminary internal review. A copy of the final revised manual will be forwarded to the Comptroller’s Office, when completed. Consideration of such operational changes, and the need to revise the Network Operations Manual will be re-enforced as part of the annual update of the agency’s Disaster Recovery Plan.”



DEPARTMENT OF EMPLOYMENT

220 Church Street, New York, New York 10013
www.nyc.gov

Betty Wu
Commissioner

April 2, 2002

Roger D. Liwer
Assistant Comptroller for Audits
Office of the New York City Comptroller
Bureau of Audits
1 Centre Street- Room 1100
New York, N.Y. 10007-2341

Re: Follow-Up Audit Report
On the Department of Employment's
Local Area Network/Wide Area
Network Environment
7F02-110

Dear Mr. Liwer:

Attached please find the Department of Employment's response to the draft of the New York City Comptroller's follow-up report cited above. Commissioner Wu is pleased to note that the Comptroller's Office agrees that the Department has implemented the nineteen (19) recommendations mentioned in the previous audit. Our response to the Follow-up Audit comments on the recommended corrective action and gives a tentative timeframe for implementation.

If there are any questions regarding this response, I can be contacted at (212) 442-2550.

Sincerely,

Richard J. Ronde, Director
Division of Audit and Review

C: Commissioner Betty Wu
Allen Monczyc- Deputy Commissioner
Bernie Schwartz- NYCCO
Sayeda Ali- NYCCO
Phyllis Atwater- DOE
Shahid Masood- DOE
Gregory Griffin-DOE

Recommendation # 1

DOE should update and conduct comprehensive tests of the plan annually.

Response # 1

The Department agrees with this recommendation. Beginning this year, The Department's Information Management (IM) Unit intends to test the Disaster Recovery Plan by October of each year.

Recommendation # 2

DOE should arrange for an alternate-processing site.

Response # 2

The Department agrees with this recommendation. DOE will conduct research into its options, including costs, for alternate data processing sites in the metropolitan area, during the next six months. Although DOE does not currently have in place arrangements for an alternate processing site, DOE does send weekly full backup tapes of the network data set to off-site storage in Connecticut. Thus, in the event of a disaster that does not disable the LAN itself, DOE can retrieve these tapes to restore its data set as of the end of the prior week.

Recommendation # 3

DOE should indicate and formalize under what circumstances the agency would declare a disaster.

Response # 3

DOE agrees with this recommendation. The circumstances under which the agency would declare a disaster are currently being drafted. This document will be incorporated into the Department's Disaster Recovery Plan.

Recommendation # 4

DOE should update its inventory of workstation, network hardware and software and other system components as needed.

Response # 4

The Department agrees with this recommendation. DOE's MIS will update the NDS (Network Directory Services) Objects in the Disaster and Recovery Plan. These Objects or user ID's show the number of workstations connected to the LAN. File server, Router, Hub and Switch hardware will be updated in Visio Network Diagrams in the Disaster and Recovery Plan. LAN Operating System (software) and other System components will also be updated into the Department's Disaster Recovery Plan. This will be completed by May 2002. Going forward, it will be updated as needed.

Recommendation # 5

DOE should also periodically update its Network Operations Manual to take into account changes in its operations.

Response # 5

The Department agrees with this recommendation. A re-draft of the Network Operations Manual has been prepared for preliminary internal review. A copy of the final revised Manual will be

forwarded to the Comptroller's Office, when completed. Consideration of such operational changes, and the need to revise the Network Operations Manual will be re-enforced as part of the annual update of the agency's Disaster Recovery Plan.