AUDIT REPORT

CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
BUREAU OF FINANCIAL AUDIT
WILLIAM C. THOMPSON, JR., COMPTROLLER

Follow-up Audit Report on the Department of Health and Mental Hygiene Wide Area Network

7F04-139

June 30, 2004

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, N.Y. 10007-2341

WILLIAM C. THOMPSON, JR.
COMPTROLLER

To the Citizens of the City of New York

Ladies and Gentlemen:

In accordance with the Comptroller's responsibilities contained in Chapter 5, §93, of the New York City Charter, my office has reviewed the implementation status of eight recommendations made in an earlier audit issued June 20, 2001, entitled *Audit Report of the New York City Department of Health's Wide Area Network*.

The results of our audit, which are presented in this report, have been discussed with the Department of Health and Mental Hygiene officials, and their comments have been considered in preparing this report.

Audits such as this provide a means of ensuring that City agencies have adequate controls in place to protect their equipment and records from inappropriate access and use.

I trust that this report contains information that is of interest to you. If you have any questions concerning this report, please contact my Audit Bureau at 212-669-3747 or e-mail us at audit@Comptroller.nyc.gov.

Very truly yours,

Will C.

William C. Thompson, Jr.

WCT/gr

Report: **7F04-139**
Filed: **June 30, 2004**

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

Follow-up Audit Report on the Department of Health and Mental Hygiene Wide Area Network

7F04-139

AUDIT REPORT IN BRIEF

This is a follow-up audit to determine whether the Department of Health and Mental Hygiene (DOHMH) (formerly the Department of Health) implemented the eight recommendations made in a previous audit of its Wide Area Network (WAN). In this report, we discuss the eight recommendations from the prior audit in detail, as well as the implementation status of each recommendation.

In Fiscal Year 2001, our office conducted an audit to evaluate whether DOHMH was in compliance with the City standards applicable to regulating its WAN environment. The audit also determined whether DOHMH had adequate computer network maintenance and security controls, as well as adequate computer operations and contingency plans. The audit found a number of weaknesses existing in DOHMH's WAN environment. Specifically, DOHMH: lacked policies and procedures regarding its computer operations, system access, and data security; did not install cameras and fire detection systems in some of its data centers to ensure their physical security; and did not have a complete disaster recovery plan for its computer environments.

<u>Audit Findings and Conclusions</u>

We made eight recommendations in the previous audit, DOHMH has implemented five, partially implemented two, and did not implement one.

To address the unresolved issues from the prior audit, we recommend that DOHMH:

- Install a state-of-the-art fire detection and suppression system in each of its data centers.
- Include the names, addresses, and telephone numbers of all people who may be required in any backup or recovery scenario in its disaster recovery plan.
- Install additional video cameras in its Worth Street location, make the back-up site's cameras operational, and ensure that the data centers are sufficiently lighted so that transmitted images may be seen.

INTRODUCTION

Background

DOHMH was created in 2002 by a merger of the Department of Health (DOH) and the Department of Mental Health, Mental Retardation and Alcoholism Services. DOHMH's mission is to protect the health and mental health of all City residents through health-promotion and disease-prevention programs, and to enforce City health regulations. Department programs and activities include: health information and laboratory services; disease investigations and surveillance; inspecting, permitting, licensing, and monitoring a wide range of enterprises related to public health; maintaining the City's health-related vital statistics; and registering and issuing birth and death certificates.

DOHMH supports both mainframe and wide area network (WAN) applications for its day-to-day business activities. The Department of Information Technology and Telecommunications maintains DOHMH's mainframe computer systems (hardware and software); DOHMH is responsible for its mainframe user applications. The DOHMH Management Information Services unit (MIS) is responsible for maintaining the computer network and telecommunication connections among DOHMH sites. MIS responsibilities include: supporting all the WAN users, connecting equipment for each workgroup, upgrading computer equipment, and initiating proposals for computer staffing and new technology.

The DOHMH WAN connects users at 42 buildings. Each site has one or more floors containing computer equipment that provides users with access to the network. Each site is categorized as "Administrative" (if it contains a data center and can also service users) or "Clinic" (if it only services users).

Objectives

This follow-up audit determined whether DOHMH implemented the eight recommendations made in the previous report, *Audit Report of the New York City Department of Health's Wide Area Network* (7A01-067, issued June 20, 2001).

Scope and Methodology

The time period reviewed in this audit was March through June 2004.

To determine the implementation status of the recommendations, we:

- Interviewed DOHMH officials;
- Toured the six data centers to ascertain whether DOHMH implemented the physical security measures recommended in the previous report;
- Reviewed and analyzed the policies and procedures for the DOHMH Help Desk;

- Reviewed and analyzed the policies and procedures for network data, general security, remote dial-in-access, assignment of temporary user accounts, and accessing the WAN environment;

- Reviewed and evaluated the disaster recovery plan to ensure that its medical billing applications are included; and

- Reviewed and evaluated the detailed manual temporary processing contingency plans for the applications maintained by DoITT.

For the audit criteria to assess system controls, we used: the *Federal Information Processing Standards* (FIPS); standards of the National Institute of Standards and Technology (NIST); the Department of Investigation's *Citywide Information Security Architecture, Formulation and Enforcement Policies*; and the New York City Comptroller's Internal Control Directive 18, "Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems."

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 audit responsibilities of the City Comptroller, as set forth in Chapter 5, §93, of the New York City Charter.

Discussion of Audit Results

The matters covered in this report were discussed with DOHMH officials during and at the conclusion of this audit. A preliminary draft was sent to DOHMH officials and was discussed at an exit conference held on May 26, 2004. On June 1, 2004, we submitted a draft report to DOHMH officials with a request for comments. We received a written response from DOHMH officials on June 16, 2004, in which they agreed that the "data centers still lack fire detection and suppression systems." In this regard, DOHMH stated that "the cost of implementing non-water based, oxygen depletion, fire suppression systems, requiring an air-sealed room with specialized HVAC systems, was prohibitive." Instead, DOHMH "conducted a risk-based assessment . . . and have prepared a modified plan that addresses all identified risks in a more cost effective and reasonable approach." DOHMH officials, however, believe that they fully implemented our recommendations dealing with including the names, addresses, and telephone numbers of all people who may be required in any backup or recovery scenario in its disaster recovery plan and installing and using video cameras at the data centers.

The full text of the Department's comments is included as an addendum of this report.

RESULTS OF FOLLOW-UP AUDIT

Previous Finding: "DOH does not have written policies and procedures covering all aspects of its computer operations."

Previous Recommendation #1: "DOH should establish written policies and procedures related to:

- the day-to-day responsibilities of MIS and Help Desk personnel;
- general security issues; and
- temporary user accounts."

Previous DOH Response: "Written policies and procedures:

- for the day-to-day responsibilities of MIS and Help Desk personnel were provided to the auditors at the Exit Conference;
- for general security issues will be completed by August 15th; and
- will include our restrictive policy for temporary user accounts."

Current Status: IMPLEMENTED

DOHMH provided written policies and procedures covering the day-to-day responsibilities of MIS and Help Desk personnel, general security issues, and guidelines for temporary user accounts. Accordingly, we consider Recommendation #1 implemented.

Previous Finding: "DOH does not require that its users periodically change their passwords. In addition, DOH did not implement the dial-back feature available on its network"

Previous Recommendation #2: "DOH should implement and enforce policies requiring that:

- users periodically change their passwords; and
- its MIS staff activates the dial-back feature on the network."

Previous DOH Response: With regard to password changes, DOH's response indicated that it "has already put new procedures into effect . . . [and] has required users to change their passwords as of May 21, 2001."

With regard to activating the dial-back feature on the network DOH officials stated that "we believe that we are in compliance with the spirit of Directive #18 and do not agree with the recommendation to change our procedures. Remote DOH users do not access the network or their own PCs. They are solely allowed access to the DOH Intranet, and through the Intranet, access to their email. Users are not able to access agency applications or local or shared files through dial-in. In addition, users are authenticated through the use of a password to gain entry to the Intranet and a separate password to gain email access. As such, DOH does not believe that the absence of a dial-back requirement presents any risk to agency information assets. In addition, its use would prevent mobile DOH employees from accessing their email when traveling."

Current Status: IMPLEMENTED

DOHMH provided its policies and procedures requiring users to periodically change their passwords. Further, DOHMH provided a report showing that passwords were changed in accordance with the procedure. Also, DOHMH has purchased and installed a hardware device known as "Demilitarized Zone," which is placed between the DOHMH WAN and the user computers at remote sites to secure the remote access to the WAN. DOHMH is in the process of connecting the user computers at remote sites to this device. Accordingly, we consider Recommendation #2 implemented.

Previous Finding: "Other than user passwords, DOH has no security measures in place to protect against misuse of confidential data."

Previous Recommendation #3: "DOH should determine the types and extent of its data that current law requires be kept confidential, or where it may be desirable to keep data confidential even though current law does not require it. DOH should then enhance the security of the data by implementing one or more data security solutions, such as data encryption."

Previous DOH Response: "DOH has always been aware of the types and extent of data which are required to be kept confidential, and substantial efforts and continual attention is paid to this issue by the DOH General Counsel. Implementation is ongoing. The DOH data security architecture and plan will be implemented by January, 2002."

Current Status: IMPLEMENTED

DOHMH provided documentation that contains its criteria for determining what types of data should be kept confidential. Further, DOHMH also implemented data encryption methods that employees use when transmitting the confidential data. Accordingly, we consider Recommendation #3 implemented.

Previous Finding: "DOH needs to improve the security of its data centers by installing improved fire detection systems and by upgrading its video monitoring devices."

Previous Recommendation #4: "DOH should ensure that all sites have adequate fire detection and suppression systems. Special attention should be paid to the Administrative sites and the five Clinic sites that contain backup servers."

Previous DOH Response*:* "DOH has prioritized our two largest data centers for completion of these systems by June, 2002. We will request capital funding for the remaining sites, and upon funding, expect all sites to be completed by fiscal year 2005."

Current Status: NOT IMPLEMENTED

One of the six DOHMH data centers has a fire detection system and an obsolete water-based suppression system. The remaining data centers, including the disaster recovery hot site, do not have any fire detection or suppression systems. Accordingly, we consider Recommendation #4 not implemented.

Previous Recommendation #5: "Install and use video cameras at the data centers."

Previous DOH Response: "DOH has prioritized our two largest data centers for completion of this project by June, 2001. We will request capital funding for the remaining sites, and upon funding, expect all sites to be completed by fiscal year 2003."

Current Status: PARTIALLY IMPLEMENTED

Although all seven DOHMH data centers have video cameras, we found that the images transmitted to the central monitoring area in the MIS Director's office are too dark for viewing. In addition, we believe that the Worth Street data center and the Laboratory need additional cameras to cover the entire data center—this center has only one camera. Finally, the backup site's cameras are not operational. Accordingly, we consider Recommendation #5 partially implemented.

Previous Finding: "Although DOH issued a "Disaster Recovery Plan . . . it was deficient, in that the plan did not: (1) describe each application involved in the plan, (2) describe hardware and software inventories, (3) list sufficient detail information about the people involved in the disaster recovery process, (4) list the vendors that are considered necessary during a recovery scenario, and (5) specify the servers used for recovery purposes.

"Moreover, the plan does not contain:

- Recovery procedures for one of DOH's two applications—the Medical Billing System—controlled by a third-party vendor.

- Manual temporary processing contingency procedures covering DOH mainframe applications being handled by DoITT."

Previous Recommendation #6: "Ensure that its Disaster Recovery Plan contains detailed recovery information specific to each application, including the hardware and software components necessary to run the application. In addition, the plan should list the names, addresses, and telephone numbers of all people who may be required in any backup or recovery scenario."

Previous DOH Response: "This plan will be implemented by January, 2002."

Current Status: PARTIALLY IMPLEMENTED

The disaster recovery plan provided by DOHMH contains detailed recovery information for all the applications. The plan also includes a list of all the applications and a list of the hardware and software that run these applications. However, the plan does not list the names, addresses, and telephone numbers of all people who may be required in the event of a disaster. Accordingly, we consider Recommendation #6 partially implemented.

Previous Recommendation #7: "Develop a plan covering its medical billing application, which is run by a third-party vendor."

Previous DOH Response: "The vendor has submitted a plan which is under review."

Current Status: IMPLEMENTED

DOHMH has created a detailed disaster recovery plan to cover its Patient Information and Billing system, which is run by a third-party vendor. Therefore, we consider Recommendation #7 implemented.

Previous Recommendation #8: "Develop detailed manual temporary processing contingency plans for the applications maintained by DoITT."

Previous DOH Response: "Manual processing exists for customer-service related, mission critical procedures, to be performed by Vital Records in the event of a mainframe failure, which includes issuance of certified copies of birth and death certificates, and looking-up birth and death records. Documentation will be completed by August 1, 2001.

"Procedures exist to track the status of TB cases. The Tuberculosis Control Program receives a download from the mainframe file on a monthly basis to ensure that surveillance staff would be able to refer to the status of current TB cases if the mainframe cannot be accessed. Formal procedures will be developed by September 1, 2001."

Current Status: IMPLEMENTED

DOHMH has created contingency plans for tracking both the vital records and the status of tuberculosis (TB) cases that are maintained by DoITT in the event of a disaster. Accordingly we consider Recommendation #8 implemented.

RECOMMENDATIONS

To address the issues that still exist, we recommend that DOHMH:

1. Install a state-of-the-art fire detection and suppression system in each of its data centers.

DOHMH Response: "DOHMH agrees that the relevant recommendation from the prior audit has not been implemented. DOHMH agreed to prioritize the implementation of fire detection and suppression systems in our various data centers. However, the cost of implementing non-water based, oxygen depletion, fire suppression systems, requiring an air-sealed room with specialized HVAC systems, was prohibitive.

"As a result, DOHMH conducted a risk-based assessment relative to fire risk in our data centers, and have prepared a modified plan that addresses all identified risks in a more cost effective and reasonable approach. In summary, DOHMH identified four principal risks. They are:

- loss of information assets
- loss of business continuity
- loss of physical equipment
- increased risk of electrical fire to building

"DOHMH's current Disaster and Recovery Plan, which was provided as part of this follow-up audit, sufficiently addresses the first two identified risks, relative to protection of information assets and business continuity.

"Regarding the loss of physical equipment in the event of a fire, DOHMH currently replaces all data center equipment on a five-year replacement schedule to maintain technological relevancy. The amortized cost of replacing data center equipment earlier in the replacement cycle would be far less than the cost associated with the installation of the type of fire suppression system described above.

"Finally, DOHMH acknowledges that the concentration of equipment in a data center presents an increased risk of an electrical fire to the building. As such, DOHMH agrees to install remote fire detection capability, in accordance with existing building fire detection systems, and to evaluate and install chemical fire suppression systems at these locations. DOHMH will develop a project plan for this work by the end of 2004."

2. Include the names, addresses, and telephone numbers of all people who may be required in any backup or recovery scenario in its disaster recovery plan.

DOHMH Response: "The recommendation from the prior audit called for five improvements to the agency's disaster recovery plan. This issue was the only one questioned by the auditors. DOHMH's existing communications strategy for reaching out to employees needed during any backup or recovery scenario not only satisfies, but far exceeds the intent of that recommendation. As such, DOHMH believes the audit recommendation to be fully implemented.

“DOHMH currently utilizes, agency-wide, a very extensive communications strategy that ensures that key agency employees can be contacted to respond to emergencies, including any technology-related emergencies. This strategy has a number of major components:

- a centralized data repository of employee contact and skills information
- dedicated resources to continuously work with all employees to keep contact and skills information current
- on-line access to employee contact information
- backup electronic and hard copies of employee contact information, refreshed on a routine basis and stored in multiple locations
- additional hard copies of IT employees contact information, refreshed on a routine basis and held by all IT section leaders that may be called upon to respond to any backup or disaster recovery scenario.

“The inclusion of employee contact information in hard copy format in the Disaster and Recovery Plan prevents it from being kept up to date, and would be far less effective than the standard methodology used throughout the agency to effectively keep all contact information up to date and immediately available to those who need it.”

Auditor’s Comments: In the event of a disaster, the first component to be affected would be the extensive communication system that DOHMH indicates will ensure that key personnel will be contacted. As seen in previous disasters (e.g., 9/11 and the blackout of 2003), computer and telephone lines were severely impacted. While we agree that distributing hardcopies of contact information to multiple locations is acceptable; we do not see how including a hard copy in the Disaster Recovery Plan will prevent it from being kept up to date, and would be less effective than DOHMH’s stated methodology.

3. Install additional video cameras in its Worth Street data center and the Laboratory, make the back-up site’s cameras operational, and ensure that the data centers are sufficiently lighted so that the transmitted images may be seen.

DOHMH Response: “DOHMH believes that this is a new recommendation, as the original recommendation, to ‘install and use video cameras at the data centers’ has been fully implemented and verified by this follow-up audit.

“At the time of the audit, the backup site was under construction and inoperable, which is why the video camera equipment was installed but not functioning at that location. Regarding the other components of this recommendation—to install additional cameras and to provide sufficient lighting—DOHMH agrees to consider these suggestions and to determine whether action is appropriate.”

Auditor's Comments: We do not agree with DOHMH's assessment that it complied with the report's recommendation to install and use video cameras in the data centers'. Obviously, the recommendation assumed that a sufficient number of cameras would be installed to cover the entire area of each data center and that the images captured on the cameras would be visible—without such coverage and visibility, the cameras are useless.

THE CITY OF NEW YORK
DEPARTMENT OF HEALTH AND MENTAL HYGIENE
OFFICE OF THE COMMISSIONER

125 WORTH STREET, CN-28
NEW YORK, NY 10013
NYC.GOV/HEALTH

THOMAS R. FRIEDEN, M.D., M.P.H.
COMMISSIONER
TEL (212) 788-5261
FAX (212) 964-0472

June 16, 2004

Greg Brooks
Deputy Comptroller for Policy, Audits, Accountancy & Contracts
The City of New York Office of the Comptroller
1 Centre Street, Room 530 South
New York, New York 10007-2341

Dear Mr. Brooks:

The Department of Health and Mental Hygiene (DOHMH) is responding to your draft follow-up audit report on the DOHMH Wide Area Network. We appreciate your acknowledgement that we have fully implemented five of the eight recommendations in the original audit, issued in FY2001. We believe, however, that we have fully implemented two other recommendations, which your auditors identify as partially implemented.

We agree that our data centers still lack fire detection and suppression systems. The cost of implementing non-water based fire suppression systems was prohibitive. We have prepared a modified plan that addresses all identified risks in a more cost effective and reasonable approach. We will soon have a backup main data center, so that there would be minimal data loss in case of a fire, as well as the ability to resume operations.

Attached is a response to the findings and the new recommendations. We appreciate the courtesy and professionalism of your audit staff in the performance of this audit. If you have any questions or need further information, please contact Charles Troob, Assistant Commissioner, Business Systems Improvement at (212) 788-4757.

Sincerely,

Isaac B. Weisfuse for

Thomas R. Frieden, M.D., M.P.H.
Commissioner

cc: Vince Liquori, Assistant Director for Support Services

TRF/ct

RESPONSE TO CITY COMPTROLLER'S FOLLOW-UP AUDIT REPORT ON THE DEPARTMENT OF HEALTH AND MENTAL HYGIENE WIDE AREA NETWORK (7FE04-139)

Recommendation 1

Install a state of the art fire detection and suppression system in each of its data centers

DOHMH agrees that the relevant recommendation from the prior audit has not been implemented. DOHMH agreed to prioritize the implementation of fire detection and suppression systems in our various data centers. However, the cost of implementing non-water based, oxygen depletion, fire suppression systems, requiring an air-sealed room with specialized HVAC systems, was prohibitive.

As a result, DOHMH conducted a risk-based assessment relative to fire risk in our data centers, and have prepared a modified plan that addresses all identified risks in a more cost effective and reasonable approach. In summary, DOHMH identified four principal risks. They are:

- loss of information assets
- loss of business continuity
- loss of physical equipment
- increased risk of electrical fire to building

DOHMH's current Disaster and Recovery Plan, which was provided as part of this follow-up audit, sufficiently addresses the first two identified risks, relative to protection of information assets and business continuity.

Regarding the loss of physical equipment in the event of a fire, DOHMH currently replaces all data center equipment on a five-year replacement schedule to maintain technological relevancy. The amortized cost of replacing data center equipment earlier in the replacement cycle would be far less than the cost associated with the installation of the type of fire suppression system described above.

Finally, DOHMH acknowledges that the concentration of equipment in a data center presents an increased risk of an electrical fire to the building. As such, DOHMH agrees to install remote fire detection capability, in accordance with existing building fire detection systems, and to evaluate and install chemical fire suppression systems at these locations. DOHMH will develop a project plan for this work by the end of 2004.

Recommendation 2

Include the names, addresses and telephone numbers of all people who may be required in any backup or recovery scenario in its disaster recovery plan.

The recommendation from the prior audit called for five improvements to the agency's disaster recovery plan. This issue was the only one questioned by the auditors. DOHMH's existing communications strategy for reaching out to employees needed during any backup or recovery scenario not only satisfies, but far exceeds the intent of that recommendation. As such, DOHMH believes the audit recommendation to be fully implemented.

DOHMH currently utilizes, agency-wide, a very extensive communications strategy that ensures that key agency employees can be contacted to respond to emergencies, including any technology-related emergencies. This strategy has a number of major components:

- a centralized data repository of employee contact and skills information
- dedicated resources to continuously work with all employees to keep contact and skills information current
- on-line access to employee contact information
- backup electronic and hard copies of employee contact information, refreshed on a routine basis and stored in multiple locations
- additional hard copies of IT employees contact information, refreshed on a routine basis and held by all IT section leaders that may be called upon to respond to any backup or disaster recovery scenario.

The inclusion of employee contact information in hard copy format in the Disaster and Recovery Plan prevents it from being kept up to date, and would be far less effective than the standard methodology used throughout the agency to effectively keep all contact information up to date and immediately available to those who need it.

Recommendation 3

Install additional video cameras in its Worth Street location, make the back-up site's cameras operational, and ensure that the data centers are sufficiently lighted so that transmitted images may be seen.

DOHMH believes that this is a new recommendation, as the original recommendation, to 'install and use video cameras at the data centers' has been fully implemented and verified by this follow-up audit.

At the time of the audit, the backup site was under construction and inoperable, which is why the video camera equipment was installed but not functioning at that location.

Regarding the other components of this recommendation--to install additional cameras and to provide sufficient lighting--DOHMH agrees to consider these suggestions and to determine whether action is appropriate.