

AUDIT REPORT



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

Follow-up Audit Report on Department of Juvenile Justice Data Centers

7F04-105

March 10, 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 performed a follow-up audit to determine whether the New York City Department of Juvenile Justice (DJJ) implemented recommendations made in a previous audit of the agency's data centers. The results of our audit, which are presented in this report, have been discussed with DJJ officials, and their comments have been considered in the preparation of this report.

Audits such as this provide a means of ensuring that City agency data centers are operated in an effective, efficient, and in a cost-effective manner.

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,

A handwritten signature in cursive script that reads 'William C. Thompson, Jr.'.

William C. Thompson, Jr.

WCT/GR

Report: 7F04-105
Filed: March 10, 2004

*Office of the Comptroller
Bureau of Financial Audit
EDP Audit Division*

**Follow-up Audit Report on
The Department of Juvenile Justice
Data Centers**

7F04-105

AUDIT REPORT IN BRIEF

This follow-up audit determined whether the New York City Department of Juvenile Justice (DJJ) implemented recommendations made in a previous audit of the agency's data centers. In this report, we discuss in detail the seven recommendations from the prior audit, as well as the implementation status of each recommendation.

In Fiscal Year 2002, the Comptroller's Office conducted an audit to evaluate the adequacy of the data centers' disaster recovery plans, program-change control procedures, data security procedures, physical security procedures, and operational procedures to protect DJJ computer assets and information. The audit also determined whether the agency complied with the Comptroller's Internal Control and Accountability Directive 18, "Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems."

Audit Findings and Conclusions

Of the seven recommendations in the prior audit, DJJ has implemented five and partially implemented one; one recommendation is no longer applicable. In addition, this audit identified weaknesses in access controls over DJJ's network.

To address the unresolved issue from the prior audit, DJJ should:

- Include in its policies and procedures a list of individuals responsible for network program changes, disaster recovery, and security issues.

To address the new issue identified during this audit, DJJ should:

- Develop written policies and procedures for removing multiple user IDs, inactive IDs, and IDs of individuals no longer working for the agency.

- Require that its personnel department notify MIS of those employees leaving the agency so that their user IDs can be removed from the system.

INTRODUCTION

Background

The Department of Juvenile Justice (DJJ) provides detention, aftercare, and delinquency prevention services to juveniles in New York City. Individuals detained in DJJ facilities include juvenile delinquents whose cases are pending, and those whose cases have been adjudicated and who await transfer to State Office of Children and Family Services facilities. DJJ operates secure and non-secure detention facilities and a community-based intervention program.

DJJ's mission-critical application is the Criminal Justice Information System (CJIS), which enables DJJ to track the movement of juveniles between detention facilities and the courts. In addition, this system allows DJJ to access information from the Department of Probation, the Law Department, and the Police Department. The CJIS mainframe application is maintained and operated by the Department of Information, Technology, and Telecommunications (DoITT).

This audit reviewed DJJ data centers, namely, those for: the Central Office in Manhattan; the Crossroads Juvenile Detention Center in Brooklyn; and the Bridges Juvenile Detention Center and the Horizon Juvenile Detention Center in the Bronx.

Objectives

This follow-up audit determined whether DJJ implemented the seven recommendations contained in the previous audit, *Audit of the City of New York's Department of Juvenile Justice's Data Centers* (Audit # 7A01-146, issued August 6, 2001).

Scope and Methodology

The time period covered by this audit was October 2003 to December 2003.

To determine the implementation status of the previous audit's recommendations, we:

- Toured the four data centers to ascertain whether DJJ implemented the physical and system security measures recommended in the previous audit;
- Reviewed and analyzed DJJ disaster recovery documentation;
- Reviewed and analyzed the DJJ tape back-up process;
- Tested the DJJ automatic time-out function;

- Reviewed and analyzed the security procedures for DJJ network data, remote dial-in-access, assignment of passwords, and accessing the Local Area Network (LAN), Internet, and mainframe environment for tracking user activity; and
- Reviewed and analyzed the DJJ Internet Security Architecture Plan and results from its penetration testing.

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 audit responsibilities of the City Comptroller audit 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 DJJ officials during and at the conclusion of this audit. A preliminary draft report was sent to DJJ officials and was discussed at an exit conference held on January 22, 2004. On January 27, 2004, we submitted a draft report to DJJ officials with a request for written comments. We received a written response from DJJ officials on February 12, 2004. DJJ stated that it "substantially agrees with" the audit recommendations. The full text of their comments is included as an addendum to this report.

RESULTS OF FOLLOW-UP AUDIT

Previous Finding: “Terminals do not automatically disconnect users.”

Previous Recommendation #1: “Implement an automatic time-out function to disconnect User log-on sessions after a specified period of user inactivity on the system.”

Previous DJJ Response: “Currently all users are forced off the network at midnight each night for two hours so that the backup systems at each site can run. In response to the audit, we have activated the Novell screensaver lockout feature. After thirty minutes of inactivity, the workstation screensaver is activated, which disables the computer and can only be accessed again by entering the users’ login password.”

Current Status: IMPLEMENTED

The MIS Director demonstrated an automatic time-out function that disconnects user log-on sessions after 20 minutes of inactivity. Accordingly, we consider recommendation #1 implemented.

Previous Finding: “Computer systems do not generate audit trails.”

Previous Recommendation #2: “Reactivate the AUDITCON audit trail function on the agency’s systems or acquire and utilize another software package that generates audit trails of user activity.”

Previous DJJ Response: “We activated AUDITCON at the auditor’s suggestion and it severely degraded network operations. In compliance with your recommendation, we have ordered LT Auditor from Blue Lance, Inc. to generate audit trails of user activity.”

Current Status: IMPLEMENTED

In September 2001, DJJ installed new software on its network that generates audit trails. In addition, MIS generates monthly reports that are used to monitor all network activity. Accordingly, we consider recommendation #2 implemented.

Previous Finding: “The Microcomputer Policies and Procedures do not satisfy Comptroller’s Directive 18.”

Previous Recommendation #3: “Create policies, procedures, and standards that address all aspects of its information systems environment, emphasizing the separation of duties and compliance with the requirements of Comptroller’s Directive 18.”

Previous DJJ Response: “The Department is currently working to upgrade its policies and procedures to address all aspects of its information systems environment in compliance with Comptroller’s Directive 18.”

Current Status: PARTIALLY IMPLEMENTED

DJJ has policies and procedures that are adequate for the management, protection, and control of its network information processing systems, including their connections to the Internet and other City networks through DoITT. However, the procedures do not address the mainframe environment. Since DoITT is responsible for servicing the mainframe, the procedures should list those DoITT officials responsible for program changes, disaster recovery, and security issues. Accordingly, we consider recommendation #3 only partially implemented.

Previous Finding: “Environmental security is inadequate.”

Previous Recommendation #4: “Strengthen its data center environmental security at all locations by installing an alternate fire-suppression system and humidity controllers. In addition, the Central Office data center window should be replaced with shatterproof glass.”

Previous DJJ Response: “The Department of Juvenile Justice will explore the feasibility of implementing this recommendation.”

Current Status: IMPLEMENTED

We found that DJJ has taken measures to strengthen its data center environmental security. Specifically, DJJ installed an alternate fire-suppression system and humidity controllers, and replaced the Central Office data center window with shatterproof glass. Accordingly, we consider this recommendation implemented.

Previous Finding: “There is no back-up generator at the Central Office.”

Previous Recommendation #5: “Obtain a backup generator for the Central Office.”

Previous DJJ Response: “We disagree with this recommendation. The Department currently operates three secure detention facilities with backup generators. The Department’s Wide Area Network configuration allows computer operations to be transferred to anyone of these facilities. This will allow DJJ to maintain the same level of internal service if a power outage or disaster occurs at the Central Office.”

Previous Auditor Comment: “We acknowledge that in the event that Central Office computers are disrupted, the Central Office has the ability to transfer its computer operations to one of DJJ’s three secure detention facilities. While this provides adequate back-up coverage to Central Office operations, it does not ensure that DJJ’s four group

homes (non-secure detention facilities) have access to CJIS—DJJ’s mission-critical application—if the Central Office computer operations are interrupted. The four group homes can access CJIS only through the Central Office and do not have the equipment needed to interface with the three secure detention facilities. Therefore, we repeat our recommendation to obtain a back-up generator.”

Current Status: NO LONGER APPLICABLE

DJJ’s network has been reconfigured to allow for transfer of its computer operations to any one of its four facilities in the event of a power outage. Accordingly, there is no need for DJJ to install a back-up generator. We therefore, consider recommendation #5 no longer applicable.

Previous Finding: “DJJ’s locations do not maintain records of on-site back-up tapes.”

Previous Recommendation #6: “Maintain a record of all back-up tapes received from other data centers as well as those tapes sent to the off-site location.”

Previous DJJ Response: “The Department has instituted logbooks and procedures for tracking backup tapes movement.”

Current Status: IMPLEMENTED

MIS now maintains logbooks to track back-up tapes. Accordingly, we consider recommendation #6 implemented.

Previous Finding: “The DJJ Internet Security Architecture Plan does not address penetration testing.”

Previous Recommendation #7: “Include penetration testing in the agency’s *Internet Security Architecture Plan*.”

Previous DJJ Response: “The Department of Juvenile Justice has been informed by the Department of Investigation that they will be conducting the penetration test. They have reviewed the configurations and logs of all our penetration detection software. The testing will be done through Cybercop Monitor and Scanner.”

Current Status: IMPLEMENTED

DJJ included penetration testing in its *Internet Security Architecture Plan*. Therefore, we consider recommendation #7 implemented.

NEW ISSUE

Access Control Weaknesses

Directive 18 states that “there are many software based controls that can be employed to help protect the information processing environment.” One of these controls is to restrict access to only those users who are authorized to access information on the system. User identification (ID) and passwords are among the most widely used forms of access control. In addition, Comptroller’s Directive 18, §8.1.2, states, “Active password management includes deactivation of inactive user accounts and accounts for employees whose services have terminated.”

DJJ provided a list of 549 “active” user IDs. Our review disclosed that 176 of these IDs are assigned to individuals who are not listed on the City’s Payroll Management System (PMS) as ever having been employed by DJJ; four IDs are assigned to employees on leave; and two IDs are assigned to individuals whose DJJ employment is listed on PMS as terminated.

We also noted that three DJJ employees have two user IDs and that 21 IDs are not assigned to any employees. Section 3.11.1 of NIST, “Generally Accepted Principles and Practices for Securing Information Technology Systems,” states, “An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system.”

RECOMMENDATIONS

To address the unresolved issue from the prior audit, DJJ should:

1. Include in its policies and procedures a list of individuals responsible for network program changes, disaster recovery, and security issues.

DJJ Response: “DJJ does include in its MIS Disaster Recovery Plan the names, titles and telephone numbers of the individuals responsible for our network environment. We will also incorporate in a policy and procedure that is planned for release in March 2004, a list of the office titles responsible for network program changes, disaster recovery and security issues.

“DJJ’s response to concerns (page 5 – paragraph 2) that our procedures do not address the mainframe environment is that DoITT is responsible for servicing the mainframe. We respond to mainframe problems by calling the DoITT help desk and this method is prescribed in our MIS Disaster Recovery Plan. DJJ has, however, sent the attached letter to DoITT requesting a list of individuals responsible for their mainframe environment so it can be included in our MIS Disaster Recovery Plan.”

To address the new issue identified during this audit, DJJ should:

2. Develop written policies and procedures for removing multiple user IDs, inactive IDs, and IDs of individuals no longer working for the agency.
3. Require that its personnel department notify MIS of those employees leaving the agency so that their user IDs can be removed from the system.

DJJ Response: “DJJ does currently require its personnel department to notify MIS of those employees leaving the agency resulting in the removal of their user IDs from the system. Additionally, DJJ is currently drafting a policy and procedure that is planned for release in March 2004 addressing the issues raised in recommendations 2 and 3.”



The City of New York
Department of Juvenile Justice
365 Broadway, New York, NY 10013

Neil Hernandez
Commissioner

Tel. 212.925.7779 Ext. 254
Fax 212.431.4874
TTY/TDD 212.334.6873
www.nyc.gov/nycdjj

February 12, 2004

Mr. Greg Brooks
Deputy Comptroller
Policy, Audits, Accountancy & Contracts
Office of the Comptroller
1 Centre Street
New York, NY 10007

Re: Follow-up Audit Report on
Department of Juvenile Justice (DJJ)
Data Centers
7F04-105

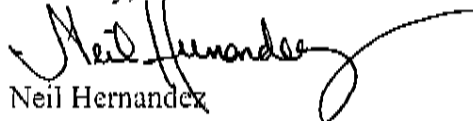
Dear Deputy Comptroller Brooks:

Attached is DJJ's response to the above draft report dated January 27, 2004.

We are pleased that overall our data centers' procedures are adequate to protect DJJ's computer assets and information and that we are significantly in compliance with Comptroller's Internal Control and Accountability Directive #18. As indicated in our Implementation Plan, DJJ substantially agrees with your recommendations. We appreciate your efforts in conducting this audit and your continuing effort to bring about improvements in the Department's data centers.

If you have any further questions, please feel free to contact me at 212-925-7779 ext. 254 or Andrew Gonzalez, Deputy Commissioner of Administration and Policy, ext. 294.

Sincerely,


Neil Hernandez



Department of Juvenile Justice

365 Broadway • New York, NY 10013

Tel. 212.925.7779 • Fax 212.925.8170 • TDD/TTY 212.334.6873

www.nyc.gov/nycdjj

Neil Hernandez
Commissioner

Andrew Gonzalez
Deputy Commissioner
Administration & Policy

February 11, 2004

Peter Tighe
Deputy Commissioner
Department of Information
Technology and Telecommunications
11 Metro Tech Center, 3rd Floor
Brooklyn, NY 11201

Dear Deputy Commissioner Tighe:

The City of New York Office of the Comptroller issued a Follow-up Audit Report on the Department of Juvenile Justice (DJJ) Data Centers dated January 27, 2004. One of the audit recommendations, with regard to the mainframe system, is that DJJ should list in its policies and procedures "those DoITT officials responsible for program changes, disaster recovery, and security issues." To comply with the recommendation, please supply DJJ with this information

If you have any questions, I can be reached at 212-925-7779 ext. 294.

Sincerely,

Andrew Gonzalez

NEW YORK CITY DEPARTMENT OF JUVENILE JUSTICE
COMMENTS ON DRAFT FOLLOW-UP AUDIT REPORT 7F04-105
DATA CENTERS

FEBRUARY 12, 2004

AUDITOR'S RECOMMENDATION 1: *Include in its policies and procedures a list of individuals responsible for network program changes, disaster recovery, and security issues.*

DJJ RESPONSE: DJJ does include in its MIS Disaster Recovery Plan the names, titles and telephone numbers of the individuals responsible for our network environment. We will also incorporate in a policy and procedure that is planned for release in March 2004, a list of the office titles responsible for network program changes, disaster recovery and security issues.

DJJ's response to concerns (page 5 - paragraph 2) that our procedures do not address the mainframe environment is that DoITT is responsible for servicing the mainframe. We respond to mainframe problems by calling the DoITT help desk and this method is prescribed in our MIS Disaster Recovery Plan. DJJ has, however, sent the attached letter to DoITT requesting a list of individuals responsible for their mainframe environment so it can be included in our MIS Disaster Recovery Plan.

AUDITOR'S RECOMMENDATION 2: *Develop written policies and procedures for removing multiple user IDs, inactive IDs, and IDs of individuals no longer working for the agency.*

AUDITOR'S RECOMMENDATION 3: *Require that its personnel department notify MIS of those employees leaving the agency so that their user IDs can be removed from the system.*

DJJ RESPONSE TO RECOMMENDATIONS 2 & 3: DJJ does currently require its personnel department to notify MIS of those employees leaving the agency resulting in the removal of their user IDs from the system. Additionally, DJJ is currently drafting a policy and procedure that is planned for release in March 2004 addressing the issues raised in recommendations 2 and 3.