Alan G. Hevesi
COMPTROLLER

OFFICE OF THE
NEW YORK STATE COMPTROLLER

DIVISION OF STATE SERVICES

METROPOLITAN TRANSPORTATION AUTHORITY

CONTROLS OVER SECURITY-SENSITIVE INFORMATION FOR THE CAPITAL PROJECTS PROGRAM

Report 2006-S-6

AUDIT OBJECTIVE

Our objective was to determine whether the Metropolitan Transportation Authority (MTA) has adequate controls over the dissemination of security-sensitive information for the capital projects program.

The MTA Capital Construction (MTACC), one of seven MTA affiliates, serves as the construction management arm of the MTA for capital projects. In addition, the MTACC is primarily responsible for managing the MTA Security Program to implement major capital construction projects relating to security enhancement of the MTA transportation network in the aftermath of the September 11, 2001 terrorist attack. The primary focus of our audit was the MTA Security Sensitive Information Handbook (Handbook), published in May 2004. The Handbook provides direction to MTA affiliates and vendors on how to safeguard MTA security-sensitive information (e.g., blueprints, design documents, risk assessments, etc.), and also describes the requirements, evaluation criteria, restrictions, and other procedures necessary to prevent unauthorized disclosure of this information.

AUDIT RESULTS - SUMMARY

Overall, we found the MTA established a reasonable control framework to protect security-sensitive information through the creation of the Handbook. However, compliance with the controls outlined in the Handbook is weak. As a result, there is increased risk that access to security-sensitive information related to the capital construction program could be compromised.

We found that individuals were not always complying with established security protocols before accessing and transferring MTA security-sensitive information to other individuals. For example, the MTACC does not have a complete list of individuals who have or have had access to MTA security-sensitive information. If current practices are not improved, such information could be compromised. (See pp. 4-6)

To ensure that only appropriate personnel are able to access MTA security-sensitive information, periodic background screenings should be performed. However, we found that the MTA does not routinely update background screenings on its employees (some background screenings are as much as 20 years old), and it does not ensure that background screenings are performed on all vendor employees who have access to security-sensitive information. (See pp. 7-8)

For a document control system to be effective, the system must clearly identify the location and the individual in possession of security-sensitive information at any point in time. However, at the time of our request, affiliate and vendor security officers were not able to readily locate 55 percent of the security-sensitive documents we tested, based on the information recorded in the document control system. (See pp. 8-11)

Vendors who are utilizing electronic security-sensitive information should have adequate controls in place to prevent unauthorized access. However, we found that MTA officials do not effectively ensure that vendors who keep MTA security-sensitive information on their own computer systems adequately protect that information. Further, we found that vendors are not submitting the Information Technology (IT) Management Plan to MTA for review as required in the Handbook. As a result, MTA officials do not have assurance that vendors have developed and implemented adequate measures to

protect MTA security-sensitive information maintained on their respective IT systems from unauthorized access. (See pp. 11-13)

To prevent unauthorized access to construction sites for security-related capital projects, security personnel should review and approve all construction site security plans specified in the construction contract. We found that appropriate security personnel do not review and approve all construction site security plans in MTA construction contracts. As a result, construction site security plans may not contain adequate security provisions. (See pp. 13-14)

Our report contains 18 recommendations to improve controls over access to MTA security-sensitive information. MTACC officials generally agree with our findings and have taken immediate actions to make changes and correct some issues. For example, another staff member has been added to assist the MTA Security Officer, and the MTACC will be engaging the staff of the MTA Audit Services Division to develop and operate an ongoing program to review vendor and MTA agency document security programs.

In addition, MTACC officials are anticipating further revision of the Handbook in the near future to reflect their experiences with managing the substantial volume of documents and the parties who create, transmit and manage the use of the documents. Further, the MTACC has since developed a draft Security-Sensitive Information Document Control Policy and Procedure that addresses some of the concerns raised in this audit.

This report, dated September 6, 2006, is available on our website at: http://www.osc.state.ny.us. Add or update your mailing list address by contacting us at:
(518) 474-3271 or
Office of the State Comptroller
Division of State Services
State Audit Bureau
110 State Street, 11th Floor
Albany, NY 12236

BACKGROUND

The Metropolitan Transportation Authority (MTA) is a public-benefit corporation chartered by New York State in 1965. The MTA consists of seven affiliates, including the MTA Capital Construction (MTACC), which was formed in July 2003. The MTACC serves as the construction management arm of the MTA on projects that may cost as much as $20 billion over the next two decades. The MTACC focuses on projects that will expand MTA's regional transportation network, including: the East Side Access, the Second Avenue Subway, the extension of subway service to the far West Side of Manhattan, the Fulton Street Transit Center, and the South Ferry Terminal.

The MTA Security Program was initiated shortly after the September 11, 2001 terrorist attack on the World Trade Center. The MTACC developed and implemented this program to assess the vulnerabilities of the MTA's transportation infrastructure in order to mitigate risks and exposure to future attacks of a similar nature. The MTACC's objective was to implement as quickly and responsibly as possible the capital construction projects relating to security enhancement of the MTA transportation

network. The Security Program was originally budgeted at $591 million and, as of December 27, 2005, was expected to cost $721 million.

In developing the Security Program, the MTACC considered the known and potential vulnerabilities to the transportation network infrastructure. The MTACC engaged a consulting firm to develop a regimen for managing information and documents that might be deemed security-sensitive and that would need to be created, transmitted, and managed across a large number of projects, vendors, MTA affiliated agencies and the staff of all of those entities. This resulted in the publication of the MTA Security Sensitive Information Handbook (Handbook) in May of 2004, the appointment of MTA affiliate and vendor "security officers" to ensure compliance with the Handbook, and the establishment of the Authorized Personnel Listing (Authorized List), which contains the names of individuals who are authorized to access security-sensitive documents.

The Handbook provides direction on how to safeguard MTA security-sensitive information that, if subject to unauthorized access, modification, loss or misuse, could adversely affect the security of MTA employees and facilities, and the public. The Handbook also describes the requirements, evaluation criteria, restrictions, and other safeguards necessary to prevent unauthorized disclosure of MTA security-sensitive information. The objective of the Handbook is to enhance the management and protection of MTA security-sensitive information. The Handbook has been updated twice and the MTACC expects a further revision in the near future. All affiliates and vendors are required to adhere to the goals of the Handbook. MTACC officials added that affiliates have the flexibility to achieve the goals articulated in the Handbook in accordance with their own policies and practices. Given the importance of maintaining security over the nation's largest mass transit system, MTA officials should make sure that affiliates uniformly interpret the Handbook.

AUDIT FINDINGS AND RECOMMENDATIONS

Access to MTA Security-Sensitive Information

According to the Handbook, access to MTA capital program security-sensitive information is authorized only on a "need-to-know basis." MTA and vendor employees are required to sign a Non-Disclosure Agreement (Agreement), which calls for the non-disclosure of security-sensitive information to unauthorized persons. The individuals and vendor organizations that have signed the Agreement must also abide by the control procedures outlined in the Handbook and take responsibility for protecting information from unauthorized disclosure. MTACC officials stated that once an individual signs the Agreement, his or her name is added to the master Authorized List. Only those employees (MTA or vendor) who have signed the Agreement and who are on the Authorized List are allowed access to security-sensitive information. The MTA Security Officer maintains the master Authorized List, which as of March 1, 2006 contained 1,842 names, based on information supplied by affiliate and vendor security officers.

To determine whether unauthorized persons have accessed security-sensitive information, we compared the 1,842 names on the master Authorized List to the 71 names of individuals from various MTA affiliates and vendors who received security-sensitive information during the period June 24, 2004 through March 15, 2006. We obtained the 71 names from the MTACC's web-based project management software package, known as

ProjectSolve. The ProjectSolve document management tool is a module of a project management software program developed by a vendor. This software is intended to track the location of security-sensitive information, including key information such as the number of copies, identity of the sender, transmission history, ultimate disposition and a brief description for each item listed. We identified nine persons (13 percent), including two high level MTA officials who, although not listed on the Authorized List, received almost 150 security-sensitive documents. It is important for high level officials to sign the Agreement in order to set an example for the rest of the organization.

In addition, when we were reviewing the security-sensitive information inventory at one MTA affiliate, the MTA Metro-North Railroad (Metro-North Railroad), officials informed us that, despite the requirements in the Handbook, their employees are not required to sign the Agreement before accessing MTA security-sensitive information. Metro-North Railroad officials told us that they have their own internal procedures requiring training and confidentiality. The MTACC's General Counsel confirmed the Metro-North Railroad statement, and added that the New York State Public Officers Law, which prohibits the disclosure of confidential information acquired during the course of an employee's official duties, covers Metro-North Railroad employees.

However, not requiring Metro-North employees to sign the Agreement is contrary to the rules established in the Handbook for all MTA and vendor employees. Moreover, the prohibition in the Public Officers Law against disclosure of confidential information is not a substitute for the Agreement. In fact, under these circumstances, it is important that agreements be entered into in order to effectuate that statutory prohibition. Section 74(4) of the Public Officers Law (Law) provides that "…any…officer, member or employee who shall knowingly and intentionally violate any of the provisions of this section may be fined, suspended or removed from office or employment in the manner provided by law."

By requiring employees to sign the Agreement, the employee is specifically on notice of the information that is to be kept confidential. Therefore, any disclosure of such information would likely fall within the "knowing and intentional" requirement of Section 74(4), and subject the employee to the fines, suspension and removal from office as provided under the Law.

If no such Agreement is signed, it will be more difficult to demonstrate that the employee was on notice and acknowledged that such information was confidential. As a result, eliminating this requirement weakened the MTA's security controls. It should be noted that, as of June 22, 2006, Metro-North Railroad officials have agreed to have their employees sign the Agreement.

Metro-North Railroad officials developed their own authorized list, which represents individuals who attended their security-sensitive information training program. These individuals are allowed to access security-sensitive information for Metro-North Railroad security projects that are part of the MTA Security Program. To determine the number of Metro-North Railroad employees who may access MTA Security Program security-sensitive information without having signed the Agreement, we compared Metro-North Railroad's authorized list to the master Authorized List and found that only 2 of the 103 names listed on Metro-North Railroad's list were also on the MTA master Authorized List. Therefore, 101

individuals could have access to Metro-North Railroad security-sensitive information (maintained by the MTACC) without the knowledge of the MTA Security Officer.

Furthermore, we identified three Metro-North Railroad employees who had not signed the Agreement and have actually accessed Metro-North Railroad security-sensitive information for projects within the MTA Security Program. We identified these individuals through a review of Metro-North Railroad internal memorandums. Of the three employees, one employee was not even listed on Metro-North Railroad's own authorized list.

The Handbook requires that a central filing system be developed to identify all individuals who currently have or have had access to MTA security-sensitive information. This information may be used for investigative purposes later, if necessary. MTACC officials stated that their master Authorized List is their central filing system. However, in addition to the names on the master Authorized List, the central filing system is to include information such as the date the Agreement was signed; title, function and contact information for the authorized individuals; and other relevant information, such as the date the authorized privilege has been revoked, if any. Based on the results of our testing, we conclude that the MTA central filing system is inaccurate and incomplete. As a result, the MTA and other authorities (e.g., police) would not have an adequate record of all who have examined security-sensitive information and may not be able to adequately perform an investigation, if necessary. We noted the following weaknesses:

- The names of the individuals (who signed Agreements during the procurement process and had access to security-sensitive information) who were not awarded security-related contracts, are not provided to the MTA Security Officer. As a result, the names of these individuals are not recorded in the central filing system.

- The Authorized List is not easy to update or practical for individuals to use. Further, MTACC officials told us the amount of information will grow substantially as additional construction projects begin. They also agree that the current format may not be practical and are considering a more efficient system.

- The central filing system does not include all the required information per the Handbook, such as the individual's title and function, and the date the Agreement was signed.

Recommendations

1. Establish controls that ensure only individuals whose names appear on the master Authorized List have access to security-sensitive information.

2. Ensure that all MTA and vendor employees with access to security-sensitive information sign the Agreement.

3. Revise the central filing system to include all required information.

4. Make the Authorized List more efficient to use as a management tool.

Background Screening

MTA Employee Background Screening

The Handbook requires that the MTA Security Officer verify the employment history and resume of each MTA employee who has access to MTA security-sensitive information. The Security Officer relies on the MTA or affiliate human resources departments to perform these checks, which are generally done when an employee is hired.

The MTA Human Resources Department conducts background screenings for newly-hired MTACC employees. Employees that have transferred to the MTACC from an affiliate have their background checks done by the affiliate's human resources department. The current background screening process is comprehensive. It verifies an employee's: social security number, education, past employment, driver and professional licenses, criminal record, pending civil actions, tax investigations or proceedings, traffic violations and/or convictions within the past three or five years, terrorist activities tracked by the United States Department of the Treasury, residences during the past ten years and credit and other financial information. Also, the employee's eligibility to work in the United States is verified with the United States Department of Homeland Security.

As of May 4, 2006, the MTACC had a total of 162 employees, 22 of whom were assigned to work on security-sensitive projects. To determine whether the 22 employees had their background verified by either the MTA Human Resources Department or an affiliate's human resource department, we asked MTACC officials to obtain the background screening data for these employees. We determined that all 22 MTACC employees had a background check performed when they were initially hired.

However, we determined that 20 of the 22 background checks were done more than 10 years ago, including 5 background checks done over 20 years ago. None of these 20 employees have had an updated background screening. Security concerns in the last five years are quite different from the concerns that existed when most of these employees were hired and, as a result, current background screenings are more extensive. Given the significance of the security-sensitive information and project sites which these employees may access, it would be prudent to have updated background checks for these employees.

Vendor and Vendor Employee Background Screening

The Handbook also requires that an employment and resume verification be done for the principals of each vendor company (consultants, contractors, and sub-contractors) as well as any of the vendor's employees who may access MTA security-sensitive information. A principal is someone who is in a position to make business decisions on behalf of the company (e.g., owners and directors of the company). Principals must complete an "Employee Employment and Resume Verification" form on which they list past employers, job-related licenses as well as other pertinent background information. The MTA Security Officer is responsible for verifying this information. Any employee found to be unsuitable, or whose employment is deemed contrary to the public interest, may be prevented from performing work under a contract containing MTA security-sensitive information.

The MTA Security Officer stated that he relies on the New York City Transit Vendor

Relations Unit (Vendor Relations) to perform vendor background screenings as part of the comprehensive pre-award bidder/contractor responsibility determination that is a component of the contract award process. Vendor Relations performs background screenings on principals, but does not perform any screenings on other vendor employees even though these individuals may access security-sensitive information and related project sites on a regular basis. The MTA Security Officer stated that he does not perform nor is he aware of any other vendor employee background checks. As of March 1, 2006, the Authorized List identified 1,357 vendor employees as being authorized to access MTA security-sensitive information. Of these employees, a significant number are not "principals." Therefore, the MTA has no assurance that vendor employees, including sub-contractor employees, who may access MTA security-sensitive information, are suitable.

MTACC officials informed us that it is the responsibility of the vendors to verify the integrity of their employees who work on the MTA Security Program. MTACC officials believe that any vendor who has received the Handbook and has signed an Agreement is under a contractual obligation to verify the employment and resume history of its employees. However, contracts do not include any provisions that explicitly require such screenings. In addition, there is no requirement that vendors perform criminal background checks and the various other checks that MTA employees undergo when hired. Furthermore, the MTA Security Officer does not verify the information that vendor employees disclosed on the Agreement, as required.

Recommendations

5. Revise the background check policy to include updated checks for employees with access to security-sensitive information.

6. Ensure that appropriate background screenings, such as those performed on MTA employees, are performed on all vendor and sub-contractor employees who have access to MTA security-sensitive information.

7. Ensure that contracts stipulate that vendors are responsible for performing appropriate background checks on employees who may access security-sensitive information and project sites.

Reliability of the Document Control System

The Handbook requires that a document control system be established to provide control and accountability over MTA security-sensitive information. The document control system should facilitate the retrieval of the security-sensitive information, provide a trail of where the material has been transferred, and clearly identify who has the materials at any point in time. The MTA and vendor security officers and project managers are responsible for developing a document control system for projects containing security-sensitive information. MTACC officials stated that their document control system is new, unique, and evolving and that it is in its early stages.

Since June 24, 2004, MTA and vendors have used ProjectSolve as part of their document control system. ProjectSolve is intended to keep track of all MTA security-sensitive documents that are transferred from one entity to another (e.g., MTACC to Metro-North

Railroad). In addition, according to the Handbook, the affiliates and vendors should maintain handwritten log books that create a paper trail of the security-sensitive information they distribute internally. Periodically, these log books should be collected by the MTA Security Officer for compliance reviews. We identified problems relating to the accuracy of the document control system, as well as the maintenance and use of ProjectSolve.

Accuracy and Completeness of the Document Control System

For a document control system over security-sensitive information to be reliable, documents should be located exactly where the document control system says they should be. To determine the accuracy of MTA's document control system for security-sensitive information, we selected a judgmental sample of 23 ProjectSolve entries from an MTA primary vendor and an MTA affiliate (Metro-North Railroad) to determine whether the documents were in possession of the individual listed in the ProjectSolve database. The sample was selected from a total population of 2,413 separate entries of document movements. For the MTA vendor, we selected 20 ProjectSolve entries (from a total population of 118 entries) consisting of single documents, each with a unique document control number. For Metro-North Railroad, we selected 3 ProjectSolve entries (from a total population of 52 entries) consisting of 11 documents, each containing a unique document control number. Therefore, the total number of documents we sampled was 31. Of the 31 total documents, 17 (55 percent) of them were not in the possession of the stated persons as listed in ProjectSolve at the time of our initial visits. During our follow-up reviews, we were able to locate all but five of these security-sensitive documents. We observed that all the documents that were located contained the appropriate markings, identifying them as security-sensitive, as specified by the Handbook.

On March 31, 2006, we made our initial visit to Metro-North Railroad. The ProjectSolve database indicated that the 11 sample pieces of security-sensitive information were in the Metro-North Railroad Security Officer's possession. We found that four documents were in the Security Officer's safe and that he did not have the seven other documents. The Metro-North Railroad Security Officer explained that five items had been returned to the project designer, and two were with the former project manager. The movement of these security-sensitive information items was not recorded in the ProjectSolve database or internal logs.

On April 18, 2006, we returned to Metro-North Railroad and found that none of the seven documents had been transferred to the project designer or project manager. Six were in the possession of four Metro-North Railroad employees, three of whom were not on the Authorized List. Metro-North Railroad officials stated that the documents were in a locked office at all times. The Security Officer stated that the seventh document had been shredded; however, this disposition was not documented. Again, these movements of security-sensitive information were not recorded in the ProjectSolve database or internal logs.

The Metro-North Railroad Security Officer provided internal memorandums during our follow-up visit indicating the transfer of some security-sensitive documents. However, this method is not consistent with Handbook requirements, is not a component of the document control system, and does not serve to readily identify the location of documents containing security-sensitive information. On April 7, 2006, we made an initial visit to a

primary vendor location where the sample of 20 security-sensitive documents was located according to ProjectSolve. Ten items were found and the other ten items were missing. We returned to the vendor on April 24, 2006 and had subsequent contacts to determine the disposition of the ten missing items and found that:

- One of the missing security-sensitive information documents was actually in the MTACC's possession.

- Three of the documents were in the possession of other vendors.

- Two other missing documents were found at the ProjectSolve location, but reportedly had been misfiled or mislabeled during our initial visit.

- Four items could not be physically located by us. Three items reportedly had been superceded or existed under another document control number. Another security-sensitive document is still unaccounted for and remains missing as of July 21, 2006.

During our review of the ProjectSolve database, we also found several instances where required information (e.g., names of recipients, dates of transmittal) was not complete. Overall, we found a significant lack of consistency in the data entered in ProjectSolve. For example, we found 563 instances (23 percent) where the "transmitted to" field was left blank and another 78 instances (3 percent) where the company was named but the specific individual was not identified, as required. In addition, we found 675 instances (28 percent) where important data, such as the number of copies transferred, was not logged.

Based on our review, we conclude that the MTACC lacks the necessary assurances that security-sensitive documents can be readily located. There are several reasons for this. For example, ProjectSolve, as currently configured, does not provide for data entry edit controls to ensure that all required information is entered into the system. Further, the MTA has not developed guidelines to inform users on how to enter data into the system. For example, a project manager at one of the MTA's primary vendors never enters project descriptions, even though the Handbook requires such information. In addition, there is an overall lack of monitoring of affiliate and vendor Handbook compliance, because the MTACC has devoted limited resources to this area. For example, the MTA Security Officer does not periodically review the log books as required. If the Security Officer had performed these reviews, he could have determined that affiliates and vendors do not maintain accurate, up-to-date inventory records of security-sensitive information.

MTACC officials acknowledge the discrepancies in ProjectSolve and have already taken steps to correct them. For example, they told us that they have reduced the number of instances where the "transmitted to" field is blank - from 563 to 28 - and they are continuing their work to resolve the remaining instances. MTACC officials also informed us that they are evaluating whether to replace the ProjectSolve document control system. The MTACC has since developed a draft Security-Sensitive Information Document Control Policy and Procedure that addresses some of the concerns raised in this audit.

MTACC officials also explained they did not want to expend a lot of resources on Handbook compliance. Rather, they needed to balance their limited resources on

implementing security vulnerability mitigation measures and on recordkeeping processes.

Further, they indicated they would like to do more compliance reviews, but do not have the staffing resources. MTACC officials told us that they plan to engage MTA Audit Services Division in the development and operation of an ongoing program to review vendor and MTA agency document security programs.

Access to ProjectSolve

MTACC officials stated that each user must sign an Agreement before obtaining access to ProjectSolve. In addition, a formal enrollment process should be in place for employees to request authorization to access the system and for such authorization to be removed when access is no longer needed. We found that controls over access to the ProjectSolve system need improvement.

To determine whether ProjectSolve users had signed Agreements, we selected a judgmental sample of 55 users from an alphabetical list containing a total population of 551 users as of April 3, 2006. We tested the first 55 persons in alphabetical order. We determined that 9 users (16 percent), who had received security-sensitive information, had not signed the Agreement. In addition, we found MTACC officials have not established a formal process for the addition and removal of employees who may access the system. Instead, database administrators may simply receive an email or memorandum notifying them to add or remove users. As a result, there is an increased risk that unauthorized individuals can access the system.

In addition, the Handbook requires that all sensitive information be destroyed upon reaching its disposal date. In reviewing the ProjectSolve database, we found that disposal dates are not always established and entered. Without set disposal dates, security-sensitive information that should have been destroyed may be unnecessarily exposed to loss or theft.

Recommendations

8. Formally investigate all instances of, and explanations for, the missing documents we identified.

9. Require the movement of security-sensitive documents be recorded in compliance with the Handbook. Provide guidance as needed to ensure requirements are met.

10. Require the MTA Security Officer to periodically monitor whether the ProjectSolve database and log books are being maintained effectively.

11. Develop a formal enrollment process for adding and removing ProjectSolve users.

12. Develop a process that ensures all required fields are entered into ProjectSolve.

13. Develop guidelines to inform users on how to enter data into ProjectSolve.

14. Establish disposal dates for security-sensitive information.

Controls over Information Technology

The Information Technology (IT) systems that vendors utilize to electronically create, process, store and/or transmit MTA security-sensitive information must be protected against unauthorized access, interception, and disclosure. The Handbook requires vendors to develop an IT Plan and submit it to the MTA for approval. At a minimum, an IT Plan must include measures the vendor has developed and implemented to address physical, operational and personnel security

safeguards. In addition, the MTA Security Officer is required to review vendor security practices to ensure compliance with the Handbook. We found that vendors were not submitting the required IT Plans and that the MTA Security Officer was not adequately reviewing vendor compliance with the Handbook.

Vendor IT Management Plan

The Handbook states that only individuals and vendors named on the Authorized List may access, modify, and transmit MTA security-sensitive information. The Handbook's subsequent paragraph states that "the vendors" shall prepare IT Plans.

As of March 1, 2006, 125 vendors had authorized access to security-sensitive information relating to MTA security projects. We found that none of the 125 vendors working on MTA security projects submitted an IT Plan to the MTA for approval.

MTACC officials stated that their interpretation of the Handbook only required the ten primary vendors with whom the MTA directly contracts to submit IT Plans. The MTA, however, did not obtain IT plans from any of its ten primary vendors.

MTACC officials stated that MTA does not require anything from the sub-contractors because a primary vendor could have agreements with its sub-contractors requiring them to follow the primary vendor's IT Plan. The MTA, however, could not provide any evidence of such arrangements, and MTACC officials stated they had no direct knowledge that such arrangements exist.

MTACC officials stated that four vendors submitted a document called the Document Security Plan (Document Plan) that contained relevant information regarding IT system safeguards. Our review of the four Document Plans determined that none of them addressed security measures for the protection of security-sensitive information utilized on their respective IT systems. In addition, none of the Document Plans described the proposed hardware and software as required.

Without proper support that IT controls are in place, the MTACC lacks adequate assurance that electronic security-sensitive information is protected against unauthorized access, interception, and disclosure.

IT Reviews

The MTA Security Officer should ensure that vendors' IT systems conform to Handbook requirements to protect MTA security-sensitive information against unauthorized acccess, interception, and disclosure. The vendor Non-Disclosure Agreements allow the MTA to periodically audit the vendors' security practices to ensure that they comply with the procedures outlined in the Handbook.

The MTA Security Officer performed Handbook compliance reviews on three vendors, including conformity with IT system requirements. We evaluated the three reports and determined that these IT compliance reviews were not adequate. For example, one report included a statement indicating that security-sensitive information was stored on a shared server and protected by a firewall. When we inquired about the basis for that conclusion, the MTA Security Officer told us that the vendor's security officer told him the server was firewall-protected. The MTA Security Officer did not actually test the vendor's IT system. In addition, MTACC officials told us they do not have sufficient resources to test vendor IT controls.

Without adequate testing, the MTA lacks assurance that electronic security-sensitive information is protected from unauthorized access, interception, and disclosure. Of the 125 vendors, MTACC officials are aware that 22 vendors have utilized or will shortly utilize their respective IT systems to maintain MTA security-sensitive information. To learn whether vendors have minimum IT controls in place, we sent a questionnaire to the 22 vendors asking them about their physical, operational, and personnel IT safeguards. Fifteen vendors responded and indicated significant compliance with IT controls. However, one area where the vendors acknowledged significant non-compliance was the encryption software requirement. The Handbook requires that encryption software be used to protect security-sensitive information during transfers between MTA and vendors. Nine vendors indicated that they do not use encryption software.

MTACC officials stated that vendors do not need to use encryption. Vendors may use password protection instead. Furthermore, they also believe that the low number of instances where security-sensitive information would be electronically transmitted does not justify the cost of this software. However, the Handbook requires the use of encryption, and vendors are required to adhere to the Handbook. If MTACC officials want to take a less rigorous approach, they should make a formal assessment of the risks, and revise the Handbook accordingly.

Recommendations

15. Require all vendors, including primary contractors and their subcontractors, to submit the required IT Plans to the MTA Security Officer for review and approval as presently outlined in the MTA's Handbook.

16. Implement a comprehensive testing process to ensure that vendors comply with the procedures outlined in the MTA's Handbook.

17. Require and ensure that encryption software is used to protect MTA security-sensitive information in electronic form, unless the Handbook is changed based on a formal assessment of the risks involved.

Construction Site Security Plan Review

The MTACC has the overall responsibility for defining and implementing the MTA Security Program for all MTA affiliate agencies. The MTA Capital Security Program Management Plan (Program Plan) states that each affiliate agency has a set of defined construction site security requirements. These requirements include the controls used to prevent unauthorized access to the construction site such as the use of identification cards and sign-in logs.

During a project's design phase, construction site security requirements are incorporated in the contract for implementation during the construction phase. The Construction Manager and the MTACC Design Manager are required to review the affiliate's construction site security requirements. Along with consultation from the involved affiliate, they decide which site security requirements to include, exclude, or modify for the contract based on the project site and the work activities incorporated into the contract. Their decisions are made based on their experience and input from affiliate and vendor personnel, who may or may not have the necessary security expertise. Therefore, it is essential that appropriate security personnel review and approve the final construction site security specifications.

To determine whether affiliates had security personnel review their construction site security plans, we contacted officials from MTA New York City Transit (NYCT), MTA Bridges and Tunnels (B&T), and Metro-North Railroad. We also made contact with MTA Long Island Rail Road (LIRR) officials through the MTACC. Security Program projects are under construction for each of these agencies. We found the following:

- NYCT officials stated that security personnel do not review or approve contract provisions dealing with construction site security requirements.

- LIRR officials informed the MTACC that they have designated two individuals as the contacts for all security related matters. When it is necessary, and if applicable, these individuals seek the services of MTA's Office of Security and/or outside third party consultants in the review of security considerations within LIRR contracts. However, it was unclear from their response to the MTACC as to whether security reviews were performed and documented.

- B&T officials stated their site security plans are reviewed and approved at numerous levels, including a review by their Internal Security Department which is made up of trained security personnel. However, officials told us that the review and approval were not documented.

Recommendation

18. Require the MTA Office of Security and other appropriate security agencies to review and approve the security provisions of MTA Security Program capital construction contracts. Ensure those reviews and approvals are documented.

AUDIT SCOPE AND METHODOLOGY

We conducted our audit in accordance with generally accepted government auditing standards. We audited the MTA's controls over capital projects program security-sensitive information for the period May 28, 2004 through June 12, 2006. To accomplish our objective, we reviewed applicable MTA policies and procedures. We also interviewed MTACC, affiliate, and vendor officials and reviewed various MTACC data and supporting documentation related to security-sensitive information. Our review included the MTA Handbook, which sets out criteria for the creation, maintenance, dissemination and destruction of security-sensitive information and documents.

To determine whether the MTA has adequate controls in place to prevent unauthorized access to security-sensitive information by MTA employees and third-party consultants or contractors, we compared the 1,842 names on the master Authorized List to the 71 names of individuals from various MTA affiliates and vendors who, according to the ProjectSolve database, received security-sensitive information during the period June 24, 2004 through March 15, 2006.

To determine whether background checks were being performed and up-to-date, we selected a sample of 22 MTACC employees to review. We also met with MTACC officials to verify whether vendor background checks were performed. To assess the accuracy and completeness of the document control system, we selected a judgmental sample of 31 security-sensitive documents and determined whether these documents were at the locations recorded in the ProjectSolve inventory control system. To assess IT controls, we sent out a questionnaire to vendors to determine compliance with the Handbook. To assess construction site

security, we met with MTACC, affiliate, and vendor officials, reviewed affiliate policies and procedures, and reviewed Security Program construction contracts.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State, several of which are performed by the Division of State Services. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these management functions do not affect our ability to conduct independent audits of program performance.

AUTHORITY

The audit was performed pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution.

REPORTING REQUIREMENTS

Draft copies of this report were provided to MTA officials for their review and comment. Their comments were considered in preparing this report and are included as Appendix A. MTA officials generally agree with the recommendations. Appendix B is the State Comptroller's Comments to the MTA's response.

Within 90 days of the final release of this report, as required by Section 170 of the Executive Law, the Chairman of the Metropolitan Transportation Authority shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons therefor.

CONTRIBUTORS TO THE REPORT

Major contributors to this report include Jerry Barber, Brian Reilly, Gene Brenenson, Stephen Lynch, Diane Gustard, Orin Ninvalle, and Paul Bachman.

APPENDIX A - AUDITEE RESPONSE

Audit Services
2 Broadway, 16th Fl
New York, NY 10004-2207
646-252-1200 Tel
646-252-1318 Fax

Metropolitan Transportation Authority
State of New York

RECEIVED
Office of the State Comptroller
AUG 24 2006
Jerry Barber
Assistant Comptroller
State Audit Bureau

August 21, 2006

Mr. Jerry Barber
Assistant Comptroller
Office of the State Comptroller
Division of State Services
State Audit Bureau
110 State Street – 11th Floor
Albany, NY 12236

Re: Report #2006-S-06 MTA's Controls Over Security-Sensitive Information For The Capital Projects Program

Dear Mr. Barber:

This is in reply to your letter to Chairman Kalikow requesting a response to the above-referenced draft audit report.

I have attached for your information the comments of Mr. Mysore Nagaraja, President, MTA Capital Construction, which address this report.

Sincerely,

Paul Spinelli
Auditor General

Attachment
C: P. Kalikow, Chairman
K. Lapp, Executive Director
M. Nagaraja, President, Capital Construction

Memorandum

Capital Construction

Date August 17, 2006

To Peter S. Kalikow, Chairman, MTA

From Mysore L. Nagaraja, President MNagaraja/mt

Re **Draft Audit Report By NYS Comptroller #2006-S-6**

MTA Capital Construction, in conjunction with the MTA Office of Security, has reviewed the attached draft Audit Report addressing controls over the MTA Security Program's security sensitive information, and provides the following comments.

General Comment:

MTA acknowledges the comprehensiveness of the Audit, and as noted in the Audit Report, has, in several instances, already implemented certain recommendations to enhance document control of security sensitive information. However, the Report does not adequately reflect the overall context of document control within the MTA Security Program. The MTA Security Program has over $500M in projects underway, involving multiple agencies, locations, projects, consultants and contractors. Thus, while the Audit measures compliance against technical requirements in the MTA Security Sensitive Information Handbook that was published in 2004, MTA Security Program staff have already acknowledged that certain requirements in the Handbook are not practicable for implementation in a program of this complexity, nor are they needed to adequately safeguard information that is truly security sensitive. In all instances, adequate safeguards are in place to address security sensitive information, and to the extent that there is deviation from the original Handbook requirements, revision to the Handbook is underway.

* Comment 1

Points of Clarification:

p.3, Column 2, Paragraph 2: The MTA Security Program was originally initiated shortly after September 11, 2001, and involved multiple MTA agencies. However, the Program was consolidated and management transferred to the MTA Office of Security and MTA Capital Construction in September 2003.

* Comment 2

p.5, Column 1 Paragraph1: In discussing the requirements of MNR regarding maintenance of confidential information, the following revision is suggested to accurately reflect conversations with Audit staff.

* See State Comptroller's Comments, page 20

"In addition, when we were reviewing the security sensitive information inventory at one MTA affiliate, the MTA Metro-North Railroad, officials informed us that their employees are not required to sign the Agreement before accessing MTA security sensitive information. Metro-North Railroad officials told us that they have their own internal procedure requiring training and confidentiality. The MTACC General Counsel confirmed that statement and further added that the New York State Public Officers Law, which prohibits information acquired during the course of an employee's duties, covers Metro-North Railroad employees..."

* Comment 2

p. 5, Column 2, Paragraph 2: Propose deleting the last sentence which states that 101 Metro-North individuals could have access to Metro-North Railroad security sensitive information without the knowledge of the MTA Security Officer. This is a bit misleading, because while true, this mixes two distinct types of security sensitive information, e.g., Metro-North specific versus MTA Security Program information. The MTA Security Officer is not required to monitor who within Metro-North has access to Metro-North specific security sensitive information.

* Comment 2

p.6, Column 1, Paragraph 1: With respect to the three Metro-North individuals who had not signed confidentiality agreements as noted on the bottom of p. 5 into top of p.6, the Metro-North Security Officer had advised the Audit staff that those individuals had received appropriate training in maintaining confidential information.

* Comment 3

p.10, Column 2, Paragraph 3: Regarding the statement about not spending resources on Handbook compliance, this statement is taken out of context wherein MTA CC staff was explaining the need to balance the use of resources within the overall Security Program.

* Comment 2

Recommendations:

As noted, MTA generally agrees with the recommendations noted in the Audit Report, with certain clarifications:

Recommendation #5: *"Revise the background check policy to include updated checks for employees with access to security-sensitive information."* MTA does not think that regularly updating background information on its employees is practicable, nor does it achieve enhanced security, and we would propose clarifying the recommendation to require MTA to periodically review the need to update background information of its employees.

* Comment 4

Recommendation #17: *"Require and ensure that encryption software is used to protect MTA security-sensitive information in electronic form, unless the Handbook is changed based on a formal assessment of the risks involved."* MTA would suggest a clarification to require encryption software to protect security sensitive information to the extent such information is transmitted in electronic form. Currently, MTACC has not electronically transmitted security sensitive information. However, in limited circumstances we have hand-delivered password-protected discs containing security sensitive information. In these situations, we have

* Comment 5

* See State Comptroller's Comments, page 20

employed the same transmission and receipt protocols that are used for paper documents, with the password-protected discs representing an additional level of security. MTACC will evaluate the introduction of encryption technology to the extent that that level of protection is needed for electronic transmission of documents.

Representation Letter:

The Representation Letter (p.14, Column 2, last paragraph) has been provided to the audit team, as requested.

* Comment 5

cc: K. Lapp
W. Morange
P. Spinelli

* See State Comptroller's Comments, page 20

APPENDIX B - STATE COMPTROLLER'S COMMENTS

1. The MTA engaged a consulting firm to develop the Handbook and presented it to us as the guidance document for managing information and documents deemed security-sensitive.

2. The final report was revised to reflect comments provided in the MTA's response to the draft report.

3. Receiving training is not a substitute for an employee's signed Agreement.

4. We continue to believe that MTA's policy should require updated background checks for employees authorized to access security-sensitive information. In the absence of periodic updates, employees without updated background checks should not be allowed to access security-sensitive information.

5. Any decision to limit encryption to only security-sensitive information transmitted in electronic form should be based on a formal assessment of risk consistent with our recommendation.