Metropolitan Transportation Authority

MTA Security Sensitive Information Handbook






March 15, 2006

Version 3.0

COPY NUMBER:

March 15, 2006

The Metropolitan Transportation Authority

MTA Security Sensitive Information Handbook

Table of Contents

Section

1 Executive Summary

2 Roles and Responsibilities

3 Procedures For Handling MTA Security Sensitive Information

- 3.1 General
- 3.2 Access to MTA Security Sensitive Information
- 3.3 Safeguarding MTA Security Sensitive Information
- 3.4 Marking of Documents
- 3.5 Authorized Personnel Listings
- 3.6 Document Control System
- 3.7 Provisions Under FOIL
- 3.8 Provisions Under 49 CFR subpart 1520
- 3.9 Authorized Personnel Listing Sample (Table 1)
- 3.10 Document Control System Sample (Table 2)
- 3.11 MTACC Audit Program

4 MTA Evaluation Guide

- 4.1 General
- 4.2 MTA Limited Distribution Document
- 4.3 MTA Evaluation Guidelines
- 4.4 Examples of MTA Evaluation Guidelines

5 Information Technology Systems

6 Non-Disclosure and Confidentiality Agreement-Individual

- 6.1 Verification and Acknowledgement (Confidentiality Agreement-Individual)
- 6.1.1 MTA Security Program Acknowledgement of Receipt – Security Sensitive Information Handbook

7 Employee Employment and Resume Verification

Table of Contents (Cont'd)

Section

8 Procurement Procedures

8.1 Document Security Notice to Prospective Vendors

8.1.1 Prime Vendor Responsibilities
8.1.2 Information to be furnished by each Vendor
8.1.3 Vendor Responsibility Data Form (Additional Questions)
8.1.4 Verification and Acknowledgment (Information to be furnished by Each Vendor)

8.2 Non-Disclosure and Confidentiality Agreement-Vendor

8.2.1 Verification and Acknowledgment (Confidentiality Agreement-Vendor)
8.2.2 Appendix A
8.2.3 Appendix B

Attachment

MTA Non-Disclosure Agreement Attachment-
Overview of MTA Security Sensitive Information Handbook

March 15, 2006

THE METROPOLITAN TRANSPORTATION AUTHORITY SECURITY SENSITIVE INFORMATION HANDBOOK

SECTION 1 EXECUTIVE SUMMARY

The procedures identified in this manual are to be used during the implementation of MTA Security Projects. This handbook prescribes requirements, restrictions and other safeguards that are necessary to prevent unauthorized disclosure of MTA Security Sensitive Information and to control authorized disclosure of such Information. In all instances, the safeguarding of MTA Security Sensitive Information is subject to law and may be superceded by, the Freedom of Information Law, Article 6 New York State Public Officers Law Sections 84 to 90 (See Section 3.7), requiring the disclosure of certain information. However; MTA may decide not to disclose under section 87 (2) (f) of the FOIL law (see Section 3.7) and under the provisions of 49 CFR subpart 1520 (See Section 3.8) which states that MTA may deny access to material containing MTA Security Sensitive Information that if disclosed could endanger the life or safety of any person and will adversely affect the security of the MTA (See Section 3.7). The procedures outlined herein, employ safeguarding requirements of control and accountability, storage, disclosure, reproduction, transmission, document shipment, disposition, and labeling. The handbook is used to safeguard MTA Security Sensitive Information and to control its authorized disclosure both internally within the MTA organizations as well as to outside entities and individuals. An evaluation guide is included in the handbook that identifies the types of information that shall be controlled and protected.

The Handbook consists of the following components:

- **Procedures for Handling MTA Security Sensitive Information:** Identifies the requirements for safeguarding against unauthorized disclosure of MTA Security Sensitive Information. It includes procedures for handling, caring, reproduction, storage, shipping, marking and labeling of MTA Security Sensitive Information.

- **Roles and Responsibilities:** defines and lists the responsibilities and roles of the individuals and employees of MTA and vendors who are authorized to work on projects containing MTA Security Sensitive Information and who play an important role in the implementation of the procedures of the MTA Security Sensitive Information Handbook.

- **MTA Evaluation Guide:** Is a guide that is used to identify the types of information that require protection. This guide applies to all design, development, construction and/or maintenance contract documents.

- **Information Technology:** Information systems require protection and all electronic media shall be destroyed by third party software to insure complete erasure. The focus is on stored and distributed design and construction documents. Protection

requires a balanced approach that includes administrative, operational, physical and personnel controls.

- **Company Non-Disclosure and Confidentiality Agreements:** Establishes the contractual agreement between MTA and the vendors (Consultants, sub-consultants, contractors, sub-contractors, suppliers and others) for acknowledgement by the vendor of its understanding that shall be required to treat strictly confidential and privileged any MTA Security Sensitive Information whether provided by the MTA or developed by the vendor as their work product.

- **MTA Non-Disclosure and Confidentiality Agreement for Individuals:** Establishes an agreement between the MTA and the individuals (from both internally within the MTA organizations as well as outside entities such as vendors) gaining access to the MTA Security sensitive Information. It requires the individual agree to not disclose Sensitive and Privileged MTA Security Sensitive Information to an unauthorized person. Additionally, this agreement informs the individual that the trust has been placed in them by providing them access to MTA Security Sensitive Information and their responsibility to protect that information from unauthorized disclosure.

- **Employee Employment and Resume Verification:** Each employee involved with MTA Security Sensitive Information has his/her employment and resume verified by the MTA Security Officer. A form is filled out by the employee to identify his/her education and employment history. The form includes the employee's educational background, military background, skills, technical licenses, names and addresses of companies that employee has worked for, and professional references not related to the employee whom he/she has known for at least one year.

- **Procurement Procedures (including Vendor's Non-Disclosure and Confidentiality Agreement):** This section contains requirements and responsibilities of the MTA when disclosing MTA Security Sensitive Information to vendors (prime consultant/Vendor as well as sub-consultants/sub-contractors, suppliers and others) during the solicitation process. A vendor's Non-Disclosure and Confidentiality Agreement is incorporated in the solicitation process.

- **Stand-Alone Handbook (Simplified and Condensed Version):** is a simplified version of the MTA Security Sensitive Information Handbook that shall be sent to vendors to read prior to executing the Non-Disclosure and Confidentiality Agreement. This shall be a supplement to the MTA Security Sensitive Information Handbook.

SECTION 2 RESPONSIBLITIES AND ROLES

This section defines the responsibilities, roles and authority of the different individuals involved with projects containing MTA Security Sensitive Information. Such individuals will be authorized to access, safeguard, use, reproduce, dispose of, and transmit all material containing MTA Security Sensitive Information.

The following individuals include:

MTA Security Officer: is an MTA employee (could be the project manager for the project containing MTA Security Sensitive Information) or is hired by MTA who is a US citizen or Permanent resident of the US who is responsible for implementing and overseeing all procedures for handling MTA Security Sensitive Information. The Security Officer is responsible for all the initial briefings, training and practice procedures provided to all authorized MTA employees. The MTA Security Officer will have a large impact on the decision whether information should be protected. The MTA evaluation guide will be evaluated by the security officer and the project manager of MTA and final decision is established by the security officer.

Agency Security Officer: is an MTA affiliate agency employee (could be the project manager for the project containing MTA Security Sensitive Information) or is hired by an MTA agency who is a US citizen or Permanent resident of the US who is responsible for implementing and overseeing all procedures for handling MTA Security Sensitive Information. The Security Officer of each agency will assist the Security Officer of MTA in implementing all briefings, trainings and practice procedures provided by MTA Security Officer to all authorized agency employees.

Vendor Security Officer: is an employee of the consultant, contractor, and sub-contractor (could be the project manager for the project containing MTA Security Sensitive Information) or is hired by the consultant, contractor, and sub-contractor who is a US citizen or Permanent resident of the US who is responsible for implementing and overseeing all procedures for handling MTA Security Sensitive Information. The Security Officer of each contractor, consultant, and sub-contractor will assist the Security Officer of MTA in implementing all briefings, trainings and practice procedures provided by MTA Security Officer to all authorized consultant, contractor and sub-contractor employees. Vendor Security Officer reports to either MTA Security Officer or Agency Security Officer.

MTA/Agency Project Manager: is the project manager of each task order on behalf of MTA or it's affiliate agency. He/she is the individual who is in charge of the project and can be the Security Officer of MTA/Agency at the discretion of MTA. The project manager should be authorized to handle all MTA Security Sensitive Information and in charge of assisting all MTA/Agency employees in implementing all briefings, trainings and practice procedures provided by the Security Officer of MTA/Agency. The project manager will have signed a Non-Disclosure Confidentiality Agreement that will establish an agreement between MTA/Agency and the project manager where by the individual

agrees to not disclose MTA Security Sensitive Information to an unauthorized person. An employee employment and resume verification will be performed on such individuals.

Vendor Project Manager: is the project manager of each task order on behalf of the Vendor. He/she is the individual who is in charge of the project and can be the Security Officer of the Vendor at the discretion of MTA. The project manager should be authorized to handle all MTA Security Sensitive Information and in charge of assisting all Vendor employees in implementing all briefings, trainings and practice procedures provided by the Security Officer of the Vendor and the Security Officer of MTA/Agency. The project manager will have signed a Non-Disclosure Confidentiality Agreement that will establish an agreement between MTA/Agency and the project manager where by the individual agrees to not disclose MTA Security Sensitive Information to an unauthorized person. An employee employment and resume verification will be performed on such individuals. The vendor Project manager reports to the MTA/Agency Project Manager.

MTA Employee, including Agency employees: are the authorized employees of MTA and its affiliate agencies that will be involved with projects related to MTA Security Sensitive Information. They are responsible for the management and supervision of all employees of consultants, contractors, sub-contractors of projects related to Mat security Sensitive Information. All such employees will have signed a Non-Disclosure Confidentiality Agreement that will establish an agreement between MTA and the employees including MTA different agencies where by the employees agree to not disclose MTA Security Sensitive Information to an unauthorized person. An employee employment and resume verification will be performed on such individuals. MTA/Agency employee reports to the MTA/Agency Project Manager.

Vendor: are the companies (consultants, contractors, and sub-contractors) who have been selected as part of a pre-select list of companies by MTA to do all work related to projects containing MTA Security Sensitive Information. All vendors have undergone a procurement procedure prior to the selection process. All vendors will sign a Non-Disclosure Confidentiality Agreement that will establish an agreement between MTA and the vendor where by the vendor will agree to not disclose MTA Security Sensitive Information to an unauthorized person during the solicitation process. Additional questionnaires will be filled out by each vendor about its background and experience in the US and other foreign countries. An employee employment and resume verification will be also performed on the principals of each vendor.

Vendor Employees: are the authorized employees of the vendors (consultants, contractors and sub-contractors) that will be involved with projects related to MTA Security Sensitive Information. They are responsible for the design, and construction of all projects containing MTA security Sensitive Information under the guidance of MTA employees. All such employees will have signed a Non-Disclosure Confidentiality Agreement that will establish an agreement between MTA and the employees of consultants, contractors, and sub-contractors where by the employees agree to not disclose MTA Security Sensitive Information to an unauthorized person. An employee employment and resume verification will be performed on vendor employees authorized

to handle MTA Security Sensitive Information. Vendor employees report to the Vendor Project Manager.

SECTION 3 PROCEDURES FOR HANDLING MTA SECURITY SENSITIVE INFORMATION

Section 3.1 General

The purpose of this document is to safeguard MTA Security Sensitive Information as related to the Security Program of the Metropolitan Transportation Authority. It describes the requirements, evaluation criteria, restrictions, and other safeguards necessary to prevent unauthorized disclosure of MTA Security Sensitive Information and to implement control mechanisms for the authorized access and disclosure of information released by the Metropolitan Transportation Authority to its employees, vendors and their employees.

The handbook will enhance the successful management and protection of MTA Security Sensitive Information while meeting the needs of MTA employees including their affiliate agency employees, vendors and their employees.

Section 3.2 Access to MTA Security Sensitive Information

All MTA and their affiliate agency employees, vendors (consultants, sub-consultants, contractors, sub-contractors, suppliers, and others) and their employees performing work, shall safeguard all MTA Security Sensitive Information in accordance with the MTA document control procedures handbook. Contractors and consultants shall provide training to all employees authorized to access MTA Security Sensitive Information and, upon the request of the MTA, provide employee employment and resume verification as to an individual's suitability to have access. Vendor employees found by MTA 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.

Only authorized personnel, organizations and vendors will be given access to MTA Security Sensitive Information. Disclosure of MTA Security Sensitive Information should only be authorized as necessary, to meet fulfillment or performance of official duties, tasks, or service, and on a need-to-know basis. All vendors must complete the MTA Security Program Non-Disclosure and Confidentiality Agreement and original copies of the completed MTA security program Non-Disclosure and Confidentiality Agreement shall be provided to the MTA project manager and the MTA Security Officer. Employment and resume verification may be sponsored by MTA to verify the employment history, educational background and personal information of employees involved with MTA Security Sensitive Information.

Each vendor shall appoint an employee (US citizen or Permanent resident of US who is a legal alien resident of the United States) to be the company's Security Officer. The Security Officer shall sign a Non-Disclosure Confidentiality Agreement and shall have an MTA employment and resume verification form (see Section 7.0 of the MTA Security Sensitive Information Handbook) filled out to verify his/her resume, educational background and past history employment record including all references known to him/her for the past two years. The role of the Security Officer is an important one. The Security Officer is responsible for implementing and overseeing the MTA Security Sensitive Information Handbook.

In order to retain control of the employees of MTA, employees of the vendors involved with MTA Security Sensitive Information, an Authorized Personnel Project List shall be developed by the Security Officers of the MTA, and the vendors. The list shall provide information about the employees in terms of their names, addresses, and name of security officer they report to. The list shall be provided to MTA Security Officer to track the employees who have authorization to access MTA Security Sensitive Information.

The vendor shall ensure that employees provided access to sensitive and privileged MTA Security Sensitive Information are either citizens of the United States of America or an alien who has been lawfully admitted for permanent residence or employment (indicated by immigration status) as evidenced by US Citizenship and Immigration Services

documentation. The vendor shall also ensure that these employees have executed the MTA Non-Disclosure and Confidentiality Agreement.

The vendor must include the above requirements in any subcontract/agreement awarded that will require access to MTA Security Sensitive Information.

If an employee (MTA or Vendors) refuses to execute the agreement, access to sensitive and privileged MTA Security Sensitive Information must be denied.

The dissemination of MTA Security Sensitive Information shall only be made upon the determination that the recipient is authorized to receive it. The measure for determining authorization is a need-to-know and the execution of MTA Non-Disclosure and Confidentiality Agreement.

All vendors shall monitor their security programs on a continuing basis and shall also provide control and accountability of documents containing MTA Security Sensitive Information by tracking the location and number of copies. A document control system in terms of logging documents shall be developed to track, identify and protect all documents related to contracts involved with MTA Security Sensitive Information.

Security requirements shall be made a material condition of MTA contracts that will require access to MTA Security Sensitive Information. Contracts shall be subject to termination for default, when it has been determined that a failure to comply with security requirements resulted from willful misconduct or a lack of good faith.

Section 3.3 Safeguarding MTA Security Sensitive Information

All individuals authorized to access MTA Security Sensitive Information are responsible for safeguarding the MTA Security Sensitive Information in their custody or under their control. Vendors shall ensure that all authorized employees are aware of the prohibition against discussing MTA Security Sensitive Information in public conveyances or places, or in any other manner that permits interception by unauthorized persons. MTA Security Sensitive Information shall be protected at all times. Individuals that work with MTA Security Sensitive Information shall be personally responsible for taking utmost care and precautions to ensure that it remains protected from the unauthorized persons."

Use and Storage

All MTA Security Sensitive Information shall be stored in environments with password protection or in a secure container such as locked file cabinet, locked desk, or a safe-type file container. It is recommended that MTA Security Sensitive Information for each agency of the MTA be gathered and stored in a minimum number of office locations. The cabinets should be strong enough to resist vandalism. Containers shall bear no external markings indicating storage of MTA security sensitive material therein. A list should be maintained as to which individuals have access to which container. The MTA, consultant and Vendor Security Officer(s) are responsible to ensure that he/she receives and updated and timely list of personnel who have access to documents containing MTA Security Sensitive Information. It is strongly suggested that more than one employee has access to each storage container. Authorized individuals must protect passwords, keys, and/or combinations used to secure the MTA Security Sensitive Information. Documents containing MTA Security Sensitive Information may not be removed from the work premises by the vendors unless authorized by MTA. At the end of each project, all documents containing MTA Security Sensitive Information shall be stored at locations where card readers shall be installed to track who has been in and out of the location, particularly if it is accessible after business hours and on weekends.

Reproduction

Contractors and employees shall establish a reproduction control system to ensure that reproduction of MTA Security Sensitive Information is held to a minimum and is consistent with contractual and operational requirements. MTA Security Sensitive Information reproduction shall be accomplished by authorized employees. All unauthorized reproduction of MTA Security Sensitive Information should be prevented.

All copies of MTA Security Sensitive Information shall be marked in the same way as the original material. After the reproduction process is complete, the material shall be reviewed to ensure the markings are legible.

Disposal of Information

All MTA Security Sensitive Information must be destroyed by cross cut shredding or any other method that prevents unauthorized retrieval. After material containing MTA Security Sensitive Information reaches its disposal date, the Security Officer of the MTA will notify all authorized individuals, handling MTA Security Sensitive Information, that such material is now eligible for disposal. All destroyed documents will be logged through the document control system as described in Section 3.6. Procedures for the disposal of electronic media are covered in Section 5 (Information Technology Systems) of the MTA Security Sensitive Information Handbook.

Transmission of Information

MTA Security Sensitive Information shall be transmitted in a manner that prevents loss or unauthorized access. The transmission can be sent via any service with a receipt attached to or enclosed in the package. The receipt will identify the sender, the addressee and the document, but shall contain no sensitive information. The documents shall be packaged in a way that does not disclose its contents or the fact that it contains MTA Security Sensitive Information. All packages addressed to authorized individuals shall be treated with proper security although there is no indication that the package includes any MTA Security Sensitive Information. The package must be addressed only to authorized individuals previously identified on the approved list of individuals. All packages have to be opened by the authorized recipients. If the authorized recipients are not present then the materials will be returned to the sender and will not be left unattended.

Safeguarding Oral Discussions

The policies of the MTA Security Sensitive Information Handbook needs to be in place that prohibits vendors from discussing MTA Security Sensitive information in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

- Telephones and Radios: The use of wireless communications and radios falls under the same criteria as Safeguarding Oral Communications. Discussing MTA Security Sensitive Information in any manner that permits interception by unauthorized persons is not permitted. Cell phones and wireless phones should not be used for transmitting MTA Security Sensitive Information. Phone connections that are hard wired, or considered a land line or wire line are secure enough for discussions regarding MTA Security Sensitive Information. It needs to be pointed out here that when teleconferencing or use of speaker phones are incorporated, the persons discussing MTA Security Sensitive Information are responsible to limit eavesdropping exposure. Speaker phones should be used only in locations at which all doors are closed. This will limit the risk of eavesdropping by unauthorized individuals in earshot proximity to the conversation.

"Need-to-Know Basis"

Who should be allowed access to MTA Security Sensitive Information? The answer is determined by several criteria. Is the information necessary? Have they read and do they understand the procedures for safeguarding MTA Security Sensitive Information? Have they signed the Confidentiality and Non-Disclosure Agreement? Failure of any of the above is grounds for denying access to MTA Security Sensitive Information

Section 3.4 Markings of Documents

It is essential that all MTA Security Sensitive Information be marked to clearly convey to the holder the level of protection assigned to the information. Physically marking MTA Security Sensitive Information with protective markings serves to warn and inform holders that the document contains MTA Security Sensitive Information and needs to be protected. Each page of the document that contains MTA Security Sensitive Information shall be marked with the protective marking **"CONFIDENTIAL AND PRIVILEGED - MTA SECURITY SENSITIVE INFORMATION NON-FOILABLE"** or with the protective marking **"LIMITED DISTRIBUTION - MTA SECURITY SENSITIVE INFORMATION NON-FOILABLE"** where appropriate. The markings shall appear in ALL CAPS, BOLD on the top and bottom of each page. Only those pages that contain MTA Security Sensitive Information shall be marked. For drawings, the required protective markings shall appear in the title block. Sets of documents large enough to be folded or rolled shall be marked so that the marking is visible on the outside of the set when it is folded or rolled.

The overall marking "***This document is the property of the MTA. Further reproduction and/or distribution outside the authorized personnel team are prohibited without the express written approval of The Metropolitan Transportation Authority***" shall be conspicuously marked or stamped on the outside of the front cover, and on the title page. If the document does not have a back cover, the outside of the back or last page, which may serve as a cover, may also be marked at the top and bottom with overall classification of the document.

Section 3.5 Authorized Personnel Listings

In order to retain necessary control, listing of authorized individuals must be maintained by MTA, its affiliate agencies, and its vendors, for their employees who are provided access to MTA Security Sensitive Information. Such listings shall be maintained by MTA Security Sensitive Information and/or on a project basis. The Security Officer(s) at the MTA are responsible for developing, updating and retaining such lists for MTA employees having access to MTA Security Sensitive Information. Each vendor shall designate a Security Officer (subject to MTA approval) who will be responsible for developing, updating, and retaining a listing of their employees having access to MTA Security Sensitive Information. The vendor Security Officers shall be responsible for transmitting such updated listing to MTA Security Officer(s) at an agreed upon intervals or when requested by MTA. The vendor Security Officer may be requested to share such listings with other vendors' Security Officers when interaction between these vendors are expected during the performance of their contract work. The vendor Security Officers are responsible for accuracy of the listing and must notify the MTA immediately of any and all changes to authorized individuals on the listings.

The listings' will be used to authenticate all individuals that are authorized to have access to MTA Security Sensitive Information. If a name does not appear on the listing, the individual must be denied access to MTA Security Sensitive Information.

The listing must be updated as frequently as deemed necessary. The individuals identified as no longer having a need to have access to MTA Security Sensitive Information shall be removed from the listing.

Central filing system shall be developed for all personnel who have or had access to MTA Security Sensitive Information for investigative use later if necessary.

The listing shall include the following minimum information (See Table 1 as a sample):

- Vendor's Name and Address and contract information
- Name and contact information for the vendor's Security Officer
- Names, title, function, and contact information for the authorized individuals needing access to MTA Security Sensitive Information
- Dates the individuals signed the Non-Disclosure/Confidentiality Agreement and the employee employment and resume verification forms
- Date the privilege has been revoked, if any
- Initial listing creation date and last update date
- Revision history as an attachment

Section 3.6 Document Control System

The implementation of a document control system will provide control and accountability of MTA Security Sensitive Information by tracking the location, number of copies, and authorized participants who are responsible for creating and handling the documents containing MTA Security Sensitive Information. The document control system shall be such that it facilitates easy retrieval of the MTA security Sensitive Information from the individuals when the information is no longer required by those individuals. The document control system includes a log book that creates a paper trail of the material that is marked MTA Security Sensitive Information. The log book also creates a trail of all authorized individuals who have created and handled such documents. The Security Officers with the project managers of the MTA, its affiliate agencies, and Vendors should be responsible for developing separate document control systems in cooperation with the authorized individuals of each MTA, its affiliate agencies, and Vendors working on projects containing MTA Security Sensitive Information. All documents for MTA, its affiliate agencies and vendors will then be collected and gathered by the MTA Security Officer for auditing and review.

The log book shall include at a minimum (See Table 2 as a sample):

- The date that a document was created or received
- The identity of the creator or sender
- A very brief description of the document
- Transmission history (sent to who, when and how many copies)
- Notification that the document has been destroyed or returned to MTA
- An identification document control number assigned to MTA Sensitive Information for tracking, The number is structured as follows:
  CCC-PPPP-XXXX-mm-dd-yy-(Company Name) (Contract #)
  This code is the unique number of the document maintained by the document control system. The letter C is utilized for the number of copies. The letter P is the total number of pages in the document, the letter X is a sequential number assigned to information newly determined to MTA Sensitive Information. The following numbers are the date the document control number was logged into the system.

This log book shall be submitted to the MTA Security Officer periodically for review.

Section 3.7 Provisions Under FOIL (Freedom of Information Law)

The New York State Freedom of Information Law (Public Officers Law, Article 6, Sections 84-90, FOIL) establishes the right of the public to obtain information from agencies of New York State government and its local entities, including New York City. Modeled after the federal Freedom of Information Act of 1974 (FOIA, which applies to information controlled by the federal government), New York State FOIL creates a specific procedure through which members of the general public can exercise their right to see and copy most state and local government records in New York State.

According to FOIL, "government is the public's business and the public, individually and collectively and represented by a free press, should have access to the records of government". FOIL is intended to give them, that access.

FOIL applies to any agency, office, or department of New York State and its political subdivisions, such as cities, countries and towns. It applies to any administrative board, bureau, committee, or commission and quasi-governmental corporations. FOIL does not apply to court records.

The following can be obtained under FOIL:

- Agency Records: consist of any information kept, filed, or reproduced by or for an agency, in any physical form, a record may be a document, file, book, photograph, drawing, computer disk or tape.
- Legislative Records: consist of bills fiscal notes, messages received from the governor, transcripts or minutes of public sessions, audits and factual or statistical tabulations of material available for public inspection, and administrative staff manuals and instructions that affect the public.

Public Officers Law, Article 6, Section 87(2) (f) and (i), Freedom of Information Law

The original statute granted rights of access to nine specified categories of records to the exclusion of all others. Therefore, unless a record conformed to one of the categories of accessible records, it was presumed deniable. The current law, reversing that presumption, states that all records are accessible, except records or portions of records that fall within one of nine categories of deniable records (Section 87(2)). Each agency shall, in accordance with its published rules, make available for public inspection and copying all records, except that such agency may deny access to any one of nine categories of deniable records. One of the deniable records (Section 87(2) (f)) includes records or portions thereof that if disclosed endanger the life or safety of any person. Another deniable record (Section 87(2) (i))includes records or portions thereof that if disclosed, would jeopardize an agency's capacity to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures.

Section 3.8 Provisions Under 49 CFR Subpart 1520

Subpart 1520.1 governs the release, by an agency and by other persons, of records and information that has been obtained or developed during security activities or research and development activities. Records include any writing, drawing, map, film, photograph, or other means by which information is preserved, irrespective of format.

Subpart 1520.7 describes the information that an agency prohibits from disclosure. The Under Secretary prohibits disclosure of information developed in the conduct of security or research and development activities if, in the opinion of the Under Secretary, the disclosure of such information be detrimental to the safety of persons traveling in transportation. The records described in Subpart 1520.7 are not available for public inspection or copying, nor is information contained in those records released to the public.

Some of the records include the following:

Subpart 1520.7(h):	covers the release of information that the agency has determined may reveal a systemic vulnerability of the transportation system, or a vulnerability of transportation facilities to attack.
Subpart 1520.7(i):	protects information released by an agency concerning threats against transportation.
Subpart 1520.7 (q):	protects “images and description of threat images for threat projection systems”
Subpart 1520.7(r):	relates to all Department of Transportation information on “vulnerability assessment” irrespective the mode of transportation.

Section 3.9

AUTHORIZED PERSONNEL LISTINGS

Vendor:_____ **Security Officer:**_____

Address:_____ **Telephone Number:**_____

E-mail: _____

SSN	Name	Date of Birth	Date of Conf. Agreement	Date of Resume And Employment Verification	Container Access
222-22-2222	John J. Johnson	01/01/55	08/08/03	08/08/03	Locked Cabinet #1

Section 3.10 # DOCUMENT ACCOUNTABILITY LOG **Contract No:_____**

Originator or Received From	Document (Description & Date)	Control No. CCC-PPPP-XXXX-mm-dd-yy	Transmission	Disposition
ABC Company	Anchorage Study (1-8-03)	002-0050-0001-01-05-03	1-5-03 (2 Copies to ABC Company)	Destroyed

Page _____ of _____

Section 3.11 MTACC Audit Program

The MTACC Audit Program evaluates compliance with the requirements set forth in the MTA Security Sensitive Handbook by the consultants and vendors working on MTACC projects. Audits are conducted on an ongoing basis. Consultants and vendors working on MTACC projects shall conduct documented, formal self-inspections at intervals consistent with risk management principles.

The audit program includes:

- Verifying compliance with MTA Security Sensitive Handbook requirements.
- Assesses vendor's facility physical layout (i.e., where MTA Security Sensitive Information is stored and worked on).
- Evaluate procedures at the vendor's facility for handling and identification of MTA Security Sensitive Information.
- Interviews of staff

SECTION 4 MTA EVALUATION GUIDE

Section 4.1 General

The purpose of the MTA evaluation guide is to identify information that shall be treated as MTA Security Sensitive Information and needs to be protected from the unauthorized access or disclosure.

In order for the evaluation process to be simple yet highly effective in protecting the MTA Security Sensitive Information, the information shall generally be classified into three categories: "**UNPROTECTED**", "**MTA LIMITED DISTRIBUTION"** and "**MTA SECURITY SENSITIVE INFORMATION**".

The development of the guide shall be in consultation with the MTA Security Officer(s). A generic evaluation guide has been developed and included in this document to provide guidance in developing a project specific MTA evaluation guide.

The information that is expected to be used or created on the project shall be anticipated and evaluated in advance. As the new information is created/developed such as drawings, design calculations, reports, and specifications, a determination of whether or not the material in this document contains MTA Security Sensitive Information must be made. The vendor's Security Officer together with MTA Project Manager and MTA Security Officer(s) shall be responsible for identifying and protecting all MTA Security Sensitive Information.

Authority

The MTA evaluation guide for classification of information into "UNPROTECTED" "MTA LIMITED DISTRIBUTION" and "MTA SECURITY SENSITIVE INFORMATION" are issued under the authority of the Metropolitan Transportation Authority for the purpose of identifying the information that is sensitive and privileged MTA Security Sensitive Information that needs protection from unauthorized access or disclosure." Each Project manager will apply the evaluation guide to identify which of the information requires to be marked as MTA Security Sensitive Information. The MTA project manager under the guidance of the MTA Security Officer shall authorize the final approval or denial of the classification of information.

Applicability

Use of the MTA evaluation guide is applicable to MTA and its employees as well as vendors' and their employees. The guide shall also be used to classify the information during the procurement phase of the project.

Users of this guide are requested and encouraged to share ideas and thoughts for its improvement as well as to aid in maintaining it current, accurate and effective.

The MTA Evaluation Guide shall be provided to all MTA employees who require access to MTA Security Sensitive Information in connection with their work performance requiring safeguarding of MTA Security Sensitive Information.

An evaluation guide shall be provided to vendors in connection with MTA Security Sensitive Information contracts.

Review and Change

MTA Project Manager and MTA Security Officer shall review the existing Evaluation Guide periodically and shall issue a revised evaluation guide when a change occurs to the existing guidance or when additional security evaluation guidance is needed. The MTA Security Officer and MTA Project Manager shall go through the evaluation guide and change it accordingly to what is applicable to the specifics of a project.

Tentative Evaluation

If the information was not previously identified as MTA security sensitive information in the MTA evaluation guide, but the vendor or its employees believes based on their interpretation of security considerations that the information may or should be MTA security sensitive information; the individual shall protect the information as though it is MTA security sensitive information and submit it to the MTA Security Officer(s) for an evaluation determination.
The final determination will be evaluated by the MTA Security Officer. In such a case, the following marking, or one that clearly conveys the same meaning, may be used

Evaluation Determination Pending
Protect as MTA SECURITY SENSITIVE INFORMATION

This marking shall appear conspicuously at least once on the material but no further markings are necessary until an evaluation determination is received.

Pubic Release

The fact that MTA Security Sensitive Information has been made public does not mean that it is automatically unprotected. Individuals and vendors shall continue to protect the information until formally advised to the contrary. Questions as to the proprietary of continued evaluation in theses cases should be brought to the immediate attention of MTA Security Officer(s).

Contractual Release

It is the vendors' responsibility to understand and apply all aspects of the evaluation guide. The MTA Evaluation Guide is a guide necessary for performance on contracts containing MTA Security Sensitive Information. If the vendor determines that some of the documents evaluated as unprotected contain MTA Security Sensitive Information, the vendor should protect the information as though it is MTA Security Sensitive Information and submit it to MTA Security Officer(s) for further evaluation.

Evaluation Responsibilities

MTA and vendor employees, who, extract, or summarize MTA Security Sensitive Information, or who apply classification markings shall be sufficiently trained to follow and practice the procedures of the MTA Security Sensitive Information Handbook, shall have signed Confidentiality and Non-Disclosure Agreements and have ready access to the MTA evaluation guide.

MTA Security Evaluation Guidance

This guidance, developed by the MTA Security Officer and MTA Project Manager, is provided to a vendor by means of the MTA Evaluation Guide. The MTA Evaluation Guide will identify the specific elements of MTA Security Sensitive Information which require protection. It is the vendors' responsibility to understand and apply all aspects of the guide. The MTA evaluation guide is the exclusive property of the MTA, and the final determination of the appropriate evaluation of the information rests with the consent of MTA.

Upon completion of a contract that includes MTA Security Sensitive Information, the vendor must return to MTA all originals and destroy all copies of MTA Security Sensitive Information per the agreement with the MTA. The disposal of papers and electronic media containing MTA Security Sensitive Information shall follow the standards and procedures as described in Sections 2.3 and 4 of the MTA Security Sensitive Information Handbook. If MTA determines that the vendor has a continuing need for the information, the MTA must issue a letter to show the retention period and to provide final disposition instructions for material containing MTA Security Sensitive Information under the contract.

Section 4.2

MTA Limited Distribution Information is a designation used to identify a category of MTA Security Sensitive information that does not require entry into the document accountability system. MTA Limited Distribution Information is subject to all other handling and safeguarding requirements.

MTA Limited Distribution Information, typically generated during preliminary project work, is limited to drawings, presentations, calculations, administrative items and other related material. Vulnerability assessments, threat assessments and security related design criteria are not to be classified as MTA Limited Distribution at any time. MTA Limited Distribution material shall be entered into the document accountability when: (1) completed as a finished document; or (2) they are transmitted outside the design team.

MTA Limited Distribution information generated in the preparation of a finished document shall be: (1) dated when created; (2) marked as MTA Limited Distribution, with the cover or title sheet annotation, " This document contains information exempt from mandatory disclosure under the FOIA;" and (3) destroyed when no longer needed.

Section 4.3 Evaluation Guidelines for MTA

Topic	Evaluation	Remarks
Information, typically generated during preliminary project work, limited to drawings, presentations, calculations, administrative records and other related material excluding vulnerability & threat assessments and security related design criteria.	**MTA Limited Distribution Document**	
Any mention of information that reveals vulnerabilities, built-in or potential, relating to critical infrastructure	**MTA SECURITY SENSITIVE**	
That a facility is designed with extensive security features	**UNPROTECTED**	
Identity of Individual Security Systems installed at a facility	**MTA SECURITY SENSITIVE**	
Time frame or schedules showing project progress	**UNPROTECTED**	**UNPROTECTED** When MTA determines upon the totality of the circumstances that the information will not cause a facility to be vulnerable to a threat.
	PROTECTED	**PROTECTED** When presented outside the MTA and when the MTA determines the totality of the information will cause a vulnerability to a facility.
The general areas of the project or where security systems will be installed	**UNPROTECTED**	
Announcement of security subcontract awards	**UNPROTECTED**	

Results of site survey documentation or review that address specific physical security vulnerabilities	**MTA SECURITY SENSITIVE**	When referring to specific terrorist threats and/or the specific capabilities of the installation to counter the threat, or when referring to site-unique technical threat.
Design and construction information revealing details unique or essential to the security system(s).	**UNPROTECTED**	**UNPROTECTED** When referring to commercially available security systems, accepted construction techniques, information which is in the public domain and/or when security systems will be installed in area accessible to public view.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** When referring to methods of defeating the security system(s) and/or covert/unexposed security systems
Design drawings with specific forced entry ratings.	**MTA SECURITY SENSITIVE**	
Shop drawings that provide specific rating information	**MTA SECURITY SENSITIVE**	
What specific security system/hardware model number is installed at a specific location.	**MTA SECURITY SENSITIVE**	When referring to fire safety systems, access denial systems, intrusion detection systems, core area security systems, core area security systems, and in-place surreptitious entry verification systems.

Details concerning overall security system(s) or individual subsystem(s), including design, engineering, construction, and fabrication. Also includes capabilities, vulnerability diagrams, operational characteristics, and support requirements.	**UNPROTECTED**	**UNPROTECTED** When data is commercially available in the public domain.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** When high technology data, which was developed by or for the MTA, is (Cont'd) revealed; or when data is site specific or concerns core area systems
Security system effectiveness, to include range maneuverability, resolutions, accuracy, and readiness cycle.	**UNPROTECTED**	**UNPROTECTED** When the information is commercially available or in the public domain.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** When the system was developed or modified for or by the MTA; or when information concerns a specific special application.
Information identifying critical elements of the system; such as master controls, overrides, backup power sources	**UNPROTECTED**	**UNPROTECTED** If equipment is readily observable to the public
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** When an element has been developed and/or modified by or for the MTA for a special application; or when such elements are not readily observable by the public.
Security systems command and control operating instructions and supporting countermeasures when referring to a specific site or project location.	**MTA SECURITY SENSITIVE**	

Blast protection design requirements for new or existing MTA facilities.	**MTA SECURITY SENSITIVE**	
Blast analysis that addresses specific vulnerabilities to new or existing MTA facilities	**MTA SECURITY SENSITIVE**	If specific weaknesses are reflected or maximum tolerances are provided.
Structural plans, details, and specifications.	**UNPROTECTED**	**UNPROTECTED** When generic criteria are used, Site-specific information generated from generic criteria is MTA SENSITIVE
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** If site –specific information involves details of security system(s) or additional protection.
Design data revealing engineering, construction, or fabrication details of a Communications Center electrical system or facility support systems with signal cables (e.g., intercom, telephone). This includes grounding systems	**UNPROTECTED**	**UNPROTECTED** If generic design criteria/terms are used.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** If data reflects calculations resulting in selection of specific items to be used inside a specific Communications Center and/or listing of those items.
Drawings and specifications for emergency generator room or building	**MTA SECURITY SENSITIVE**	**MTA SECURITY SENSITIVE** If site-specific or if any reference to control or security system.
What vulnerabilities will	**MTA SECURITY**	

render the electrical and communications system(s) inoperative.	**SENSITIVE**	
Record documents identifying protective measures around Operations & Control Centers.	**MTA SECURITY SENSITIVE**	
Record documents identifying the location of Police and Emergency Communication Lines	**MTA SECURITY SENSITIVE**	
Any details or calculations that reveal security vulnerabilities at critical facilities[1]	**MTA SECURITY SENSITIVE**	If the details and calculations are related to the identification / protection of vulnerable systems with regards to security.

[1] Critical Facilities: facilities whose operation is deemed to be vital to the MTA and its agencies

Section 4.4 Examples: MTA Evaluation Guidelines

Topic	Evaluation	Examples
Information, typically generated during preliminary project work, limited to drawings, presentations, calculations, administrative records and other related material.	**MTA Limited Distribution Document**	Not to include any vulnerability assessments, threat assessments and security related design criteria.
Any mention of information that reveals vulnerabilities, built-in or potential, relating to critical infrastructure	**MTA SECURITY SENSITIVE**	Explicit details concerning identification of vulnerabilities within a security system, or strategies to mitigate against these vulnerabilities.
That a facility is designed with extensive security features	**UNPROTECTED**	Presence of bollards and barrier gates around access points to a facility, no explicit detail is revealed
Identity of Individual Security Systems installed at a facility	**MTA SECURITY SENSITIVE**	Identity of specific system that would allow for the knowlege of the system's capabilities and vulnerabilities.
Time frame or schedules showing project progress	**UNPROTECTED**	General construction schedules for work related to security projects.
The general areas of the project or where security systems will be installed	**UNPROTECTED**	Identification of general areas where construction will be implemented without revealing any explicit details or explicit capabilities.
Announcement of security subcontract awards	**UNPROTECTED**	Announcement of award.

Design and construction information revealing details unique or essential to the security system(s).	**UNPROTECTED**	**UNPROTECTED** Information about barriers and bollards placed around vulnerable locations of the facility is available to the public through the internet.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** Unique or essential information related to the security system that reveals capabilities or vulnerabilities.
Design drawings with specific forced entry ratings.	**MTA SECURITY SENSITIVE**	Drawings that indicate the rating of doors that access vulnerable locations inside a facility such as: doors for a bridge anchorage chambers or doors that access the pump stations in tunnels or cross passage doors in tunnels between the two tubes.
Shop drawings that provide specific rating information	**MTA SECURITY SENSITIVE**	Drawings that show the rating of bollards and barriers in terms of the weight and speed required to mitigate against threat.
What specific security system/hardware model number is installed at a specific location.	**MTA SECURITY SENSITIVE**	When referring to fire safety systems, access denial systems, intrusion detection systems, core area security systems, core area security systems, and in-place surreptitious entry verification systems.

Details concerning overall security system(s) or individual subsystem(s), including design, engineering, construction, and fabrication. Also includes capabilities, vulnerability diagrams, operational characteristics, and support requirements.	**UNPROTECTED**	**UNPROTECTED** Film application on glazing for minimizing human injuries due to glass fragmentation.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** The film capacity (thickness and attachment capacity at existing glazing frames) required to resist blast pressures and maintain integrity and function of the film and the attachments to the existing mullions.
Security system effectiveness, to include range maneuverability, resolutions, accuracy, and readiness cycle.	**UNPROTECTED**	**UNPROTECTED** The use of LASCOR protection **panels** and fiber reinforced composites for wall and column protection is available in the public. The use of fibers composites and LASCOR increases the strength of the structure and confines the existing concrete.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** LASCOR protection panels and fiber reinforced composites can be used to resist blast pressures. The resistance to blast pressures depends on the thickness of the panels and composites. Shock absorbers to be placed between the existing structures and mitigation panels.

Information identifying critical elements of the system; such as master controls, overrides, backup power sources	**UNPROTECTED**	**UNPROTECTED** Power generators installed for non critical rooms at under river tunnels.
	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** Auxiliary pumps in addition to the existing pumps installed to mitigate water leaks inside the tunnels due to an explosive event.
Security systems command and control operating instructions and supporting countermeasures when referring to a specific site or project location.	**MTA SECURITY SENSITIVE**	Equipment operating and maintenance procedures for countermeasure systems within command and control rooms.
Blast protection design requirements for new or existing MTA facilities.	**MTA SECURITY SENSITIVE**	Requirements including threat sizes, ratings, safe stand-off distances from threats to minimize damage, measured ductilitiy, strains, rotations and deflections of existing and new facilities.
Blast analysis that addresses specific vulnerabilities to new or existing MTA facilities	**MTA SECURITY SENSITIVE**	Analysis that reveals specific vulnerabilities (members, columns, locations) at the facility and required mitigation.
Structural plans, details, and specifications.	**UNPROTECTED**	**UNPROTECTED** All plans and structural drawings that show generic criteria and details not related to security issues.

	MTA SECURITY SENSITIVE	**MTA SECURITY SENSITIVE** Structural drawings that show security related reinforcement of structural components of facilities. For example, structural drawings that reveal steel paneling systems covering interior walls of tunnels or reinforcement of walls of vulnerable structures exposed to vehicular traffic. Drawings that show blast resistant walls around tower bases of bridges and fender systems in water around bridge piers will resist boat impact and to maintain minimum stand-off distance between the boats the piers. Other drawings that are considered sensitive will quantify the threat sizes used in design and the rating, strength and details required to resist blast pressures.
Design data revealing engineering, construction, or fabrication details of a Communications Center electrical system or facility support systems with signal	**UNPROTECTED**	**UNPROTECTED** Systems that are not related to security monitoring. The systems are intended for monitoring day to day passenger and traffic flow.

cables (e.g., intercom, telephone). This includes grounding systems	**MTA SECURITY SENSITIVE**	**MTA SECURITY SENSITIVE** Systems that are related to security monitoring. The systems could include camera screening inside transit facilities that are intended for monitoring suspicious activities due to a possible terrorist attacks. Television monitoring systems for tunnel facilities placed at the entrances of the tunnels to detect suspicious vehicles approaching the tunnels and can eventually be detained using rated barrier gates at the entrances of the tunnels. Sensor equipment placed on the suspender cables of a bridge that will detect any intruder trying to cut the cables of the bridges and will provide warning signals for immediate action.
Drawings and specifications for emergency generator room or building	**MTA SECURITY SENSITIVE**	Drawings and Specifications related to the reinforcement and mitigations measures related to reinforcing the structure of the emergency generator room for tunnel and transit facilities including vent buildings of underground tunnels, control stations of Tunnels, administration buildings of tunnels and pump stations and emergency power generator facilities.
What vulnerabilities will render the electrical and communications system(s)	**MTA SECURITY SENSITIVE**	Revealing vulnerabilities that will damage the electrical and

inoperative.		communications system of the facilities. These will include threats that will cause catastrophic failure of the structure containing such systems. Vandalism and terrorist attacks related to damaging electrical wiring, electrical and control panels related to communication systems.
Record documents identifying protective measures around Operations & Control Centers.	**MTA SECURITY SENSITIVE**	Documents that could include anti-ram perimeter protection (such as provided by adequately anchored bollards) at the curbs in order to prevent the scenario where a suicide attacker could have his or her vehicle hop the curb and ram into the control center buildings, possibly triggering explosives in the vehicle. Structural mitigations to the control facilities that will provide the necessary protection against threats inside the outside the building structures.
Record documents identifying the location of Police and Emergency Communication Lines	**MTA SECURITY SENSITIVE**	Site and civil drawings showing the location of buildings for the facility personnel (Police stations and emergency control stations) and identifying all possible vulnerable locations that will assist a terrorist in planning a suicide attack on such structures. Such facilities will include police stations for the tunnels, bridges, and transit systems, and

		administration buildings, control and communication stations.
Any details or calculations that reveal security vulnerabilities at critical facilities[1]	**MTA SECURITY SENSITIVE**	If the details and calculations are related to the identification / protection of vulnerable systems with regards to security.

[1] Critical Facilities: facilities whose operation is deemed to be vital to the MTA and its agencies

SECTION 5: INFORMATION TECHNOLOGY SYSTEMS

The Information Technology (IT) Systems that are utilized to electronically create, capture, process, store and/or transmit MTA Security Sensitive Information must be managed to protect against unauthorized access, interception, or disclosure of such information. The focus is on stored and distributed design and construction documents. Protection from unauthorized fabrication or modification of electronic media without knowledge is also a concern and, should be dramatically mitigated by following the procedures described in this section. Protection requires a balanced approach that includes operational, physical and personnel controls. The approach will initially focus on protecting Information Technology Systems containing MTA Security Sensitive Information pertaining to the present work at MTA. MTA may gradually undertake steps necessary to identify and protect MTA Security Sensitive Information that currently exists on the IT systems that are not pertaining to present work at MTA.

The major objectives of managing IT systems to protect MTA Security Sensitive Information on include:

- Restrict access to MTA security sensitive information exclusively to authorized users
- Complete removal of all MTA security sensitive information from the IT systems when it is no longer needed to be on it"

The procedures for protecting Information Technology Systems shall include the following:

Physical

Physical security safeguards shall be established by the use of user ID's and passwords to prevent unauthorized access to networked computers utilized in the day to day operations related to projects containing MTA Security Sensitive Information.

Physical security safeguards shall be established by the use of User ID's and passwords to prevent any unauthorized modification of the Automated Information Systems hardware and software related to MTA Security Sensitive Information. During overnight and non-working hours, when an Automated Information System is processing information unattended, or when MTA Security Sensitive Information remains on an unattended Automated Information system, the Automated Information Systems shall be located in a locked office space to prevent unauthorized entry into the space.

Operational

The following operational issues must be addressed:

- Security awareness training must be provided prior to assigning the individual access to Automated Information Systems and updated as needed.
- Users shall be required to authenticate their identities at "logon" time by supplying their password in conjunction with their user ID.
- MTA Security Sensitive Information files must be stored on a file system with a fire wall security (e.g. NTFS drives for Windows)
- All passwords and User ID of authorized employees shall be secured by the vendor.
- Successive logon attempts shall be controlled by denying access after multiple unsuccessful attempts on the same user ID.
- The individuals who are employees of MTA or vendors and who have authorized access to MTA Security Sensitive Information and who will control, restrict and evaluate the Information Technology Systems, shall ensure that all user ID's are revalidated at least within 30 days and all necessary information is updated as necessary.
- All data Files containing MTA Security Sensitive Information shall be access restricted to individuals listed on the authorized personnel listing.
- Unauthorized modification of the Automated Information System hardware and software containing MTA Security Sensitive Information shall be protected through user ID's and passwords. All accessories and storage media of systems hardware and software such as floppy disks and CD's will be kept in approved locked cabinets or locked areas/rooms which can be accessed through card readers or keys that are distributed to all authorized employees listed on the authorized personnel listings.
- All computer terminals containing MTA security sensitive Information shall be used by authorized individuals only and shall be networked among all other terminals used by authorized individuals who are listed on the authorized personnel listings. All such terminals shall be accessed through individual used ID's and passwords.
- All authorized employees of MTA, its affiliate agencies, and vendors shall have their own access rights expeditiously removed the minute they no longer work for their firms.
- Remote access to all servers and computers used by vendors working on projects containing MTA Security Sensitive Information shall be through a VPN or through a secured firewall specific to the vendors' authorized individuals listed on the authorized personnel listings.
- All electronic media that has stored information deemed MTA Security Sensitive Information at the time of disposition must be erased or destroyed.
- Access to protective-design software is restricted. Project-specific data is internally segregated and access is restricted to authorized users. Backup procedures and storage preserve security while providing redundancy.

- Project-specific data transfer between MTA and the Vendor offices shall be encrypted using the necessary software.

Personnel

Only individuals including MTA, its affiliate agencies and vendors listed on the authorized personnel listing are authorized to access, create, transmit or modify files containing MTA Security Sensitive Information.

The vendors shall be required to develop and submit to MTA their Information Technology (IT) System Management Plan for approval. At a minimum, the Management Plan must include measures developed and implemented by the vendor to address the objectives outlined in this section including physical, operational and personal procedures. The Management Plan shall also describe the IT Systems proposed to be used (both hardware and software)."

SECTION 6: METROPOLITAN TRANSPORTATION AUTHORITY

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT-INDIVIDUAL MTA SECURITY SENSITIVE INFORMATION

Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to certain sensitive information (MTA Security Sensitive Information) in connection with my participation in Metropolitan Transportation Authority Security initiatives.

1. **MTA Security Sensitive Information.** In the course of participating in MTA Contract #_____, that relates to various Security Initiatives, I may be given access to or entrusted with MTA Security Sensitive Information, and/or data belonging to or marked or considered as "MTA Security Sensitive Information". The MTA Security Sensitive Information and/or data that is covered by this Agreement is any information, including, but not limited to, technical information, security studies, threat correspondence, research and development activities, operating procedures, emergency services plans, studies, reports, drawing, specifications, calculations and other materials and information, that is provided by or on behalf of the MTA to me and is conspicuously identified as MTA Security Sensitive Information by markings, notice or otherwise.

2. **Obligations of Nondisclosure.** I agree that all MTA Security Sensitive Information is of a highly confidential nature and that such information shall only be used in the performance of the MTA Security Program or Project related business. I will not make any use of the MTA Security Sensitive Information for any purpose other than as expressly permitted by this Agreement or as expressly directed in writing by the MTA, and I agree that, from the date hereof and until such time the information is no longer considered MTA Security Sensitive Information, I will hold and treat the MTA Security Sensitive Information in the strictest confidence and will not:

A. except as required by law, directly or indirectly disclose or permit anyone to disclose such MTA Security Sensitive Information to any other person who is not a party to an MTA Non-Disclosure and Confidentiality Agreement of MTA Security Sensitive Information (and in the case of a person who is a party to an MTA Non-Disclosure and Confidentiality Agreement for MTA Security Sensitive Information, only to the extent that such information is required in connection with the MTA on a need-to-know basis without the prior written consent of an authorized representative of the MTA.

B. discuss with, disclose, release, reproduce or otherwise provide or make available the data containing MTA Security Sensitive Information, or any portion thereof, to unauthorized employee of MTA, Consultant and Vendor or to any person or entity (including, but not limited to subcontractor, joint venture, affiliate, successor or assignee of the Contractor) even after the completion of the contract.

C. use the data containing MTA Security Sensitive Information solely except for the purpose of performing duties under the subject contract. Any other use, disclosure release or reproduction is unauthorized and may result in adverse personnel action including termination from my employment.

3. **Protection of Information.**

A I will maintain the security of all documents, working papers, designs, and other materials related to the MTA, which contain MTA Security Sensitive Information in the manner consistent with MTA document control procedures handbook, and I will password protect all such information stored by me in electronic form. Any data stored by me in a computer shall be password protected, and secured in a manner agreed to by the MTA Security Officer.

B. If I am served with a subpoena or discovery request or receive a Freedom of Information Law request relating to, or am otherwise required by law to disclose, any MTA Security Sensitive Information, or a claim under Chapter 8 of the Contract between the Owner and the Contractor or Vendor, I will immediately notify MTA thereof to permit MTA to seek protective order or take other appropriate action. I will also cooperate in MTA's efforts to obtain a protective order or other assurance that secure treatment will be afforded the MTA Security Sensitive Information. In the absence of the protective order, I may disclose to the party compelling the disclosure only the part of the MTA Security Sensitive Information as is required to be disclosed (in which case, prior to such disclosure, I will advise and consult with MTA and its Security Officer as to such disclosure and the nature and wording of the such disclosure) and I will use my best efforts to obtain confidential treatment thereof.

I agree that if at any time I discover that MTA Security Sensitive Information has been inappropriately disclosed. I will immediately report the same to the MTA.

Return of Information. Upon the earlier of MTA's written request or completion of my need for such information, any and all MTA Security Sensitive Information obtained by me from the MTA or produced by me or Vendor and all copies thereof, and all writings and materials describing, analyzing or containing any MTA Security Sensitive Information and all copies thereof, shall be promptly delivered by the vendor to MTA at the vendor's expense, except that I may retain copies of such information in accordance with the requirements of this Agreement if (a) such retention is required for professional reasons and (b) I have received the express written consent of the MTA Security Officer for such retention.

Term. I understand that my obligations under this Agreement will be perpetual or until such time the information is no longer considered as MTA Security Sensitive Information.

Miscellaneous. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

I acknowledge that the unauthorized disclosure and handling of the MTA Security Sensitive Information could cause substantial damage and expose MTA and its facilities and customers to significant danger and could result in civil or criminal fines and penalties.

I acknowledge that the obligations of confidence required hereunder are extraordinary and unique and are vital to the security and well-being of MTA and its customers and that damages at law may be an inadequate remedy for any breach or threatened breach of this Agreement. MTA shall be entitled, in addition to all other rights or remedies, to seek injunctions restraining such breach, without being required to show any actual damage or to post any bond or other security.

This Agreement shall be governed by and construed in accordance with laws of the State of New York, without reference to its conflicts of laws principles.

Name: _____

Signature: _____

Title: _____

Date: _____

Employer: _____

Witness: (PRINT) _____
Signature: _____
Date: _____

Distribution Upon execution of this agreement

Vendor Security Officer (Original):_____
Employee (Copy):_____

Section 6.1 VERIFICATION AND ACKNOWLEDGEMENT (CONFIDENTIALITY AGREEMENT- INDIVIDUAL)

STATE OF _____

COUNTY OF _____

On the _____ day of _____ 2006 before me personally came and appeared _____ by me known to be said person, who swore under oath as follows:

1. He/she is _____ (print title)
   of_____ (firm / entity).

Sworn to before me the _____ day of _____, 2006.

NOTARY STAMP AND

SIGNATURE _____

Section 6.1.1

MTA SECURITY PROGRAM

ACKNOWLEDGEMENT OF RECEIPT

SECURITY SENSITIVE INFORMATION HANDBOOK

In connection with your work on the MTA Security Program, you will be given access to documents that are marked as Security Sensitive Information. Procedures for handling MTA Security Sensitive Information are provided in the MTA Security Sensitive Information Handbook, a copy of which has been provided to you.

In order to retain control of documents containing Security Sensitive Information, Authorized Personnel Project Lists will be maintained of staff who have received copies of the Handbook and signed this acknowledgement. These lists are intended to keep track of the employees who have authorization to access MTA Security Sensitive Information. If a name does not appear on a Project List, the individual will not be able to access MTA Security Sensitive Information relevant to that project.

I have received a copy of, carefully read, understand and will abide by the information outlined in the Security Sensitive Information Handbook.

Employee's Signature_____ Date: _____

Employee's Name (Please Print)_____

Employee's Work Location_____ Agency_____

SECTION 7.0 EMPLOYEE EMPLOYMENT AND RESUME VERIFICATION

All applicants are considered without regard to race, color, gender, religion, national origin, age, marital or veteran status, mental or physical disability unrelated to job performance or any other legally protected status.

PERSONAL INFORMATION

_____

Legal Name: First Middle Initial Last

_____

Address: Street City State Zip Code

Home Telephone: _____ Other Telephone: _____

E-mail: _____ Social Security #: _____

Driver's License #: _____ State: _____

Are you legally eligible for employment in the United States? □ Yes □ No

Are you a citizen of the United States? □ Yes □ No

Immigration/Visa Status: _____

Have you been convicted of a felony? □ Yes □ No

If yes, pleases explain circumstances: _____

_____

Are you at least 18 years old? □ Yes □ No

List of Residences(s) in reverse chronological order most recent for the past 10 years	From Mo/Yr	From Mo/Yr

Were you ever dismissed, removed or disqualified from a position, including public employment? □ Yes □ No

If you answer Yes, give full details including dates:

_____

_____

_____

EMPLOYMENT HISTORY (Most Recent First)

1. Job Title		Duties:
Employer:		
Dates of Employment (month/year) From: To:		
Starting Salary:	Ending Salary:	□ Full Time □ Part Time □ Temp
Employer's Address:		
Supervisor:	May we contact? □ Yes □ No	Phone:
Reason For Leaving		
2. Job Title		Duties:
Employer:		
Dates of Employment (month/year) From: To:		
Starting Salary:	Ending Salary:	□ Full Time □ Part Time □ Temp
Employer's Address:		
Supervisor:	May we contact? □ Yes □ No	Phone:
Reason For Leaving		
3. Job Title		Duties:
Employer:		
Dates of Employment (month/year) From: To:		
Starting Salary:	Ending Salary:	□ Full Time □ Part Time □ Temp
Employer's Address:		
Supervisor:	May we contact? □ Yes □ No	Phone:
Reason For Leaving		

MILITARY INFORMATION

1. Have you served in the U.S. Armed Forces? □ Yes □ No
   If Yes, indicate entry and separation dates.

_____

2. What was you Military Occupational Specialty (MOS)?

_____

3. Were you dishonorably discharged? □ Yes □ No
   If Yes, explain:

_____

EDUCATION INFORMATION

Type of School	Name and Location	Dates Attended	Degree Received	Subjects Studied	Did you Graduate?
High School					
College/ University					
Graduate School					
Tech School					
Grammar					

Special courses, training or experience required acquired, including military experience:

_____

_____

PROFESSIONAL OR TRADE LICENSE INFORMATION

1. List state professional or trade licenses issued, number and expiration date: _____

_____

2. Was any license/certification held by you ever suspended, restricted or revoked, or have you ever been censured or disciplined by any licensing or certifying organization? □ Yes □ No

   If the answer is yes, specify type of license or certification, action taken, from/to date and reason for action on a separate page.

SKILLS

Clerical/Office Skills		
Computer Skills	Name of Software:	□ WINDOWS □ MAC
Languages		
Other Special Knowledge or Skills		

Please describe any other experience, abilities or skills that might be helpful in considering your application: _____
_____

REFERENCES

Below, give the name of three professional references, not related to you whom you have known for at least one year

Name	Address	Phone Number	Years Acquainted

CERTIFICATION & AUTHORIZATION

I hereby certify that all statements made in this form are true and correct to the best of my knowledge and belief. I understand that any misrepresentations or omissions of facts in this application are grounds for disqualification from further consideration or for dismissal from employment.

I authorize investigation of all statements contained herein and to educational, professional and past employment history references as needed to research my qualifications for this position. I release the company from all liability for any damage that may result from utilization of such information.

If employed, I agree to conform to the rules, regulations and policies of the company. I understand that I will be an employee "at will" and either the company or I may terminate my employment relationship at any time for any reason not in violation of law.

I hereby acknowledge that I have read and fully understand the forgoing and seek employment under these conditions.

_____ _____

Signature of Employee **Date**

SECTION 8.0 PROCUREMENT PROCEDURES

Section 8.1 Document Security Notice to Prospective Vendors

Before releasing bid documents deemed to contain MTA Security Sensitive Information, the MTA should require all bidders to fill out a company Non-Disclosure and Confidentiality Agreement Form and an Information and Responsibility Request form revised to include security questions. All bids and proposal information containing MTA Security Sensitive Information must be protected by the contractors from unauthorized disclosure.
No person or other entity, who has been authorized to handle MTA Security Sensitive Information, may disclose vendor bid or proposal information to any person other than an authorized MTA person. If MTA deems a vendor unauthorized, that vendor should be denied bid documents containing MTA Security Sensitive Information.

The procurement procedures shall address all type of procurements:

- RFP for professional services
- RFP for construction and operation/maintenance contracts

Biddings, request for quotes, for construction and operation/maintenance contracts, as well as supply contracts.

No person or other entity may disclose Vendor bid or proposal information or MTA Security Sensitive Information other than a person who will sign an individual Non-Disclosure and Confidentiality Agreement and hence become authorized to handle MTA Security Sensitive Information. Bid or proposal information and MTA Security Sensitive Information must be protected from unauthorized disclosure. Individuals unsure if particular information is MTA Security Sensitive Information, should consult with the Security Officers of MTA and its affiliate agencies as necessary and mark the cover page and each page that the individual believes contains MTA Security Sensitive Information.

The following procedures are developed to provide guidance and are recommended to be incorporated into MTA procurement contracts containing MTA Security Sensitive Information for the MTA, upon approval from the respective legal departments. These procedures represent recommended language and concepts to ensure security in the procurement process at MTA. All awarded contract wording should include these procedures under the review and approval of the agency's legal department.

1. The vendor shall provide appropriate and reasonable physical and logical security for all data, files and programs containing MTA Security Sensitive Information of the MTA. The vendor shall ensure that similar, and equally adequate, procedures are employed by any party that will store, handle, use or examine any of the MTA Security Sensitive Information data.
2. The vendor shall take steps reasonably necessary to provide logical security for the computer-stored an off-line records, data, files and programs of the MTA.

Such logical security shall be in accordance with the highest standards in use in accordance with mutually agreed upon specifications with MTA.

3. No MTA Security Sensitive Information may be sent, shipped, mailed, e-mailed in any fashion whether manually or electronically or digitally to any site outside the borders of the United States. Within the borders of the United States, all senders and receivers of material containing MTA Security Sensitive Information will have signed a Non-Disclosure Confidentiality Agreement to authorize access to MTA Security Sensitive Information.
4. The vendor acknowledges that all MTA Security Sensitive Information is the exclusive property of MTA and is not to be shared with any third party other than what is required in order to perform the obligations under the awarded contracts.
5. The vendor shall take and continue to take during the term of this Contract, the appropriate employee confidentiality measures, by way of non-disclosure agreements, for the employees of the vendors who have access to MTA Security Sensitive Information.
6. The vendor shall not disclose the MTA Security Sensitive Information to a third party government, person or firm of representative thereof with out prior consent of the MTA Security Officer and MTA Project Manager.
7. The vendor shall not use MTA Security Sensitive Information for any other purpose other than for which it was provided or generated, with out the prior written consent of the MTA Security Officer and MTA Project Manager.
8. All MTA Security Sensitive Information and material containing MTA Security Sensitive Information provided or generated under awarded contracts will continue to be protected in the event of withdrawal by the recipient party or upon termination of the contract.
9. The vendor shall fully relinquish to MTA at the end of the project all original documents containing MTA Security Sensitive Information pertaining to the Work. The vendor warrants that its employees shall retain and return any original document containing MTA Security Sensitive Information and shall destroy all copies of such materials after the completion of the project. MTA Security Sensitive Information includes notes, photographs, renderings whether manual or electronic and digitally, sketches, scans or diagrams that may have been created by the vendor and its employees.
10. The vendor agrees to include similar procedures in each subcontract under any awarded contract.
11. The vendors shall inform the Security Officer of the MTA of the location where all MTA Security Sensitive Information will be kept during the duration of the work, and will have signed a Non-Disclosure Confidentiality Agreement stating the vendor's commitment towards and awareness of handling MTA Security Sensitive Information according to the MTA Security Sensitive Information handbook stated herein.
12. There shall be no dissemination or publication, except within and between the vendor and any subcontractors, of MTA Security Sensitive Information developed herein or contained in the reports to be furnished pursuant to these procedures without the prior written approval of the MTA Security Officer.

13. The vendor is prohibited from posting, modifying, copying, reproducing, republishing, uploading, transmitting or distributing in any way images, photographs, or renderings of the MTA property on any electronic media that can be accessed by an authorized individual listed on the authorized personnel listings without signing a Non-Disclosure Confidentiality Agreement and without the prior written consent and approval of the MTA.
14. All contractors shall provide MTA with their existing protocols for procedures to ensure security in the procurement process and in handling MTA security Sensitive Information. Such protocols shall be reviewed and certified by MTA Security Officer for compliance with procedures included in the MTA Security Sensitive Information Handbook.

Section 8.1.1 Prime Vendor Responsibilities

1. Limiting Distribution to Authorized Users: All documents and information containing MTA Security Sensitive Information shall be distributed to prospective contractors, subcontractors, architects, engineers, consultants, and suppliers that have completed an MTA company Non-Disclosure and Confidentiality Agreement. In addition, Contractors and sub-contractors will complete a responsibility and information request forms in addition to the company Non-Disclosure and Confidentiality Agreement. The responsibility and information request forms shall include the following identification requirements:

- A copy of the valid business license or other documentation granted by the State or jurisdiction to conduct business
- Verification of a valid DUNS Number
- A valid IRS tax ID number
- A valid picture state driver's license
- Response to some additional questions related to the Vendor's work history.

2. Retaining and Destroying Documents: At the conclusion of all contracts, all copies of MTA Security Sensitive Information shall be destroyed by the contractor. Copies of MTA Security Sensitive Information shall be destroyed as soon as possible after it has served the purpose for which it was released by MTA, developed and prepared by the contractor, and originals shall be retained and returned to MTA after completion or termination of the contract. Destruction shall be done by cross shredding hardcopies, and/or physically destroying CD's, deleting and removing files from the electronic recycling bins, and removing material from computer hard drives using a permanent erase utility or similar software.

3. Term of Effectiveness: all efforts required above shall continue throughout the entire term of contract. All MTA Security Sensitive Information shall be safeguarded against unauthorized use for the term of the retention.

4. Written Agreement of Disposal: A written statement is required for the disposal of MTA Security Sensitive Information. The written statement shall include the date of disposal, identify the material destroyed, and be signed by the individuals designated to destroy and witness the destruction. MTA shall be required to know, through their personal knowledge, that such material was destroyed. At the contractor's discretion, the destruction information required may be combined with other required control records. Destruction of document records shall be maintained by the vendor for 2 years.

I agree that I will abide by this agreement and will only disseminate Sensitive Security Information to other authorized users under the conditions set forth above

Signature:_____

Title: _____

Date: _____

Section 8.1.2 Information to be Furnished by Each Vendor

THE METROPOLITAN TRANSPORTATION AUTHORITY
SOLICITATION NO._____

Vendor's Full Legal Name: _____

Form of legal entity: _____* (corporation, partnership, joint venture, sole proprietorship, etc.)

Organized in: _____ (state or country under whose laws vendor is organized)

Authorized Officer: _____ (Print)

IRS Federal Taxpayer Identification Number: _____

DUNS Number:_____

Mailing Address: _____

_____

Telephone Number: _____

Fax Number: _____

Copy of Business License Attached

March 15, 2006

Section 8.1.3 **Vendor Responsibility Data Form (Additional Questions)**

1. Will the vendor ensure each employee/staff requiring access to MTA Security Sensitive Information sign a Non-Disclosure Agreement and an Authorization to verify the Vendors Resume and Employment History?

   YES ☐ NO ☐

2. Does the vendor have any foreign property, foreign business connections, or foreign financial interests?

   YES ☐ NO ☐

3. Does vendor, any director, officer, principal or managerial employee of vendor, or any person or entity with a 10% or more interest in Vendor have any contact with a foreign government, its establishments (embassies or consulates), or its representatives, whether inside or outside the U.S., other than on official U.S. Government business?
   (Does not include routine visa applications and border crossing contracts)

   YES ☐ NO ☐

4. Has vendor, any director, officer, principal or managerial employee of Contractor, or any person or entity with a 10% or more interest in vendor now or ever been employed by or acted as a consultant for a foreign government, firm, or agency.

   YES ☐ NO ☐

March 15, 2006

Section 8.1.4 VERIFICATION AND ACKNOWLEDGMENT (INFORMATION TO BE FURNISHED BY EACH VENDOR)

* If the bid be submitted by a corporation, an affidavit must be submitted with the questionnaire showing the names and addresses of the directors and principal officers. The full legal title must be given here and a certified copy of the certificate of incorporation must be submitted together with the names and addressed of the directors and principal officers. If the vendor is a foreign corporation, proof must be submitted of its authority to transact business in the State of New York. If the bid is submitted by a partnership or a Joint Venture, the above blank must be filled in the following form: "the firm of A.B. & Co., composed of A., B., C., D., etc."(giving the names of all the partners or firms).

The MTA reserves the right to inquire further with respect to vendor's response: and vendor consents to such further inquiry and agrees to furnish all relevant documents and information as requested by the MTA.

Proposer must sign here: _____

STATE OF _____
COUNTY OF _____

On the _____ day of _____ 2006, before me personally came and appeared _____ by me know to be said person, who swore under oath as follows:

1. He/she is duly authorized to sign this questionnaire on behalf of said firm and duly signed this document pursuant to said authorization.
2. He/she is duly authorized to sign this questionnaire on behalf of said firm and duly signed this document pursuant to said authorization.
3. The answers to the questions set forth in this questionnaire and the representations set forth in this questionnaire are true, accurate and complete.

4. He/she acknowledged and understands that the questionnaire includes provisions which are deemed included in the contract if award to the firm.

Sworn to before me the _____ day of _____ 2006

Notary's Stamp and Signature. _____

8.2 THE METROPOLITAN TRANSPORTATION AUTHORITY

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT-VENDOR

Solicitation / Contract No. _____

1. This Confidentiality Agreement shall govern the disclosure to and use by _____ ("Vendor"), of all MTA Security Sensitive Information Materials provided by the Metropolitan Transportation Authority ("The MTA"), as well as any work product developed by the Vendor including conclusions of security assessments, evaluations and/or recommendations.

2. For purposes of this Agreement, "The MTA" may designate, as Security Sensitive those documents and materials that are marked "MTA Security Sensitive Information", to be confidential or sensitive in nature and not releasable to the public. Such documents may include but not limited to, plans, drawings, specifications, photographs, videotapes, or other such documents of any nature or description, that pertain to "The MTA" owned and/or operated facilities.

3. These Protected Materials are to be disclosed by the Vendor only to those persons or entities as explicitly authorized to view these Protected Materials on behalf of the Vendor as set forth in Appendix A (Solicitation) or Appendix B (Contract Performance) respectively, which are attached and made a part of this agreement. A complete Appendix A of this agreement shall be submitted with your Bid Proposal in the second phase of the solicitation and Appendix B shall be submitted after the contract is awarded for a finalized list of vendors performing the work.

4. Vendor agrees to the following:

a) That all "The MTA" documents marked "MTA Security Sensitive Information" and made available to the Vendor and its employees, shall be kept safe, secure, and confidential at all times.

b) Vendor represents that all such "The MTA" documents pertaining to the solicitation, shall be relinquished to "The MTA" within five (5) business days after the Bid Administration Unit has taken action at the end of the solicitation. The three (3) apparent lowest vendors may be directed in writing by the Contract Manager to not relinquish these documents until further notice. After the contract is awarded, the vendor warrants that all MTA Security Sensitive Information pertaining to the contract shall be relinquished to the MTA at the completion of the contract unless it has been requested by MTA to be retained by the vendor. Vendor further warrants that its employees, consultants, sub-consultants, subcontractors and agents shall not retain any of the materials containing MTA Security Sensitive Information or copies of such materials from the Solicitation or after the end of the Project Work. This includes any notes, photographs, renderings whether manual or electronic, sketches, scans, or diagram that may have been made by the Vendor or its consultants, sub-consultants, contractors, subcontractors and agents using "The MTA" documents.

c) Within seven (7) days after execution of this agreement, Vendor shall state in writing, to "The MTA" Security Officer where the documents used for the solicitation process or used during the Project Work are kept and the methods and safeguards the Vendor will undertake in order to prevent any unauthorized access or duplication of the "The MTA" documents, during the time period that these materials containing MTA Security Sensitive Information are in the possession of the Vendor.

5. In the event that any unauthorized persons or entities to whom the MTA Security Sensitive Information is disclosed, ceases to be engaged during the bidding process or during the Project Work, access to MTA Security Sensitive Information shall be terminated by the Vendor and the "The MTA" shall be

notified of the same in writing. Vendor shall ensure that such a person returns and relinquishes all MTA Security Sensitive Information to the Vendor.

6. "The MTA" shall create an inventory of all Materials containing MTA Security Sensitive Information being provided to the Vendor for control purposes. After completion of the Solicitation, all materials relinquished to the "The MTA" (to Bid Administration Mgr.) by the Vendor shall be checked against the inventory. During the Project Work, all material containing MTA Security Sensitive Information used by the vendor shall be periodically checked by MTA against the inventory list. At the end of the contract, all material relinquished to MTA will be checked against the inventory. All copies of the checked inventory during solicitation and the project work shall be forwarded to "The MTA".

7. Nothing contained in this Agreement shall create any relationship between the "The MTA" and any Third Party. Further, nothing in this Agreement shall create any rights for any third party nor any obligation on the part of the "The MTA" to any third party, including but not limited to the Vendors.

8. The MTA reserves the right to periodically audit the vendors' security practices during the solicitation process or during the Project Work to ensure that they are in compliance with the procedures outlined in the MTA Security Sensitive Information Handbook.

The contents of the materials that contain MTA Security Sensitive Information shall not be disclosed to anyone other than in accordance with this Agreement.

THIS AGREEMENT HAS BEEN DULY EXCECUTED THIS _____ day of _____, 2006.

By _____

On behalf _____)

(Vendor)

_____

Print name and title of Authorized Officer

_____

Vendor Federal ID number (EIN)

8.2.1 VERIFICATION AND ACKNOWLEDGEMENT (CONFIDENTIALITY AGREEMENT-VENDOR)

STATE OF _____

COUNTRY OF _____

On the _____ day of _____ 2006 before me personally came and appeared _____ by me known to be said person, who swore under oath as follows:

1. He/she is _____ (print title) of_____ (firm / entity).

2. He/she is duly authorized to sign this Confidentiality Agreement on behalf of _____ (firm / entity), and duly signed this document pursuant to said authorization.

Sworn to before me the _____ day of _____, 2006.

NOTARY STAMP AND

SIGNATURE _____

8.2.2 **APPENDIX A**

(Solicitation No._____)

Entities Authorized to view protected materials

1. Vendor Name: _____ Federal ID# _____

Address: _____

_____

Contact: _____ Phone Number: _____

2. Vendor Name: _____ Federal ID# _____

Address: _____

_____

Contact: _____ Phone Number: _____

3. Vendor Name: _____ Federal ID# _____

Address: _____

_____

Contact: _____ Phone Number: _____

4. Vendor Name: _____ Federal ID# _____

Address: _____

_____

Contact: _____ Phone Number: _____

8.2.3 APPENDIX B

(Contract No. _____)

Entities Authorized to view protected materials

1. Vendor Name: _____ Federal ID# _____
Address: _____
_____
Contact: _____ Phone Number: _____

2. Vendor Name: _____ Federal ID# _____
Address: _____
_____
Contact: _____ Phone Number: _____

3. Vendor Name: _____ Federal ID# _____
Address: _____
_____
Contact: _____ Phone Number: _____

4. Vendor Name: _____ Federal ID# _____
Address: _____
_____
Contact: _____ Phone Number: _____

March 15, 2006

MTA NON-DISCLOSURE AGREEMENT-ATTACHMENT

OVERVIEW OF MTA SECURITY SENSITIVE INFORMATION HANDBOOK

Table of Contents

Section

1	Summary
2	Procedures For Handling MTA Security Sensitive Information
3	Access to MTA Security Sensitive Information
4	Safeguarding MTA Security Sensitive Information
5	Marking of Documents
6	Authorized Personnel Listings
7	Document Control System
8	Information Technology Systems
9	Procurement Procedures
10	MTA CC Audit Program

March 15, 2006

Section 1 Summary

The procedures identified in this manual are to be used during the implementation of MTA Security Projects. This handbook prescribes requirements, restrictions and other safeguards that are necessary to prevent unauthorized disclosure of MTA Security Sensitive Information and to control authorized disclosure of such Information. In all instances, the safeguarding of MTA Security Sensitive Information is subject to law and may be superceded by, the Freedom of Information Law, Article 6 New York State Public Officers Law Sections 84 to 90 (See Section 3.7), requiring the disclosure of certain information. However; MTA may decide not to disclose under section 87 (2) (f) of the FOIL law (See Section 3.7) and under the provisions of 49 CFR subpart 1520 (See Section 3.8) which states that MTA may deny access to material containing MTA Security Sensitive Information that if disclosed could endanger the life or safety of any person and will adversely affect the security of the MTA. The procedures outlined herein, employ safeguarding requirements of control and accountability, storage, disclosure, reproduction, transmission, document shipment, disposition, and labeling. The handbook is used to safeguard MTA Security Sensitive Information and to control its authorized disclosure both internally within the MTA organizations as well as to outside entities and individuals. An evaluation guide is included in the handbook that identifies the types of information that shall be controlled and protected.

The Handbook consists of the following components:

- **Procedures for Handling MTA Security Sensitive Information:** Identifies the requirements for safeguarding against unauthorized disclosure of MTA Security Sensitive Information. It includes procedures for handling, caring, reproduction, storage, shipping, marking and labeling of MTA Security Sensitive Information.

- **Roles and Responsibilities:** defines and lists the responsibilities and roles of the individuals and employees of MTA and vendors who are authorized to work on projects containing MTA Security Sensitive Information and who play an important role in the implementation of the procedures of the MTA Security Sensitive Information Handbook. (Refer to Main MTA Handbook)

- **MTA Evaluation Guide:** Is a guide that is used to identify the types of information that require protection. This guide applies to all design, development, construction and/or maintenance contract documents. (Refer to Main MTA Handbook)

- **Information Technology:** Information systems require protection and all electronic media shall be destroyed by third party software to insure complete erasure. The focus is on stored and distributed design and construction documents. Protection requires a balanced approach that includes administrative, operational, physical and personnel controls.

- **Company Non-Disclosure and Confidentiality Agreements:** Establishes the contractual agreement between MTA and the vendors (Consultants, sub-consultants, contractors, sub-contractors, suppliers and others) for acknowledgement by the vendor of its understanding that shall be required to treat strictly confidential and privileged any MTA Security Sensitive Information whether provided by the MTA or developed by the vendor as their work product.

- **MTA Non-Disclosure and Confidentiality Agreement for Individuals:** Establishes an agreement between the MTA and the individuals (from both internally within the MTA organizations as well as outside entities such as vendors) gaining access to the MTA Security sensitive Information. It requires the individual agree to not disclose Sensitive and Privileged MTA Security Sensitive Information to an unauthorized person. Additionally, this agreement informs the individual that the trust has been placed in them by providing them access to MTA Security Sensitive Information and their responsibility to protect that information from unauthorized disclosure.

- **Employee Employment and Resume Verification:** Each employee involved with MTA Security Sensitive Information has his/her employment and resume verified by the MTA Security Officer. A form is filled out by the employee to identify his/her education and employment history. The form includes the employee's educational background, company names and addresses employee has worked for, and professional references not related to the employee whom he/she has known for at least one year.

- **Procurement Procedures (including Vendor's Non-Disclosure and Confidentiality Agreement):** This section contains requirements and responsibilities of the MTA when disclosing MTA Security Sensitive Information to vendors (prime consultant/Vendor as well as sub-consultants/sub-contractors, suppliers and others) during the solicitation process. A vendor's Non-Disclosure and Confidentiality Agreement is incorporated in the solicitation process.

Section 2 Procedures for handling MTA Security Sensitive Information

The purpose of this document is to safeguard MTA Security Sensitive Information as related to the Security Program of the Metropolitan Transportation Authority. It describes the requirements, evaluation criteria, restrictions, and other safeguards necessary to prevent unauthorized disclosure of MTA Security Sensitive Information and to implement control mechanisms for the authorized access and disclosure of information released by the Metropolitan Transportation Authority to its employees, vendors and their employees.

The handbook will enhance the successful management and protection of MTA Security Sensitive Information while meeting the needs of MTA employees including their affiliate agency employees, vendors and their employees.

Section 3 Access to MTA Security Sensitive Information

All MTA and their affiliate agency employees, vendors (consultants, sub-consultants, contractors, sub-contractors, suppliers, and others) and their employees performing work, shall safeguard all MTA Security Sensitive Information in accordance with the MTA document control procedures handbook. Contractors and consultants shall provide training to all employees authorized to access MTA Security Sensitive Information and, upon the request of the MTA, provide employee employment and resume verification as to an individual's suitability to have access. Vendor employees found by MTA 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.

Only authorized personnel, organizations and vendors will be given access to MTA Security Sensitive Information. Disclosure of MTA Security Sensitive Information should only be authorized as necessary, to meet fulfillment or performance of official duties, tasks, or service, and on a need-to-know basis. All vendors must complete the MTA Security Program Non-Disclosure and Confidentiality Agreement and original copies of the completed MTA security program Non-Disclosure and Confidentiality Agreement shall be provided to the MTA project manager and the MTA Security Officer. Employment and resume verification may be sponsored by MTA to verify the employment history, educational background and personal information of employees involved with MTA Security Sensitive Information.

Each vendor shall appoint an employee (US citizen or Permanent resident of US who is a legal alien resident of the United States) to be the company's Security Officer. The Security Officer shall sign a Non-Disclosure Confidentiality Agreement and shall have an MTA employment and resume verification form (see Section 7.0 of the MTA Security Sensitive Information Handbook) filled out to verify his/her resume, educational background and past history employment record including all references known to him/her for the past two years. The role of the Security Officer is an important one. The Security Officer is responsible for implementing and overseeing the MTA Security Sensitive Information Handbook.

In order to retain control of the employees of MTA, employees of the vendors involved with MTA Security Sensitive Information, an Authorized Personnel Project List shall be developed by the Security Officers of the MTA, and the vendors. The list shall provide information about the employees in terms of their names, addresses, and name of security officer they report to. The list shall be provided to MTA Security Officer to track the employees who have authorization to access MTA Security Sensitive Information.

The vendor shall ensure that employees provided access to sensitive and privileged MTA Security Sensitive Information are either citizens of the United States of America or an alien who has been lawfully admitted for permanent residence or employment (indicated by immigration status) as evidenced by US Citizenship and Immigration Services

documentation. The vendor shall also ensure that these employees have executed the MTA Non-Disclosure and Confidentiality Agreement.

The vendor must include the above requirements in any subcontract/agreement awarded that will require access to MTA Security Sensitive Information.

If an employee (MTA or Vendors) refuses to execute the agreement, access to sensitive and privileged MTA Security Sensitive Information must be denied.

The dissemination of MTA Security Sensitive Information shall only be made upon the determination that the recipient is authorized to receive it. The measure for determining authorization is a need-to-know and the execution of MTA Non-Disclosure and Confidentiality Agreement.

All vendors shall monitor their security programs on a continuing basis and shall also provide control and accountability of documents containing MTA Security Sensitive Information by tracking the location and number of copies. A document control system in terms of logging documents shall be developed to track, identify and protect all documents related to contracts involved with MTA Security Sensitive Information.

Security requirements shall be made a material condition of MTA contracts that will require access to MTA Security Sensitive Information. Contracts shall be subject to termination for default, when it has been determined that a failure to comply with security requirements resulted from willful misconduct or a lack of good faith.

Section 4 Safeguarding MTA Security Sensitive Information

All individuals authorized to access MTA Security Sensitive Information are responsible for safeguarding the MTA Security Sensitive Information in their custody or under their control. Vendors shall ensure that all authorized employees are aware of the prohibition against discussing MTA Security Sensitive Information in public conveyances or places, or in any other manner that permits interception by unauthorized persons. MTA Security Sensitive Information shall be protected at all times. Individuals that work with MTA Security Sensitive Information shall be personally responsible for taking utmost care and precautions to ensure that it remains protected from the unauthorized persons."

Use and Storage

All MTA Security Sensitive Information shall be stored in environments with password protection or in a secure container such as locked file cabinet, locked desk, or a safe-type file container. It is recommended that MTA Security Sensitive Information for each agency of the MTA be gathered and stored in a minimum number of office locations. The cabinets should be strong enough to resist vandalism. Containers shall bear no external markings indicating storage of MTA security sensitive material therein. A list should be maintained as to which individuals have access to which container. The MTA, consultant and Vendor Security Officer(s) are responsible to ensure that he/she receives and updated and timely list of personnel who have access to documents containing MTA Security Sensitive Information. It is strongly suggested that more than one employee has access to each storage container. Authorized individuals must protect passwords, keys, and/or combinations used to secure the MTA Security Sensitive Information. Documents containing MTA Security Sensitive Information may not be removed from the work premises by the vendors unless authorized by MTA. At the end of each project, all documents containing MTA Security Sensitive Information shall be stored at locations where card readers shall be installed to track who has been in and out of the location, particularly if it is accessible after business hours and on weekends.

Reproduction

Contractors and employees shall establish a reproduction control system to ensure that reproduction of MTA Security Sensitive Information is held to a minimum and is consistent with contractual and operational requirements. MTA Security Sensitive Information reproduction shall be accomplished by authorized employees. All unauthorized reproduction of MTA Security Sensitive Information should be prevented.

All copies of MTA Security Sensitive Information shall be marked in the same way as the original material. After the reproduction process is complete, the material shall be reviewed to ensure the markings are legible.

Disposal of Information

All MTA Security Sensitive Information must be destroyed by cross cut shredding or any other method that prevents unauthorized retrieval. After material containing MTA Security Sensitive Information reaches its disposal date, the Security Officer of the MTA will notify all authorized individuals, handling MTA Security Sensitive Information, that such material is now eligible for disposal. All destroyed documents will be logged through the document control system as described in Section 3.6. Procedures for the disposal of electronic media are covered in Section 5 (Information Technology Systems) of the MTA Security Sensitive Information Handbook.

Transmission of Information

MTA Security Sensitive Information shall be transmitted in a manner that prevents loss or unauthorized access. The transmission can be sent via any service with a receipt attached to or enclosed in the package. The receipt will identify the sender, the addressee and the document, but shall contain no sensitive information. The documents shall be packaged in a way that does not disclose its contents or the fact that it contains MTA Security Sensitive Information. All packages addressed to authorized individuals shall be treated with proper security although there is no indication that the package includes any MTA Security Sensitive Information. The package must be addressed only to authorized individuals previously identified on the approved list of individuals. All packages have to be opened by the authorized recipients. If the authorized recipients are not present then the materials will be returned to the sender and will not be left unattended.

Safeguarding Oral Discussions

The policies of the MTA Security Sensitive Information Handbook needs to be in place that prohibits vendors from discussing MTA Security Sensitive information in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

- Telephones and Radios: The use of wireless communications and radios falls under the same criteria as Safeguarding Oral Communications. Discussing MTA Security Sensitive Information in any manner that permits interception by unauthorized persons is not permitted. Ell phones and wireless phones should not be used for transmitting MTA Security Sensitive Information. Phone connections that are hard wired, or considered a land line or wire line are secure enough for discussions regarding MTA Security Sensitive Information. It needs to be pointed out here that when teleconferencing or use of speaker phones are incorporated, the persons discussing MTA Security Sensitive Information are responsible to limit eavesdropping exposure. Speaker phones should be used only in locations at which all doors are closed. This will limit the risk of eavesdropping by unauthorized individuals in earshot proximity to the conversation.

"Need-to-Know Basis"

Who should be allowed access to MTA Security Sensitive Information? The answer is determined by several criteria. Is the information necessary? Have they read and do they understand the procedures for safeguarding MTA Security Sensitive Information? Have they signed the Confidentiality and Non-Disclosure Agreement? Failure of any of the above is grounds for denying access to MTA Security Sensitive Information

Section 5 Markings of Documents

It is essential that all MTA Security Sensitive Information be marked to clearly convey to the holder the level of protection assigned to the information. Physically marking MTA Security Sensitive Information with protective markings serves to warn and inform holders that the document contains MTA Security Sensitive Information and needs to be protected. Each page of the document that contains MTA Security Sensitive Information shall be marked with the protective marking **"CONFIDENTIAL AND PRIVILEGED - MTA SECURITY SENSITIVE INFORMATION NON-FOILABLE"** or with the protective marking **"LIMITED DISTRIBUTION - MTA SECURITY SENSITIVE INFORMATION NON-FOILABLE"** where appropriate. The markings shall appear in ALL CAPS, BOLD on the top and bottom of each page. Only those pages that contain MTA Security Sensitive Information shall be marked. For drawings, the required protective markings shall appear in the title block. Sets of documents large enough to be folded or rolled shall be marked so that the marking is visible on the outside of the set when it is folded or rolled.

The overall marking "***This document is the property of the MTA. Further reproduction and/or distribution outside the authorized personnel team are prohibited without the express written approval of The Metropolitan Transportation Authority***" shall be conspicuously marked or stamped on the outside of the front cover, and on the title page. If the document does not have a back cover, the outside of the back or last page, which may serve as a cover, may also be marked at the top and bottom with overall classification of the document.

Section 6 Authorized Personnel Listings

In order to retain necessary control, listing of authorized individuals must be maintained by MTA, its affiliate agencies, and its vendors, for their employees who are provided access to MTA Security Sensitive Information. Such listings shall be maintained by MTA Security Sensitive Information and/or on a project basis. The Security Officer(s) at the MTA are responsible for developing, updating and retaining such lists for MTA employees having access to MTA Security Sensitive Information. Each vendor shall designate a Security Officer (subject to MTA approval) who will be responsible for developing, updating, and retaining a listing of their employees having access to MTA Security Sensitive Information. The vendor Security Officers shall be responsible for transmitting such updated listing to MTA Security Officer(s) at an agreed upon intervals or when requested by MTA. The vendor Security Officer may be requested to share such listings with other vendors' Security Officers when interaction between these vendors are expected during the performance of their contract work. The vendor Security Officers are responsible for accuracy of the listing and must notify the MTA immediately of any and all changes to authorized individuals on the listings.

The listings' will be used to authenticate all individuals that are authorized to have access to MTA Security Sensitive Information. If a name does not appear on the listing, the individual must be denied access to MTA Security Sensitive Information.

The listing must be updated as frequently as deemed necessary. The individuals identified as no longer having a need to have access to MTA Security Sensitive Information shall be removed from the listing.

Central filing system shall be developed for all personnel who have or had access to MTA Security Sensitive Information for investigative use later if necessary.

The listing shall include the following minimum information (See sample in main MTA Handbook):

- Vendor's Name and Address and contract information
- Name and contact information for the vendor's Security Officer
- Names, title, function, and contact information for the authorized individuals needing access to MTA Security Sensitive Information
- Dates the individuals signed the Non-Disclosure/Confidentiality Agreement and the employee employment and resume verification forms
- Date the privilege has been revoked, if any
- Initial listing creation date and last update date
- Revision history as an attachment

Section 7 Document Control System

The implementation of a document control system will provide control and accountability of MTA Security Sensitive Information by tracking the location, number of copies, and authorized participants who are responsible for creating and handling the documents containing MTA Security Sensitive Information. The document control system shall be such that it facilitates easy retrieval of the MTA security Sensitive Information from the individuals when the information is no longer required by those individuals. The document control system includes a log book that creates a paper trail of the material that is marked MTA Security Sensitive Information. The log book also creates a trail of all authorized individuals who have created and handled such documents. The Security Officers with the project managers of the MTA, its affiliate agencies, and Vendors should be responsible for developing separate document control systems in cooperation with the authorized individuals of each MTA, its affiliate agencies, and Vendors working on projects containing MTA Security Sensitive Information. All documents for MTA, its affiliate agencies and vendors will then be collected and gathered by the MTA Security Officer for auditing and review.

The log book shall include at a minimum (See sample in main MTA Handbook):

- The date that a document was created or received
- The identity of the creator or sender
- A very brief description of the document
- Transmission history (sent to who, when and how many copies)
- Notification that the document has been destroyed or returned to MTA
- An identification document control number assigned to MTA Sensitive Information for tracking, The number is structured as follows:
  CCC-PPPP-XXXX-mm-dd-yy (Company Name) (Contract #)
  This code is the unique number of the document maintained by the document control system. The letter C is utilized for the number of copies. The letter P is the total number of pages in the document, the letter X is a sequential number assigned to information newly determined to MTA Sensitive Information. The following numbers are the date the document control number was logged into the system.

This log book shall be submitted to the MTA Security Officer periodically for review.

Section 8 Information Technology Systems

The Information Technology (IT) Systems that are utilized to electronically create, capture, process, store and/or transmit MTA Security Sensitive Information must be managed to protect against unauthorized access, interception, or disclosure of such information. The focus is on stored and distributed design and construction documents. Protection from unauthorized fabrication or modification of electronic media without knowledge is also a concern and, should be dramatically mitigated by following the procedures described in this section. Protection requires a balanced approach that includes operational, physical and personnel controls. The approach will initially focus on protecting Information Technology Systems containing MTA Security Sensitive Information pertaining to the present work at MTA. MTA may gradually undertake steps necessary to identify and protect MTA Security Sensitive Information that currently exists on the IT systems that are not pertaining to present work at MTA.

The major objectives of managing IT systems to protect MTA Security Sensitive Information on include:

- Restrict access to MTA security sensitive information exclusively to authorized users
- Complete removal of all MTA security sensitive information from the IT systems when it is no longer needed to be on it"

The procedures for protecting Information Technology Systems shall include the following:

Physical

Physical security safeguards shall be established by the use of user ID's and passwords to prevent unauthorized access to networked computers utilized in the day to day operations related to projects containing MTA Security Sensitive Information.

Physical security safeguards shall be established by the use of User ID's and passwords to prevent any unauthorized modification of the Automated Information Systems hardware and software related to MTA Security Sensitive Information. During overnight and non-working hours, when an Automated Information System is processing information unattended, or when MTA Security Sensitive Information remains on an unattended Automated Information system, the Automated Information Systems shall be located in a locked office space to prevent unauthorized entry into the space.

Operational

The following operational issues must be addressed:

- Security awareness training must be provided prior to assigning the individual access to Automated Information Systems and updated as needed.
- Users shall be required to authenticate their identities at "logon" time by supplying their password in conjunction with their user ID.
- MTA Security Sensitive Information files must be stored on a file system with a fire wall security (e.g. NTFS drives for Windows)
- All passwords and User ID of authorized employees shall be secured by the vendor.
- Successive logon attempts shall be controlled by denying access after multiple unsuccessful attempts on the same user ID.
- The individuals who are employees of MTA or vendors and who have authorized access to MTA Security Sensitive Information and who will control, restrict and evaluate the Information Technology Systems, shall ensure that all user ID's are revalidated at least within 30 days and all necessary information is updated as necessary.
- All data Files containing MTA Security Sensitive Information shall be access restricted to individuals listed on the authorized personnel listing.
- Unauthorized modification of the Automated Information System hardware and software containing MTA Security Sensitive Information shall be protected through user ID's and passwords. All accessories and storage media of systems hardware and software such as floppy disks and CD's will be kept in approved locked cabinets or locked areas/rooms which can be accessed through card readers or keys that are distributed to all authorized employees listed on the authorized personnel listings.
- All computer terminals containing MTA security sensitive Information shall be used by authorized individuals only and shall be networked among all other terminals used by authorized individuals who are listed on the authorized personnel listings. All such terminals shall be accessed through individual used ID's and passwords.
- All authorized employees of MTA, its affiliate agencies, and vendors shall have their own access rights expeditiously removed the minute they no longer work for their firms.
- Remote access to all servers and computers used by vendors working on projects containing MTA Security Sensitive Information shall be through a VPN or through a secured firewall specific to the vendors' authorized individuals listed on the authorized personnel listings.
- All electronic media that has stored information deemed MTA Security Sensitive Information at the time of disposition must be erased or destroyed.
- Access to protective-design software is restricted. Project-specific data is internally segregated and access is restricted to authorized users. Backup procedures and storage preserve security while providing redundancy.

- Project-specific data transfer between MTA and the Vendor offices shall be encrypted using the necessary software.

Personnel

Only individuals including MTA, its affiliate agencies and vendors listed on the authorized personnel listing are authorized to access, create, transmit or modify files containing MTA Security Sensitive Information.

The vendors shall be required to develop and submit to MTA their Information Technology (IT) System Management Plan for approval. At a minimum, the Management Plan must include measures developed and implemented by the vendor to address the objectives outlined in this section including physical, operational and personal procedures. The Management Plan shall also describe the IT Systems proposed to be used (both hardware and software)."

Section 9 Procurement Procedures

Before releasing bid documents deemed to contain MTA Security Sensitive Information, the MTA should require all bidders to fill out a company Non-Disclosure and Confidentiality Agreement Form and an Information and Responsibility Request form revised to include security questions. All bids and proposal information containing MTA Security Sensitive Information must be protected by the contractors from unauthorized disclosure.
No person or other entity, who has been authorized to handle MTA Security Sensitive Information, may disclose vendor bid or proposal information to any person other than an authorized MTA person. If MTA deems a vendor unauthorized, that vendor should be denied bid documents containing MTA Security Sensitive Information.

The procurement procedures shall address all type of procurements:

- RFP for professional services
- RFP for construction and operation/maintenance contracts

Biddings, request for quotes, for construction and operation/maintenance contracts, as well as supply contracts.

No person or other entity may disclose Vendor bid or proposal information or MTA Security Sensitive Information other than a person who will sign an individual Non-Disclosure and Confidentiality Agreement and hence become authorized to handle MTA Security Sensitive Information. Bid or proposal information and MTA Security Sensitive Information must be protected from unauthorized disclosure. Individuals unsure if particular information is MTA Security Sensitive Information, should consult with the Security Officers of MTA and its affiliate agencies as necessary and mark the cover page and each page that the individual believes contains MTA Security Sensitive Information.

The following procedures are developed to provide guidance and are recommended to be incorporated into MTA procurement contracts containing MTA Security Sensitive Information for the MTA, upon approval from the respective legal departments. These procedures represent recommended language and concepts to ensure security in the procurement process at MTA. All awarded contract wording should include these procedures under the review and approval of the agency's legal department.

1. The vendor shall provide appropriate and reasonable physical and logical security for all data, files and programs containing MTA Security Sensitive Information of the MTA. The vendor shall ensure that similar, and equally adequate, procedures are employed by any party that will store, handle, use or examine any of the MTA Security Sensitive Information data.
2. The vendor shall take steps reasonably necessary to provide logical security for the computer-stored an off-line records, data, files and programs of the MTA. Such logical security shall be in accordance with the highest standards in use in accordance with mutually agreed upon specifications with MTA.

3. No MTA Security Sensitive Information may be sent, shipped, mailed, e-mailed in any fashion whether manually or electronically or digitally to any site outside the borders of the United States. Within the borders of the United States, all senders and receivers of material containing MTA Security Sensitive Information will have signed a Non-Disclosure Confidentiality Agreement to authorize access to MTA Security Sensitive Information.
4. The vendor acknowledges that all MTA Security Sensitive Information is the exclusive property of MTA and is not to be shared with any third party other than what is required in order to perform the obligations under the awarded contracts.
5. The vendor shall take and continue to take during the term of this Contract, the appropriate employee confidentiality measures, by way of non-disclosure agreements, for the employees of the vendors who have access to MTA Security Sensitive Information.
6. The vendor shall not disclose the MTA Security Sensitive Information to a third party government, person or firm of representative thereof with out prior consent of the MTA Security Officer and MTA Project Manager.
7. The vendor shall not use MTA Security Sensitive Information for any other purpose other than for which it was provided or generated, with out the prior written consent of the MTA Security Officer and MTA Project Manager.
8. All MTA Security Sensitive Information and material containing MTA Security Sensitive Information provided or generated under awarded contracts will continue to be protected in the event of withdrawal by the recipient party or upon termination of the contract.
9. The vendor shall fully relinquish to MTA at the end of the project all original documents containing MTA Security Sensitive Information pertaining to the Work. The vendor warrants that its employees shall retain and return any original document containing MTA Security Sensitive Information and shall destroy all copies of such materials after the completion of the project. MTA Security Sensitive Information includes notes, photographs, renderings whether manual or electronic and digitally, sketches, scans or diagrams that may have been created by the vendor and its employees.
10. The vendor agrees to include similar procedures in each subcontract under any awarded contract.
11. The vendors shall inform the Security Officer of the MTA of the location where all MTA Security Sensitive Information will be kept during the duration of the work, and will have signed a Non-Disclosure Confidentiality Agreement stating the vendor's commitment towards and awareness of handling MTA Security Sensitive Information according to the MTA Security Sensitive Information handbook stated herein.
12. There shall be no dissemination or publication, except within and between the vendor and any subcontractors, of MTA Security Sensitive Information developed herein or contained in the reports to be furnished pursuant to these procedures without the prior written approval of the MTA Security Officer.
13. The vendor is prohibited from posting, modifying, copying, reproducing, republishing, uploading, transmitting or distributing in any way images, photographs, or renderings of the MTA property on any electronic media that can

be accessed by an authorized individual listed on the authorized personnel listings without signing a Non-Disclosure Confidentiality Agreement and without the prior written consent and approval of the MTA.

14. All contractors shall provide MTA with their existing protocols for procedures to ensure security in the procurement process and in handling MTA security Sensitive Information. Such protocols shall be reviewed and certified by MTA Security Officer for compliance with procedures included in the MTA Security Sensitive Information Handbook.

Section 10 MTACC Audit Program

The MTACC Audit Program evaluates compliance with the requirements set forth in the MTA Security Sensitive Handbook by the consultants and vendors working on MTACC projects. Audits are conducted on an ongoing basis. Consultants and vendors working on MTACC projects shall conduct documented, formal self-inspections at intervals consistent with risk management principles.

The audit program includes:

- Verifying compliance with MTA Security Sensitive Handbook requirements.
- Assesses vendor's facility physical layout (i.e., where MTA Security Sensitive Information is stored and worked on).
- Evaluate procedures at the vendor's facility for handling and identification of MTA Security Sensitive Information.
- Interviews of staff