Washington Metropolitan Area Transit Authority

Board Action/Information Summary

Action / Information	MEAD Number:	Resolution:
(•) Action ( ) Information	100007	( ) Yes (•) No

TITLE:

IT Data Security Assessment

PURPOSE:

The purpose of this request is to initiate and award new competitive contracts and/or modifications to existing contracts for implementing a comprehensive IT Security program for WMATA. This is a request for a base year (FY 2009) and one option year. There is no obligation for the option year, which is based upon availability of funding and budget approval in FY 2010.

DESCRIPTION:

Information Technology (IT) has implemented WMATA enterprise-wide software applications supporting the major business and operational areas of the Authority. A critical aspect of any IT program is the assurance that the overall environment is secure and provides safeguards to assure the continuity of operations. To that end, IT has established the Office of Metro IT Security (MITS) to serve as the IT security risk management organization for the Authority. Independent of this action, the IT Security organization has a staff of six full time employees (FTE) who support the operational aspects of the security program with operational funds.

In support of the capital aspects of the security program, MITS will review, create, design, build and implement the following with FY09 and FY10 capital funding:

Information Security Policies, Standards, and Guidelines
Secure Remote Access
Enterprise Security Zones
Computer Incident Response

Implementation of these elements will complete Phase 1 of the security program. These are the most core elements of Metro`s enterprise security program, and provide the most basic security protections, even if further funding to complete the entire enterprise security program is not available in FY11 - FY13.

With the availability of FY11 - FY13 funding (estimated three-year capital funding required for Phase 2 is $12M), the remaining components of the Enterprise Security Architecture can be reviewed, created, designed and built. These components include:

Vulnerability Management
Enterprise Intrusion Detection and Prevention Systems
Enterprise Data Encryption
Identity Management System
Forensic Investigations and Analysis

Upon the complete implementation of these systems and services in FY13, the projects will be transferred to the MITS Operations staff for ongoing maintenance and support.

MITS will be a:

- catalyst for ensuring that information security risks are considered in both planned and ongoing operations,
- central resource for advice and expertise to business units throughout WMATA,
- conduit for keeping senior and executive management informed about security-related issues and activities affecting the organization

MITS is charged with implementing the elements of the IT security risk management program described above, involving the identification, documentation, development and implementation of policies, standards, procedures, and guidelines to ensure the confidentiality, integrity, and availability of WMATA`s electronic information assets. MITS will identify and implement strategies and tools for data classification and risk assessments. These will help to identify vulnerabilities and their associated threats so effective controls can be implemented.

To this end, MITS will acquire services, tools, and technologies to help facilitate review and generation of security policies, standards, guidelines, and procedures; compliance with commercial and federal regulations/laws (e.g. PCI, HIPAA); review of internal and external infrastructure; design and implementation of technical security controls; monitoring of ingress and egress points; Authority-wide audit and validation of user access to enterprise applications; review and audit of privacy and confidentiality controls to customer data.

FUNDING IMPACT:

Budget: Metro Matters
Project: Information Technology
Page: 125 & 126

Metro Matters

Budget Information:	FY09	FY10	TOTAL
Budget Amount:	$37,925,000	$24,695,000	$62,620,000
This Action:	$5,525,000	$2,800,000	$8,325,000
Prior Actions:	$0	$0	$0
Subtotal:	$5,525,000	$2,800,000	$8,325,000
Remaining Budget:	$32,400,000	$21,895,000	$54,295,000

Operating Budget Impact: In FY11, the operating impact will be $1M. If the program is funded through FY13 and the full program is completed, the additional impact in FY14 will be an additional $750K per year.

Capital Budget Impact: Hardware and software refresh of the enterprise security technology will occur every three years, at an estimated cost of $200K at the time of each refresh.

REMARKS: This action is subject to Board approval of the FY09 and FY10 budgets and availability of funds.

RECOMMENDATION:

The Board approves the initiation and award of new competitive contracts and/or modifications to existing contracts to implement a comprehensive IT Security program in compliance with the Authority`s policies and procedures and to exercise the option year based upon approved budget and availability of funds.

Enterprise Information Security Architecture Implementation

Project Description: The Enterprise Information Security Architecture implementation will provide the Authority with a comprehensive set of architectural controls to protect against both unintentional and targeted attacks on its voice and data infrastructure.

- Benefit to Customers
  - Prevents malicious attacks on Metro's rail operations
  - Protects automatic train control (ATC) systems
  - Safeguards customer and Authority's personnel and financial data

Customers' financial data protected

- Implications to Service
  - Prevents complete system disruption due to malicious, targeted intrusions
  - Prevents train derailments due to "hijacking" and manipulation of automatic train control (ATC) systems
  - Prevents financially-motivated identity theft, which leads to loss of customer confidence
  - Prevents unauthorized access and intrusions into Metro's core personnel and financial data

Service disruptions prevented