

Special Review

**Maryland Aviation Administration
Maryland Transportation Authority**

Improper Use of State Computer Resources

Certain Employees Used State Issued Computers to Access Sexually Oriented
Websites

Better Monitoring of Computer Usage is Needed

February 2007



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

-
- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.
 - Electronic copies of our audit reports can be viewed or downloaded from our website at <http://www.ola.state.md.us>.
 - Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.
 - The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.
-



Karl S. Aro
Executive Director

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Bruce A. Myers, CPA
Legislative Auditor

February 28, 2007

Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Senator Nathaniel J. McFadden, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We conducted a review of an allegation received through our fraud hotline related to the Maryland Aviation Administration (MAA), a unit of the Maryland Department of Transportation (MDOT). This allegation related to possible improper usage of State computer resources by certain employees. Our preliminary assessment disclosed that the allegation appeared to be credible and identified similar concerns related to employees at the Maryland Transportation Authority (MdTA), an agency of the State that also uses MDOT computer resources. Although MdTA is not a designated unit of MDOT, MdTA performs various activities on behalf of MDOT.

Our review disclosed that certain MAA and MdTA employees (for example, police officers and maintenance employees) used State issued computers to access sexually oriented websites, including websites containing nude and/or pornographic pictures. Specifically, our review of a 31-day period in fiscal year 2006 identified 6 MAA employees who had accessed inappropriate materials from 6 to 600 times over periods ranging from 2 to 8 days. In addition, our review also identified 16 MdTA employees who had accessed inappropriate materials from 17 to 2,200 times over periods ranging from 1 to 7 days. The majority of these incidents occurred during the employees' regular working hours. Furthermore, we were advised that the accesses made by police officers were unrelated to any type of law enforcement matter.

Our review was limited to those improper accesses where the computer system files specifically identified an employee by name. Because the computer system files frequently did not contain the names of the employees who accessed such sites, the number of employees and occurrences is understated. For example, on two days within the 31-day period tested, we noted hundreds of instances where inappropriate websites were accessed but, since none of the accesses could be identified to a specific employee, the occurrences on these days were not included in our results.

We noted that certain steps had previously been taken by MDOT to help prevent improper use of Internet resources. Specifically, an MDOT contractor used certain software to block employee access to unauthorized websites; however, such software is not fail-safe. Other procedures should be implemented to help monitor for inappropriate Internet usage by employees.

An Internet usage policy previously established by MDOT, and adopted by MAA and MdTA, limits the use of computer resources to the official business of the State. Furthermore, MdTA had previously supplemented these procedures by specifically prohibiting employees from accessing sites that contain sexual or pornographic material. In addition to being an improper use of State computer resources, employees accessing sexually oriented websites may contribute to creating a hostile work environment, thereby exposing the State to potential liability. Finally, accessing sexually oriented websites is an inappropriate use of employees' work time which adversely affects employee productivity and may compromise or degrade MDOT's computer systems through the introduction of computer viruses or other malicious software that can be contracted from these websites.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Scope, Objective, and Methodology

We conducted a review of an allegation received through our fraud hotline related to the Maryland Aviation Administration (MAA), a unit of the Maryland Department of Transportation (MDOT). The allegation related to possible misuse of State computer resources by certain employees. Our preliminary assessment disclosed that the allegation appeared to be credible and also identified similar concerns related to employees' misuse of State computer resources at the Maryland Transportation Authority (MdTA), an agency of the State that also uses MDOT computer resources. Although MdTA is not a designated unit of MDOT, MdTA performs various activities on behalf of MDOT.

The purpose of our review was to determine whether the allegation we received was valid and if the concerns identified in our preliminary review related to MdTA had merit. This review was performed in accordance with State Government Article, Section 2-1220 of the Annotated Code of Maryland.

Our review consisted of tests, analyses, observations, and discussions with MAA and MdTA personnel and others as we deemed necessary to achieve our objectives. Our review did not constitute an audit conducted in accordance with generally accepted government auditing standards. Had we conducted an audit in accordance with generally accepted government auditing standards, other matters may have come to our attention that would have been reported. Our review was conducted primarily from September 2006 through December 2006.

The MAA and MdTA responses to our findings and recommendations are included in an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise MAA and MdTA regarding the results of our review of their responses.

Background Information

The Maryland Department of Transportation (MDOT) - Office of Transportation Technology Service (OTTS) provides computing resources to the various modal units (including MAA) of MDOT, as well as to MdTA, and operates as a computer service bureau for these agencies. Specifically, OTTS staff provides computing, networking and telecommunications services for these agencies. Additionally, OTTS maintains the operating system and security software from which all applications are executed. OTTS, in conjunction with a MDOT contractor, operates a wide area network connecting computer users from MDOT's modal units, headquarters and MdTA, as well as providing Internet connections.

MAA is responsible for the operation, maintenance, protection, and development of the Baltimore/Washington International Thurgood Marshall Airport and the Martin State Airport.

MdTA performs activities on behalf of MDOT with regard to the supervision, financing, construction, operation, maintenance, and repair of the State's toll road facilities. The Secretary of MDOT serves as the Chairman of MdTA's oversight board.

Findings and Recommendations

Improper Use of State Computer Resources

Finding 1

Certain employees used State issued computers to access sexually oriented websites (including websites containing nude and/or pornographic pictures).

Analysis

Our limited review identified a total of 22 MAA and MdTA employees (for example, police officers and maintenance employees) who used State issued computers to access sexually oriented websites, including websites containing nude and/or pornographic pictures. Specifically, our review of a 31-day period in fiscal year 2006 identified 6 MAA employees who had accessed these inappropriate materials from 6 to 600 times over periods ranging from 2 to 8 days. In addition, our review also identified 16 MdTA employees who had accessed inappropriate materials from 17 to 2,200 times over periods ranging from 1 to 7 days. The majority of these incidents occurred during the employees' regular working hours. Furthermore, we were advised that the accesses made by police officers were unrelated to any type of law enforcement matter.

Our review was limited to those improper accesses where the computer system files specifically identified an employee by name. Because the computer system files frequently did not contain the names of the employees who accessed such sites, the number of employees and occurrences is understated. For example, on two days within the 31-day period tested, we noted hundreds of instances where inappropriate websites were accessed but, since none of the accesses could be identified to a specific employee, the occurrences on these days were not included in our results. Furthermore, although the files contained the time of website accesses, the duration of time for each access was not recorded.

An Internet usage policy previously established by MDOT, and adopted by MAA and MdTA, limits the use of computer resources to the official business of the State. The policy further provides that disciplinary action, up to and including termination, may be imposed for misuse of Internet privileges. Furthermore, MdTA had previously supplemented these procedures by specifically prohibiting employees from accessing sites that contain sexual or pornographic material. In addition to being an improper use of State computer resources, employees accessing sexually oriented websites may contribute to creating a hostile work environment, thereby exposing the State to potential liability. Finally, accessing sexually oriented websites is an inappropriate use of employee's work time which

adversely affects employee productivity and may compromise or degrade MDOT's computer systems through the introduction of computer viruses or other malicious software that can be contracted from these websites.

We provided senior management of both MAA and MdTA with documentation (for example, a computer disk) of the aforementioned accesses for further investigation.

Recommendation 1

We recommend that MAA and MdTA, in conjunction with MDOT, take immediate action to eliminate the improper use of State computer resources. Furthermore, since our findings were based on a review of a limited time period, we recommend that MAA and MdTA, in conjunction with MDOT, expand the time period reviewed and take appropriate corrective actions, including any disciplinary actions, as deemed necessary.

Finding 2

Additional controls should be implemented to monitor for improper use of State computers.

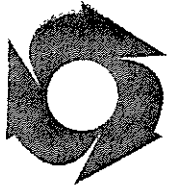
Analysis

While we noted that certain steps had been taken by MDOT to help prevent unauthorized Internet usage, additional steps could be taken to improve controls. Specifically, MDOT-OTTS's contractor used certain software to help block employee access to unauthorized websites. While this did prevent access to certain inappropriate sites, such software is not fail-safe. In that regard, we were advised by the contractor responsible for maintaining and operating the MDOT-OTTS operating system that additional procedures could be implemented to help monitor such accesses; however, the contractor advised us that MDOT had not directed it to monitor such accesses.

Recommendation 2

We recommend that MAA and MdTA, in conjunction with MDOT, develop and implement appropriate procedures to help monitor employee access to inappropriate websites and ensure compliance with Internet usage policies.

APPENDIX



Maryland Department of Transportation
The Secretary's Office

February 26, 2007

Martin O'Malley
Governor

Anthony G. Brown
Lt. Governor

John D. Porcari
Acting Secretary

Beverley K. Swaim-Staley
Deputy Secretary

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
Department of Legislative Services
Room 1202
301 West Preston Street
Baltimore MD 21201

Dear Mr. Myers:

Enclosed please find the Maryland Department of Transportation (MDOT) responses to the Legislative Auditor's draft special review dated February 9, 2007 for the Maryland Aviation Administration (MAA) – Maryland Transportation Authority (MdTA) – Improper Use of State Computer Resources. Additionally, an electronic version of this document has been sent to your office via e-mail (file name: MAASpecialReviewFeb2007) to response@ola.state.md.us.

If you or your staff have any questions or need additional information, please do not hesitate to contact me or Mr. David L. Fleming, Chief Financial Officer. Mr. Fleming can be reached at 410-865-1035.

Sincerely,

A handwritten signature in black ink, appearing to read "John D. Porcari".

John D. Porcari
Acting Secretary

Enclosures

cc: Mr. Timothy L. Campbell, Executive Director, Maryland Aviation Administration
Ms. Deborah A. Donohue, Principal Counsel, Maryland Transportation Authority
Mr. David L. Fleming, Chief Financial Officer, Office of Finance,
Maryland Department of Transportation
Mr. Ronald L. Freeland, Executive Secretary, Maryland Transportation Authority
Ms. Louisa H. Goldstein, Counsel, Maryland Aviation Administration
Mr. Joseph J. Lambdin, Director, Office of Audits,
Maryland Department of Transportation
Ms. Beverley K. Swaim-Staley, Deputy Secretary,
Maryland Department of Transportation

**Maryland Aviation Administration -
Maryland Transportation Authority –
Improper Use of State Computer Resources
Special Review Responses**

Improper Use of State Computer Resources

Finding 1

Certain employees used State issued computers to access sexually oriented websites (including websites containing nude and/or pornographic pictures).

MDOT/MAA Response:

The MAA concurs with the Legislative Auditors' recommendations. The MAA will or has already taken the following actions:

- The MAA has begun development of an IT Awareness Training Program to be implemented by June 30, 2007. As part of this training the proper use of the internet will be covered.
- A letter was sent to all MAA employees dated February 1, 2007 from the Executive Director reinforcing the importance of complying with the MDOT Email and Internet Policy.
- The MAA will utilize the services of an independent firm to expand the time period of review of inappropriate historical web access activities at the MAA. MAA is currently working with MDOT to procure such services and anticipates having a firm on board by June 30, 2007.
- The MAA took immediate action to appropriately discipline the six MAA employees who had accessed inappropriate websites.

In addition, MDOT and MdTA will, by December 31, 2007, take action to minimize improper use of State computer resources using personnel, funding and technology resources. The problem will be attacked in three ways: policy, procedure and technology by three organizations: Office of Human Resources, Office of the Attorney General and the Office of Transportation Technology Services. Policy will be reviewed and revised as necessary to ensure it is adequate and consistently applied throughout MDOT and MdTA. Technology will be improved and employed to screen for use of specific inappropriate websites and to confirm whether or not specific personnel have accessed inappropriate sites.

MdTA Response:

The MdTA concurs with the Legislative Auditors' (Auditors) recommendation to immediately eliminate the improper use of computer resources. The MdTA has taken the following actions:

**Maryland Aviation Administration -
Maryland Transportation Authority –
Improper Use of State Computer Resources
Special Review Responses**

- The MdTA conducted a review of the information provided by the Auditors on the 16 MdTA employees and the results sustain the Auditors’ finding regarding the improper use of computers.
- Disciplinary action, including suspension of internet privileges, was immediately taken with the employees assigned to our operation units. For the remaining employees (sworn police officers), MdTA Police management is currently evaluating the results of its review and will take appropriate disciplinary actions in accordance with the Law Enforcement Officers’ Bill of Rights.
- The MdTA will expand the testing and evaluate the best methods, including the possibility of using the services of an independent firm to expand the time period of review of inappropriate historical web access activities at the MdTA by July 1, 2007.

In addition to the above actions, a letter will be issued to all MdTA employees by March 16, 2007 from the Executive Secretary reinforcing the importance of complying with the MDOT Email and Internet Policy and that disciplinary actions will be taken with employees who are found to violate the policy. The employees will be required to sign and return a receipt to document that he or she has read the directive and understands the policy.

Finding 2

Additional controls should be implemented to monitor for improper use of State computers.

MDOT/MAA Response:

MDOT concurs with the auditors’ recommendation. MDOT and MdTA employ several procedures and technologies to help monitor and restrict access to inappropriate websites. Specifically, state of the art technology is employed to block known inappropriate websites. The developer of the technology continually expands the list of such sites and MDOT and MdTA also make updates. Other technology is used that can determine which websites particular individuals have accessed or if any particular sites have been visited. The MDOT Network Management Services (NMS) contractor, at the request of MDOT and MdTA runs this technology with results passed to the agency. Similar, but much improved, technology is nearing initial operational capability that will allow agencies to run their own queries without the need of contractor

**Maryland Aviation Administration -
Maryland Transportation Authority –
Improper Use of State Computer Resources
Special Review Responses**

involvement. The NMS contractor advises that there are no existing processes or procedures available in current internet security that completely eliminates access to inappropriate websites. However, the contractor has determined that MDOT and MdTA have sufficient software in place to reduce inappropriate use and to determine the source should it occur. MDOT and MdTA senior security professionals conducted an independent and objective review of current Web-filtering technologies and have concluded that they have implemented technologies that follow the contractor's state-of-the-art Internet security "defense in depth" best practices. That said, by December 31, 2007 more efficient and comprehensive use of available technologies, deployment of new ones as they become available and providing agencies more direct access to them will be employed by MDOT and MdTA to restrict access to inappropriate websites and monitor the Internet activities of personnel.

MdTA Response:

The MdTA concurs with the auditors' recommendation. MdTA staff has been working with the MDOT Office of Transportation Technology Services to develop and implement appropriate procedures to improve controls to prevent and detect inappropriate use of the Internet. We understand that the MDOT Network Management Services (NMS) contractor, at the request of Maryland Transportation agencies is nearing initial operational capability that will allow agencies to run their own queries without the need of contractor involvement. The MdTA will work with MDOT to define the reporting requirements and will implement procedures to monitor and control internet usage.