STATE OF IOWA

TECHNOLOGY AUDIT REPORT

FISCAL YEAR 2008

Prepared by DAS ITE:
Michael LaFary – Technician
Mary Hadd – Project Manager

October, 2008

Introduction

Per Iowa Code Section 8A.223[1] the Information Technology Enterprise of the Iowa Department of Administrative Services (DAS ITE) has completed a technology audit for Fiscal Year 2008 (July 1, 2007 – June 30, 2008).

> ***8A.223 Audits required.***
>
> *A technology audit of the electronic transmission system by which government records are transmitted electronically to the public shall be conducted not less than once annually for the purpose of determining that government records and other electronic data are not misappropriated or misused by the department or a contractor of the department.*
>
> In the above cite, the term "department" refers to the Iowa Department of Administrative Services, Information Technology Enterprise.

Methodology

Per legislative mandate, the Information Technology Enterprise conducted a technology audit of the electronic transmission system by which State of Iowa records are transferred to the public. Specifically, the audit is intended to determine if government records and electronic data were misappropriated or misused by the Department of Administrative Services Information Technology Enterprise or by contract personnel. As in past audits, the Information Technology Enterprise investigated the following potential areas of misuse and misappropriation:

- Inappropriate transmission of government records containing personal information about Iowa citizens.
- Inappropriate transmission of government records containing confidential government information.
- Inappropriate use of the State website for commercial advertising.

Research

Information Technology Enterprise personnel interviewed 37 State government employees at 16 separate State entities that were directly involved with electronic data transmission through the IowAccess network. The Information Technology Enterprise was able to conclude the following:

Directory and Document Review: Virus Scan

A virus detection scan was performed against the data the Audit Team was able to copy from the IowAccess website using the access credentials assigned to the Team. The scan product used was the ITE standard Sophos Anti-Virus software (workstation-based). A summary of the scan results follows:

- No items found containing a virus.
- No items placed in quarantine.
- No items requiring a 'fix'.
- Items containing "errors": 138.
    - Errors were of three types (assumed to be acceptable and requiring no further review):
        - "Format not supported".

[1] 8A.223 is the applicable code reference after the formation of the Iowa Department of Administrative Services. Code reference prior to July 1, 2003 was 14B.204

- "The file is encrypted".
- "Sophos Anti-Virus could not proceed – the file was corrupted."

Directory and Document Review: Age and Size of Documents

The review process revealed some directories and documents which appeared to be very old – and therefore perhaps outdated. Also discovered were files of significant size.

- Examples:
  - The server contains numerous documents which are more than three years old. Many are much older than that by several years.
  - The naming convention of some subdirectories implies the data they contain may be outdated. As an example: There are at least two with titles similar to "Old_Website".
  - Some of the sizable documents are named as 'Log Files'. One was greater than 1.2 GB in size.
    - Another significant characteristic of this particular Log File is its 'Last Modified Date' was more than three years ago.
- Additional Notes:
  - These items are mentioned primarily as a potential housekeeping task. It is assumed the vast majority of items on the website are valid and current. The age or size of a document does not mean it is invalid or should not be in the customer's directory.
  - The existence of 'old' documents could be due to maintenance of a customer's data having been performed by several staff members over the course of time.
  - There may be statutes and departmental requirements dictating certain documents are to be retained and remain available to the public for certain periods of time. Agencies should adhere to any requirements for document retention and public access.

IowAccess Server Account Maintenance

The understanding of the Audit Project Team is that it is the responsibility of the customer agency to request an IowAccess account for a staff member in their agency; and also to request deactivation of that account.

It appears the requesting agencies do not do a thorough job of keeping their account information current with ITE. Therefore, much of that burden is placed on ITE to perform this housekeeping for its customers.

The Audit Project Team has offered to assist the ITE IowAccess staff with this process. Previously, the ITE IowAccess staff has suggested possible development of an automated routine which could review account use/nonuse on a periodic or on a request basis and report these findings. (Note: Activity or inactivity on an account may not necessarily be an indication of its validity.) Also discussed was the possibility of sending emails to customer agencies inquiring about the status of their accounts and their accountholders. The Audit Project Team thinks these would be well-advised enhancements to the current account maintenance process.

Personal Information

- Iowa Interactive personnel were never given access to government records containing personal information about Iowa citizens beyond that required as part of their contract responsibilities and are subject to confidentiality provisions therein.

- DAS ITE personnel were never given access to government records containing personal information about Iowa citizens beyond that which was provided as a normal part of their job responsibilities.

Confidential Government Information

- Iowa Interactive personnel were never given access to government records containing confidential government information beyond that required as part of their contract responsibilities and are subject to confidentiality provisions therein.
- DAS ITE personnel were never given access to government records containing confidential government information beyond that which was needed as a normal part of job responsibilities.

Information Technology Enterprise personnel scanned the state's home page and reviewed all of the links to other web pages. The following table shows the links by type that were reviewed.

Fiscal Year 2008 data.	
Link Type	**Number of Links**
ftp://	68
gopher://	12
http://	138,212
https://	1,622
mailto:	16,242
news:	6
telnet://	2
file://	5,236
Other (links to local pages)	264,282
Total Links	425,682

None of the links to non-State web sites provided unauthorized commercial advertising.

Conclusion

Based upon the data reviewed, the Information Technology Enterprise found no evidence of misuse or misappropriation of government records by either DAS ITE personnel or contract personnel.

Department of Administrative Services	Department of Administrative Services Information Technology Enterprise
By:_____	By:_____
Ray Walton	John P. Gillispie
Interim Director	Chief Operating Officer
Department of Administrative Services	Information Technology Enterprise
Date:_____	Date:_____