

H. CARL McCALL
STATE COMPTROLLER



110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 11, 2002

Mr. Raymond P. Martinez
Commissioner
NYS Department of Motor Vehicles
224 South Pearl Street
Albany, NY 12228

Re: Planning and Security Policies and
Procedures for Implementing
E-Government Systems
Report 2001-S-39

Dear Mr. Martinez:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have audited the planning and security policies and procedures used by the Department of Motor Vehicles (Department) to implement its e-government systems. Our audit covered the period July 1, 1999 through December 31, 2001.

A. Background

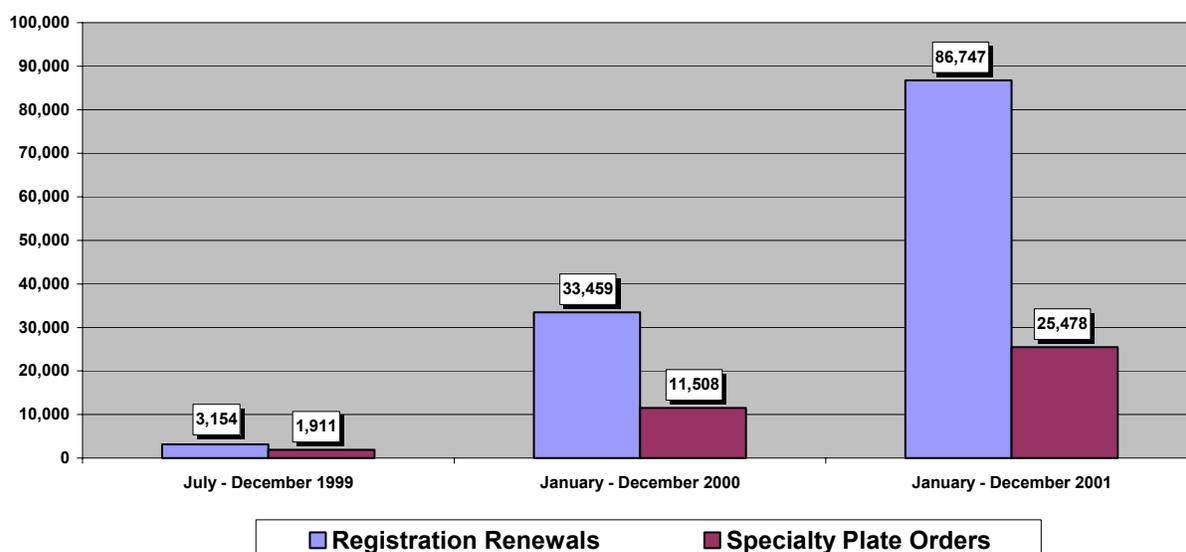
On June 12, 2000, the Governor of New York State electronically signed a proclamation to officially commence the State's electronic commerce initiative known as "Government Without Walls." The vision of this initiative is that virtually all critical government services will be available online 24 hours a day, 7 days a week to everyone from anywhere. This capability is generally referred to as electronic government (e-government). On August 15, 2000, the Commissioners and Executive Deputy Commissioners from 61 State agencies, in coordination with the Governor's Office for Technology (OFT), developed a list of the State's 75 top priority critical services and transactions that lend themselves to e-government. The Department is one of the first State agencies to embrace e-government services and establish an Internet website where citizens can transact these services.

As of December 31, 2001, the Department had three e-government services available on its website. One service, allows vehicle registration renewal as long as certain basic requirements are

met. Another service allows the public to order specialty license plates. The third e-government service allows the public to order duplicate titles in the event that the original title is lost.

According to the Department, the State has over 10.5 million registered vehicles. From July through December 1999, over 3,000 customers renewed registrations and almost 2,000 customers ordered a specialty plate using the Department's e-government services. In calendar year 2000, the first full year that the Department provided its e-government services, over 33,000 customers renewed registrations and over 11,500 customers ordered specialty plates over the Internet. In 2001 both of these totals more than doubled with nearly 87,000 registration renewals and over 25,000 specialty plates ordered over the Internet. While these transactions represent only a small percentage of the total registration renewals and specialty plate orders, the growth in these transactions, as shown in the chart below, reflects the increasing interest in having e-government services available.

Growth in e-Government Transactions



B. Audit Scope, Objectives and Methodology

We audited the planning and security policies and procedures used by the Department to implement its e-government systems for the period July 1, 1999 through December 31, 2001. One objective of our performance audit was to determine whether the Department had taken appropriate steps to plan and implement its e-government systems for vehicle registration renewal and specialty plate orders that were in place at the time of our audit. Another objective was to assess whether the Department's security policies and procedures were adequate to address the inherent risks of doing business on the Internet. To accomplish our objectives we interviewed appropriate Department staff and reviewed relevant Department documentation pertaining to e-government planning and security policies and procedures.

We conducted our audit in accordance with generally accepted government auditing standards. Such standards require that we plan and perform our audit to adequately assess those operations of the Department that are included within the audit scope. Further, these standards

require that we understand the Department's internal control structure and compliance with those laws, rules and regulations that are relevant to the operations that are included in our audit scope. An audit includes examining, on a test basis, evidence supporting transactions recorded in the accounting and operating records and applying such other auditing procedures as we consider necessary in the circumstances. An audit also includes assessing the estimates, judgments, and decisions made by management. We believe that our audit provides a reasonable basis for our findings, conclusions, and recommendations.

We use a risk-based approach to select activities for audit. We therefore focus our audit efforts on those activities we have identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we use finite audit resources to identify where and how improvements can be made. We devote little audit effort to reviewing operations that may be relatively efficient or effective. As a result, we prepare our audit reports on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities that may be functioning properly.

C. Results of Audit

We found that the Department started working on e-government services without the benefit of a strategic plan to guide the development and implementation of these services. We concluded that certain shortcomings in the Department's e-government initiative may have been avoided if such a plan had been properly prepared. We also found that the Department needs to improve security to protect its e-government services from unauthorized access and to allow for an adequate recovery of services in the event of a loss of computer resources.

D. Strategic Planning

A strategic plan specifies an organization's goals, identifies activities to meet the goals and provides performance measures to assess accomplishments. In 1997, a Department team identified the need for the agency to develop a vision for conducting its services, including defining the role of the Internet and establishing policies on the continued development and use of the Internet as a resource. However, at the time of our audit, the Department had just begun to develop a strategic plan for e-government services. In the absence of a strategic plan, we found that the Department's e-government initiative evolved without meaningful performance measures, inclusion of a key component of the Department's customer base and without a marketing approach for fully utilizing available services. Further, there was a need for greater attention to privacy and confidentiality concerns.

The Department's stated goals for e-government were to achieve customer convenience and to reduce employee workload and customer waiting times. However, the Department has not created a measurement system to gather data to assess whether, and to what extent, these goals are being met. While the Department compiles data that reflects the number of online transactions and the amount of revenues collected for e-government services, this data does not measure the accomplishment of the goals for the Department's e-government initiative. Providing appropriate performance measures for e-government services would enhance accountability for this initiative and give management a more meaningful way to assess progress.

As indicated previously, one goal of the Department's e-government services is to offer convenience to its customers. This goal is broad and applies to all citizens with vehicles registered in the State. However, since the Department did not have a strategic plan for its e-government services, the makeup and needs of its target audience were not adequately identified and addressed. For example, the Department has not designed its e-government services to effectively serve the State's non-English speaking component of the population. The Department makes manual forms available in several languages, such as Chinese, Hebrew, Italian and Spanish and prints its Drivers Manual in both English and Spanish. Spanish language telephone services are also available. However, these alternative language services are not available as part of the Department's e-government initiative. As a result of our audit, the Department has initiated additional research in this area to determine how best to proceed in providing alternative language content on its website. This information is available in a draft document issued by the Department in January 2002.

We found that the Department lacked a marketing approach to reach full utilization of e-government services. Although some services have been available since July 1999, the Department has done relatively little to promote the use of these services. Officials indicated that they have delayed significant marketing until more of the anticipated services are available online. We noted that the Department has organized a team to begin to promote these services.

In addition, according to recent studies on Internet usage, a major concern of citizens in utilizing online services is the privacy of the information they provide. To adequately address this concern, the Department has developed a privacy policy that is posted on its Internet web site. This policy addresses many areas of concern, including issues of data access and data security. However, we found that the privacy policy is neither easily located on the website, nor can it be found by using the existing search function. Further, we noted that two different versions of the privacy policy existed on the website, and neither version is dated to indicate which one is most current. These limitations may diminish public confidence in the security of e-government services. In addition, we determined that the Department's policy could be improved by defining what is meant by appropriate use of the website, and by identifying the penalties for inappropriate use.

We also found that there was no supporting documentation that the Department's legal counsel had reviewed the privacy policy. Department officials explained that the privacy policy was reviewed by legal counsel, however, the Department only requires a response if the counsel identifies an issue or concern. Since privacy is crucial to the success of e-government services, we believe the Department should obtain written confirmation of counsel's review and acceptance of the privacy policy.

E. Security Issues

The Computer Security Institute (CSI) is a nationally recognized organization dedicated to serving and training professionals involved in information, computer and network security. CSI, with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, conducts an annual survey of computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, to determine the scope of computer crime in the United States. The 2001 survey indicates that 91 percent of respondents detected computer security breaches within the last 12 months, 64 percent acknowledged financial losses due to computer breaches, and 35 percent of the respondents

estimated the total financial losses due to these breaches exceeded \$377 million. Based on this data, it is clear that organizations need to develop a comprehensive approach to information security.

According to the OFT Technology Policy 96-8, “since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls. Therefore, it is the responsibility of each State agency to protect confidential and sensitive information where intentional, inappropriate or accidental disclosure of the information might expose the State or an individual to loss or harm.” While there are many factors to be considered in establishing the intensity of the security measures that an agency should implement, there are certain basic issues that should be addressed within a security framework.

During the course of our audit, Department officials told us that they use the *Preferred Standards and Procedures for Information Security* (Preferred Standards) issued by OFT in June 1999. This document was designed to provide governmental entities with recommended minimum security standards. Section 2.5 of this document recommends the implementation of physical security that would include an assessment of the vulnerabilities along with an intrusion detection system to monitor network operations and identify when potential security breaches occur. We found that the Department does not routinely assess security vulnerabilities and has not implemented an intrusion detection system for its network operations. In addition, the Department does not have policies or procedures in place requiring a regular schedule for system maintenance and updates. Such policies and procedures are important to ensure, among other things, that the latest security updates have been installed in a timely manner. As a result of these weaknesses in security control, the Department’s information systems have an increased risk of unauthorized access without detection.

In addition, appropriate security over computer-based operations includes an adequate disaster recovery process, including procedures for business continuity. Such a process identifies a course of action to follow in the event of a disaster and loss of computer resources. OFT’s guidelines indicate that all systems should have backup and recovery procedures in place. We found that the Department does have a contingency plan in place, which was developed in response to the year 2000 crisis. However, this contingency plan does not address the Department’s e-government operations. These applications should be addressed within the Department’s disaster recovery plans to ensure that these services can recover from any potential disaster.

Recommendations

1. *Continue to develop and implement a strategic plan for e-government services.*

(Department officials indicate that the Gartner Group has been engaged to assist them in developing a strategic plan for e-commerce.)

2. *Establish performance measures for determining whether e-government is meeting related goals and objectives.*

(Department officials responded that they will continue to enhance and refine metrics for measuring the performance of e-commerce/e-government initiative in keeping with the

strategic plan. They also respond that it is inaccurate to assert that there is a lack of a measurement system to assess whether and to what extent goals are being met.)

Auditor's Comment: At the time of our audit there was no data to measure customer convenience, waiting times and employee workload in the field offices, and to determine how this data is impacted by the e-government applications.

3. *Continue to research the Department's customer base to ensure that all customer requirements, such as language needs and privacy concerns, are considered in current and future e-government applications.*

(Department officials report that they have completed their research, analysis and planning for the Spanish Web translation project, but state that it is inaccurate to indicate that this was done as a result of our audit.)

Auditor's Comment: At the time of our audit, there was no data to indicate that the Department had considered the needs of the non-English speaking population in its e-government initiative.

4. *Ensure the Department's Internet privacy policy is readily accessible and up-to-date and defines appropriate use and penalties for inappropriate use.*
5. *Maintain documentation of the Department's legal counsel's review and acceptance of the Internet privacy policy.*

(Department officials indicate that they are currently revising the security and privacy statement based on the model established by the State Office for Technology.)

6. *Continue efforts to develop and implement a marketing approach for e-government services.*

(Department officials indicate that they will continue to market the e-government initiative. They identified two initiatives that were implemented last fall.)

7. *Develop written security policies and procedures addressing vulnerability assessments, intrusion detection, and regularly scheduled system maintenance and updates.*

(Department officials indicate that they have begun developing a written security plan.)

8. *Develop a disaster recovery plan for the Department's e-government applications.*

(Department officials agree.)

We provided Department officials with a draft copy of this report for their review and comment. Their comments have been considered in the preparation of this report and are included as Appendix A. Department officials generally indicate that actions are being taken to implement the recommendations made in our report.

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

Major contributors to this report were Brian Reilly, Michael Farrar, Elizabeth Dunn, Robert Elliott, Emily Lonczak and Paul Bachman.

We wish to thank the management and staff of the Department for the courtesies and cooperation extended to our auditors during the audit.

Very truly yours,

Jerry Barber
Audit Director

cc: Deirdre A. Taylor, DOB



STATE OF NEW YORK
DEPARTMENT OF MOTOR VEHICLES
6 EMPIRE STATE PLAZA
ALBANY, NY 12228

RAYMOND P. MARTINEZ
Commissioner

GREGORY J. KLINE
Deputy Commissioner
For Administration

June 11, 2002

Mr. Jerry Barber
Audit Director
State of New York Office of the State Comptroller
110 State Street
Albany, New York 12236

Re: Audit Report 2001-S-39

Dear Mr. Barber:

Thank you for forwarding the draft audit report (2001-S-39) on the audit of DMV's E-Commerce/Internet Transactions. We have reviewed the draft and have some comments.

The Department has long recognized the potential customer service benefit from offering services and transactions to citizens of New York via the Internet. Our agency's Internet Office has been serving customers since 1996, offering traffic safety and operations information, forms to download and assistance via e-mail.

Beginning in 1998, we took our first step toward providing interactive customer service by providing access to DMV's computer system to allow customers to search the availability of personal plate combinations. Our fee-based transactions introduced in 1999 allow customers to order personal or custom plates or to renew their registrations on-line. We were able to provide these on-line services by leveraging our agency's existing computer systems and business rules and policies. These on-line transactions work the same way as transactions work in traditional service delivery channels and use the same back-end processing systems and procedures. They are subject to the same accounting and audit procedures as DMV's traditional transactions. In addition, we also maintain a log of all web transactions for additional control and to provide customer assistance.

Customer response to our Internet Services has been overwhelmingly positive. In keeping with Governor Pataki's 2000 announcement of creating a "Government Without Walls," we have begun to offer more on-line transactions and will continue to expand the Internet Office's service directory. Since September 2001, we have seen a significant

increase in the number of transactions processed on-line and are now approaching four million dollars a month in web-based revenues. We continue to implement plans to further promote the use of our web services using our existing direct mailings to DMV customers and via media outlets.

DMV has approached the Internet as an important tool for serving our customers and reducing costs. While we undertook our first efforts without a formally established strategic plan for e-commerce, it is evident that we approached this important initiative with deliberation. We have progressed incrementally, taking carefully planned steps toward expanding and improving our Web services, to reduce risk and increase the likelihood of success. The NYSDMV Internet Office has been recognized by both Accenture and the Gartner Group as being one of the leaders in Motor Vehicle web sites, in terms of the functionality and services offered. We at DMV are proud of what we have been able to achieve so far and look forward to what we expect to achieve in the future using the Internet.

While we recognize that there are always improvement opportunities to be found in any endeavor, we feel there are several findings in the audit that are in error, are misrepresented or were misunderstood. In the attached, we address each of these in an effort to clarify the findings represented in the report.

Sincerely,

A handwritten signature in black ink, appearing to read 'Gregory J. Kline', with a long horizontal flourish extending to the right.

Gregory J. Kline

Attachment

Attachment to DMV Response Re: Draft Audit Report 2001-S-39

Response to Recommendations

1. The Executive Management Guidance Team provided the strategic direction for e-commerce/e-government at DMV during our early development stage. We took a prudent, measured approach to implement our Internet Office transactions. We have also developed and continually work to improve standardized processes to guide e-commerce project analysis and planning, as well as the development, implementation and support of Internet transactions.

DMV has engaged the Gartner Group to assist us in developing an E-commerce Strategic Plan. DMV has begun the implementation of the Gartner E-commerce Strategic Plan preliminary recommendations while we await the finalization of the plan.

2. DMV believes that the assertion that “the Department has not created a measurement system to gather data to assess whether, and to what extent, [its] goals are being met” is inaccurate.

In addition to our longstanding practice of assessing performance and monitoring the adoption of Internet transactions via the number of transactions processed and revenues collected, we have also begun to measure and compare Internet volumes against transaction volumes through other available channels, including mail, phone and in-person office visits.

Our goals and objectives for e-commerce/e-government from the beginning have been to offer customer convenience, while reducing workload and wait times in our field offices. These goals have been and continue to be met with the implementation of DMV Internet transactions. We continue to experience tremendous growth in the usage of Internet transactions, now approaching four million dollars in web-generated revenues per month. Customer feedback (received via e-mail) continues to be positive. Further, DMV continuously monitors customer satisfaction for its available delivery channels. Our most recent customer survey, conducted in the spring of 2002, indicates that over 83% of our customers have found their Internet experience either “Good” or “Excellent.”

We will continue to enhance and refine our metrics in keeping with our e-commerce strategic plan.

3. We have completed our research, analysis and planning for the Spanish Web translation project, and have procured products and services which are now being used to prepare our website for automated machine translation. This includes optimization of our content using Plain English analysis tools to facilitate more accurate and reliable translations. Although our pilot will focus on Spanish as the target language, the solution we are

implementing provides us with the capability to introduce additional European languages and Asian languages when we are ready to expand the service. Our chosen solution can also support content in other formats, including e-mail, text files, databases, JavaScript, and XML. We are planning to implement our Spanish language translation pilot in August 2002.

In the meantime, we continue to identify and add Spanish content that is currently available from existing translations of DMV brochures and manuals. We are also researching arrangements for obtaining Spanish translations in an electronic format whenever we contract for the development, printing or publication of new brochures, manuals and forms.

Finally, the statement that DMV initiated additional research in this area “as a result of” the OSC audit is inaccurate. Our research efforts to identify a viable means to provide Spanish web content pre-date the audit. As a result of thorough research, we were able to identify translation technology and software that will support a practical, cost-effective and reliable long-term automated machine translation solution for our website.

- 4 & 5. In keeping with DMV’s role as a leader among state agencies in the area of e-commerce/e-government, we developed and posted a privacy and security policy statement long before a formally recognized standard was available for state agency websites. In the absence of such a standard, we researched the contemporary best practices on the Web and drafted a statement which was posted on the website following our normal content review processes.

With the recently passed Internet Security and Privacy Act (State Technology Law, Article II), a controlling standard for website privacy and security policy statements has now been established for state agencies. DMV is currently revising its security and privacy statement, using the model provided by the NYS Office for Technology (OFT), to develop a statement that will comply with the Act and other applicable laws and guidelines, including the Personal Privacy Protection Law. The draft is subject to review by our Legal unit for approval before being posted on the website. Furthermore, as was explained to OSC during the audit, the Driver Privacy Protection Act (DPPA) continues to be a guiding framework for protecting motorists’ personal information that DMV collects and stores.

6. Last fall, DMV implemented two specific strategies to increase the usage of our core transactions, including inserts in renewal invitation mailings and changes to our automated voice response system to promote the Internet transactions. Through these and additional strategies, we will continue our longstanding efforts to promote the DMV website and Internet transactions and services through press releases, advertising and promotional materials.
7. We have procured a vendor, TruSecure, to perform a perimeter scan and vulnerability assessment. The initial scan has been performed and the vulnerability assessment is underway. TruSecure will work with us to identify an intrusion detection system that

meets our needs. They also will make recommendations for information security procedures and policies, and have provided us with sample policies for our use.

Although we do not have written procedures and schedules in place for information security system maintenance and updates, we do perform them on an as-needed basis. We receive alerts from OFT frequently, sometimes several times a day. These alerts are reviewed as they come in and necessary safeguards put in place. In addition, we daily review security warnings and notifications from Microsoft, IBM, Symantec, and TrendMicro. We also research technology and security news articles from CNN, MSNBC, the Times Union, SANS, to name a few.

8. We agree that we need a written contingency plan and disaster recovery plan for our e-government operations; however, it is important to note that we do back up data and software on a routine basis for all of the servers involved in the Internet and beyond. We have cold stand-by servers available in the event of a hardware failure. All of the services available on the Internet are also available from other sources, such as via the mail, directly from Issuing Offices, and through our Call Centers.