As expected, the legislative session had ended with four new exceptions to the Sunshine Law. Now, before anyone suggests that this is a terrible turn of events, let me suggest that the session started with both the public utilities and the public hospitals looking to pass new exceptions benefitting their goals – to close a large portion of public records from those entities – and neither entity was successful, so things could have been much worse than was the final case.

Assuming the Governor signs Senate Bill 712, which is expected to occur, we will have new exceptions relating to security issues of public utilities, security systems of public bodies, access to computer records, and credit card number records.

New exception 18 states:

> A municipal utility receiving a public records request for information about existing or proposed security systems and structural plans of real property owned or leased by the municipal utility, the public disclosure of which would threaten public safety, shall within three business days act upon such public records request, pursuant to Section 610.023. Records relating to the procurement of or expenditures relating to security systems shall be open except to the extent provided in this section;

Clearly, the intent of this exception had been to use it as a vehicle to close certain records of public utilities. In the course of the legislative process, numerous changes were made to it and in the end, all it does is say that public utilities, in dealing with security system information requests, must follow existing procedure in the Sunshine Law, except as the law is amended by the new Section 19, which follows.

The new Section 19 provides:

> Existing or proposed security systems and structural plans of real property owned or leased by a public governmental body, the public disclosure of which would threaten public safety. Records related to the procurement of or expenditures relating to security systems shall be open except to the extent provided in this section. When seeking to close information pursuant to this exception, the public governmental body shall affirmatively state in writing that disclosure would impair the public governmental body's ability to protect the security or safety of persons or real property, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records. This exception shall sunset on December 31, 2006;

Homeland security advisors in the state assert that the availability of security plans for governmental buildings constitute a risk of harm to the public. With the change in concern about such issues following the September 11 actions, it is hard to argue that they are overreaching in asking for such an exception. This exception was worded so as to attempt to limit the information that will be closed while still making available to the

public the important financial issues that relate to government operations. And the language terminating the exception provides an opportunity to reconsider whether such an exception is really needed at a time when emotions are less raw on this issue.

The third new exception, Exception 20, closes:

> Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network, of a public governmental body. This exception shall not be used to limit or deny access to otherwise public records in a file, document, data file or database containing public records. Records related to the procurement of or expenditures relating to such computer, computer system, computer network, or telecommunications network, including the amount of moneys paid by, or on behalf of, a public governmental body for such computer, computer system, computer network, or telecommunications network, shall be open except to the extent provided in this section;

There has been discussion for some time about protecting access to information about computer systems that would allow disruption of a computer system by an unauthorized user. The language contained in this exception is an attempt by lawyers to deal with this issue. Since it was not written by computer technicians (no doubt in an effort to make sure that the public could understand what we were talking about), we will have to wait to see if the language used does what it was hoped to accomplish.

Finally, the last new exception, number 19, provides:

> Credit card numbers, personal identification numbers, digital certificates, physical and virtual keys, access codes or authorization codes that are used to protect the security of electronic transactions between a public governmental body and a person or entity doing business with a public governmental body. Nothing in this section shall be deemed to close the record of a person or entity using a credit card held in the name of the public governmental body or any record of a transaction made by a person using a credit card or other method of payment for which reimbursement is made by a public governmental body.

Government has begun doing e-commerce more frequently than ever. This, added to the fact that many entities now allow payment of charges by credit card, results in a situation where personal credit card numbers are more frequently showing up in public record materials. As a result, changes were suggested to protect these critical card and code numbers from public access. The language was drafted in an effort to ensure that this does not close to public scrutiny the financial transactions of public employees

spending public funds. It is critical that the watchdog role played by the public over these expenditures not be harmed in any way in the efforts to adapt to the changing role of electronic financial transactions.

All of these changes would seem to be logical and limited so as to protect the public's right to know about its government's activities. Credit goes to Doug Crews, executive director of the association, and its lobbyists, Kathi Harness and Harry Gallagher, for their fine efforts to watch proposed legislation for efforts to close this access.